Software 6 Management Guide

Release 6.8.3

Westermo Teleindustri AB

February 14, 2018

Version control

Document identification	Software 6 Management Guide
Authors	Westermo Teleindustri AB
Owner	Westermo Teleindustri AB
Revision hash	795ffa1c48c8c0ee185552ad187d6c956f163e1a

Contents

1 Introduction

This document describes the functionality and features of the *Software 6*. The *Software 6* is the firmware controlling the operation of the *RT300* family products.

The *RT300* family products are wireless communication devices for demanding industrial applications. The *RT300* family devices can operate at 2.4 and 5GHz WLAN bands depending on installation country limitations.

The devices can generally operate either as Access Point or Station. The operation is compatible with commercial IEEE 802.11 WLAN devices allowing co-existance with standard WLAN devices.

Software 6 delivers a complete set of functionality including:

- layer-2 basic switching,VLAN, etc.
- layer-3 routing, etc.
- higher-level services such as DHCP, DNS, etc.

1.1 Product versions

This document applies to the following product versions

Part Number	Name	Description
103999	RT-310	WLAN Onboard Access Point
104168	RT-320	WLAN Node
104169	RT-370	WLAN Access Point

1.2 Installation Country, Product Use

Installation country regulatory limits and operating parameters are controlled by *RT300* devices software driver Country Code. The Country Code limits are equally valid for Station and Access Point operation modes.

RT300 devices support:

Country Code	Frequency Range	Notes
Europe(EU)	2400-2483.5 MHz, 5150-5350 MHz and 5470-5725 MHz	Operation according to ETSI limitations.
United States(USA)	2400-2483.5 MHz, 5150-5350 MHz, 5470-5725 MHz and 5750-5850 MHz	Operation according to FCC limitations.

1.3 Delivery content

The *RT300* devices are delivered without connection cables, and any plugs, adapters etc. The delivery includes one dust cap for one ethernet interface.

1.3.1 Important safety notes

Danger! Do not use damaged equipment and/or accessories such as damaged power cord.

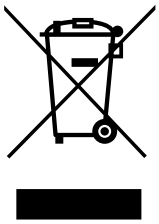
Danger! Never try to open the device. There are no serviceable parts inside! By trying to open the device you will be exposed to a risk of death or injury.

Warning! Never unplug equipment from the electrical outlet by holding the cord only, always disconnect the cable by applying force directly to the plug.

Warning! Do not operate the device in any other environmental conditions than it is designed for.

Warning! Before attaching the power cable to the device, please make sure you have antennas or terminators attached to the antenna connectors.

1.4 Information on Disposal of Old Electronic Equipment



This symbol on the product indicates that this product should not be treated as household waste when disposing it. Instead it shall be handed over to an applicable collection point for the recycling of electrical and electronic equipment. By ensuring this product is disposed correctly, you will help prevent potential negative consequences to the environment and human health, which could otherwise be caused by inappropriate disposal of this product.

2 Installation

Installation step	Description
Fixing	Fix the products in their use environment, ensuring that the fixing environment complies with the installation environment constrains. Ensure correct system grounding based on customer's electrical installation.
Antennas	Install the antenna interfaces according to customer's requirements.
Ethernet	Connect the Ethernet interfaces.
Power Feed	Connect the power cable first to the device and then to the power plug. Verify that the LED indicators shows correct power up procedure.
Configuration	Configure the device.

3 Quick Start

This section provides a simple guide to quickly get started with your WLAN modem. Only the following simple configurations will be covered:

- Access Point setup
- Client setup

3.1 Starting the product for the first time

Warning! Before attaching the power cable to the device, please make sure you have antennas or terminators attached to the antenna connectors.

When booting the WLAN modem for the first time, the modem will use the factory default settings. With factory default settings the WLAN modem operates as an access point with layer-2 bridge, where the WLAN interface and the two Ethernet ports belong to the same bridge.

The default IP setting for the WLAN modem is:

- IP address: 192.168.1.20
- Netmask: 255.255.255.0
- Default gateway: 0.0.0.0

Before you connect the modem with your LAN, you should change its IP setting according to your network topology.

3.2 Setting the IP address

The WLAN modem can be configured either to use a static IP address, or to obtain a dynamic one via DHCP.

3.2.1 Setting the IP address via WebGUI

To configure the IP settings via WebGUI your PC needs to be located on the same IP subnet as the modem, i.e. the PC should be assigned an IP address on the 192.168.1.0/24 network. For example:

- PC IP address: 192.168.1.1
- PC Netmask: 255.255.255.0

Open your web browser and enter URL **http://192.168.1.20** in the browser's address field. You will be asked to enter a username and a password. Use the the factory default account settings shown below:

- Username: webadmin
- Password: admin

From the menu choose **Configuration - Advanced** entry. The current settings will be displayed. The **IP address** (including **Netmask**) settings are under the "Network" topic, modify these to your liking. If you want to get the IP address automatically from the DHCP server change the **Protocol** to "dhcp".

You can set the **Default Gateway** under the topic "Routing". A value of "0.0.0.0" means that there is no Default Gateway in use.

To apply your changes click the "Apply" button.

Your settings will then be applied. Wait some time before accessing the WebGUI from your newly set IP address.

4 Administration

The operation parameters in configuration let you choose the needed functionality. The configuration files are stored in the device. The devices are delivered with **Default Settings**. These settings define a set of parameters for typical device use.

Following maintenance and configuration interfaces are supported by the software:

1. **Web-based management:** Web interface offers fast access to basic functions and status information - see Web-Based Management.

2. **Simple Network Management Protocol :** is the main interface for maintenance and configuration. Access is done via remote host application - see Simple Network Management Protocol (SNMP).

3. **Configuration Files:** can be used to backup the configuration of a device. Later it can be used to restore the previous configuration - see Configuration Files.

4. **Command Line Interface (CLI):** The CLI offers you the same scope of operation as with SNMP over Secure Shell (ssh) or Telnet - see Command Line Interface (CLI).

Important: During boot-up and configuration phases write operations to the flash are performed. To avoid loss of data, it is absolutely necessary to avoid power loss during these procedures.

Important: If power is switched off during boot-up or configuration phase, the device will fail to boot. It can manifest itself by green/yellow/orange LED glowing all at the same time or solid red Failure LED with device not being able to communicate.

4.1 Web-Based Management

Graphical user interface (HTTPS) can be accessed with web-browser via the IP address of the device:

- Default IP: 192.168.1.20

- Default user name: webadmin
- Default password: admin

Note that most of the device configuration items but only a limited set of commands are available via the graphical user interface (HTTPS).

4.2 Simple Network Management Protocol (SNMP)

The SNMP interface is used for controlling the device via Network Management System (NMS). The device includes an SNMP agent and a SNMP trap daemon. The SNMP agent is answering requests from the SNMP NMS. The SNMP trap daemon is responsible for sending un-requested events and exception conditions to the NMS.

As graphical SNMP tool we recommend iReasoning MIB browser. It is supported on many OS-platforms and it is easy to use. However, it is not free for professional use (see http://www.ireasoning.com/mibbrowser.shtml for details).

For command line and scripting purpose you can use Net-SNMP, which is open source and free to use (see http://www.net-snmp.org/ for details).

SNMP exposes management data in the form of variables of the managed system. These variables describe the system configuration. They can be queried and changed by managing applications.

SNMP gives you many options for configuring and monitoring the device. To get access to the configuration and other parameters use the following settings for the SNMP client:

Parameter	Default
cfgSnmpdVersion	v2c
cfgSnmpdComAdmin (Read-/Write Community)	admin-community

All variables of the device are defined and described in the Management Information Base (MIB). In case of the *RT300* devices this is done through the WESTERMO-SW6-MIB file and others, which is part of the delivered software package.

4.2.1 Supported Commands

Command	Description
GET	For reading parameters
SET	For modification of parameters
TRAP	For notifications. TRAPs can only be sent if the address of the NMS is configured (includes NOTIFICATIONS, INFORM) NOTE: TRAP messages are sent using SNMP Version 2c.

4.2.2 Availability

Access	Description
Using SNMP in custom application	For most programming languages there exists an SNMP library which can be used. This enables the integration of dedicated SNMP requests into an application without the need for additional external tools.
Accessing the SNMP parameters via command line interface (CLI)	For developing purposes, the command line tools from the Net-SNMP project has been used.
Using commercial NMS	Integrate a MIB into a full size NMS, like HP OpenView, Castle Rock SNMPc.

4.2.3 Example: Change and permanently save a Parameter through SNMP command line tool

The following information must be available for SNMP tool to access the SNMP capable device:

- MIB information
- IP address of the device
- Admin Community string if SET operations are required (admin-community)

If a parameter is changed through SNMP, the value is only stored in volatile memory. To permanently store the parameter, the change must be applied. For an example see the following steps:

1. Change the parameter

```
snmpset -v 2c -c admin-community 192.168.11.238 WESTERMO-SW6-MIB::cfgSysHostname.0 s testname
```

2. Verify the change

```
snmpget -v 2c -c admin-community 192.168.11.238 WESTERMO-SW6-MIB::cfgSysHostname.0
```

3. Apply the change

```
snmpset -v 2c -c admin-community 192.168.11.238 WESTERMO-SW6-MIB::rpcCfgApply.0 i 1
```

Now, the change has been saved to the user configuration file.

4.3 Configuration Files

The configuration items of a device can be exported to or imported from a configuration file. This export or import can be done either by using an SNMP manager or simply by using the web-based user interface. The exported configuration file is plain text, which allows to edit it using a simple text editor.

Since the parameter names and types used in the configuration file are the same as in the MIB database (WESTERMO-SW6-MIB and others), the documentation of each parameter can be found in the description of the MIB.

4.4 Command Line Interface (CLI)

The CLI offers you the same scope of operation as with SNMP over Secure Shell (ssh) or Telnet.

CLI configuration parameters with defaults:

Parameter	Default
cfgCliEnabled	enabled
cfgCliUsername	admin
cfgCliPassword	admin
cfgCliSshEnabled	enabled
cfgCliSshPort	22
cfgCliTelnetEnabled	disabled
cfgCliTelnetPort	23

CLI commands:

Command	Description
help, ?	Show available commands and help text for each command.
get	Return current value for the given key.
set	Set value. For configuration parameters the value is set in the staging configuration on the device and requires a subsequent apply. Changes done in the CLI session can be diplayed with the command *changes*.
changes	Return list of changes.
validate	Not implemented.
apply	Apply all pending changes of the staging configuration on the device.
revert	Revert all changes in the staging configuration.
reset	Reset configuration to factory defaults. Set essential configuration and apply.

The following examples shows how to access the device using ssh and getting started with the CLI commands *help*, *get*, *set* and *apply*.

```
user@host:# ssh CLI@192.168.1.20
CLI@192.168.1.20's password:


BusyBox v1.25.1 () built-in shell (ash)

/ #
```

```
/ # help

Command Line Interface (CLI) v0.2

Available commands:
 * help, ?
 * get, set
 * changes, validate, apply, apply_force, revert, reset
```

```
/ # help get

get <MIB>::<key>

Return current value.

Example: get WESTERMO-SW6-MIB::cfgSysHostname.0
```

```
/ # get WESTERMO-SW6-MIB::cfgSysHostname.0
Rmodem
```

```
/ # set WESTERMO-SW6-MIB::cfgSysHostname.0 foo

/ # apply
Apply RPC issued, waiting for apply process to terminate...
Successfully applied all pending changes.
```

4.5 Factory Settings and Reset

The *Software 6* is delivered with a default device configuration. A Factory Reset will reset the device configuration (including administrator password and https/802.1x certificates) to its default state.

The following list shows the most important default configuration values which are needed to access the device. More default configuration values are listed in Default values.

Network	
IP Address Mode	static
IP Address	192.168.1.20, Factory IP address to access the device
IP Subnet Mask	255.255.255.0
Basic Configuration	
SNMP	Enabled

4.5.1 Factory Reset using Reset Plug

1. Power off the device
2. Plug-in the RESET PLUG in one of the ethernet ports
3. Power on the device
4. Wait until Operation (orange) and Failure (red) LED are constantly on
5. Remove the RESET PLUG: Operation (orange) and Failure (red) LED will blink three times
6. Wait (approx. 1 minute) until device is rebooted, then you can access the device using the factory default IP

4.6 Technical Support File

The *Technical Support File* is a compressed tar file with collected system information, including log files and system configuration. It is accessible using the web interface. After logging in, go to *System* and then *Support*.

Download Technical Support File

Click this button to create and download the Technical Support File.

Warning: Passwords and other sensitive information may be included in the report.

The device checks during boot-up if any Kernel Log(s) are available. It will report this issue with a system message. Before resetting the Kernel Log(s) you should first download the Technical Support file and send it to your support contact.

Reset Kernel Logs

This action is **irreversible** and will take approx. 20 seconds.

4.7 Status Indication

4.7.1 LED Indicators

RT300 familiy devices are equipped with five LED indicators:

Power	The Power LED (1) indicates whether or not power is connected to the device.
Operation	The Operation LED (2) is flashing during boot up and afterwards shows a solid green after the device is booted. When wlan0 is configured in Station Mode and the wireless connection to the Access Point fails, the LED shows a solid orange.
Status	The Status LED (3) indicates errors and warnings which require the intervention of the operator. When an error occurs, the Status LED show a solid red where in case of warning the LED is orange. In this case please check the troubleshooting chapter of this manual.
ETH1/ETH2	The Ethernet LEDs (4+5) show link status and activities on the respective ethernet interfaces ETH1/ETH2.

4.7.2 Firmware Update State

When a firmware update is in progress, the Operation LED (2) is flashing orange and the Status LED (3) is flashing red until device reboot. IMPORTANT: One MUST NOT interrupt the power source until normal operation state is reached.

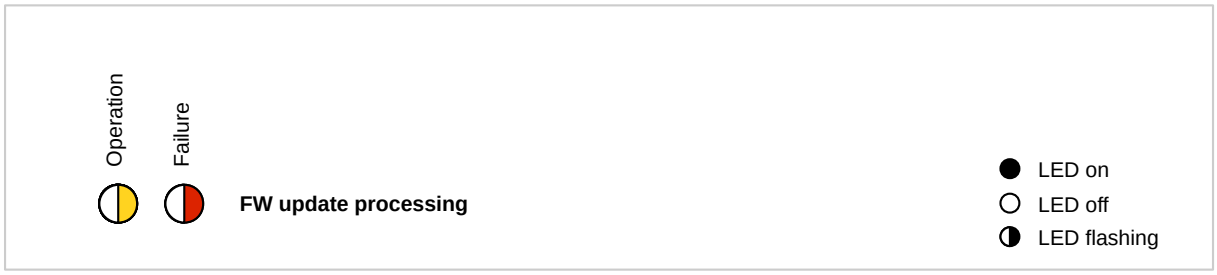


Figure 4.1: *LED state when updating the firmware*

4.7.3 Factory Reset State

Operation LED (2) is solid orange and Status LED (3) is solid red when a factory reset is detected. Both LEDs are blinking when the factory reset is in process. See also Factory Settings and Reset.

Figure 4.2: *LED state when factory reset is active*

4.8 Monitoring TRAPs

SNMP traps enable the device to notify the management station of significant events by way of an unsolicited SNMP message. The remote host can listen to SNMP traps in order to get notified about

important events (like handoff notification) of the device. For a description how to use this feature see SNMP trap daemon on page 48.

4.9 Alarm Handling

System warnings are indicated by the Status LED (solid orange). System errors are indicated by the Status LED (solid red). Warning and error messages are logged on the device and can be seen in the Web Interface (Status - View Log - System Messages). A detailed description of the single error codes can be found in Message Codes on page 200.

For additional error analysis, the system log is available in the Web Interface (Status - View Log - System Log).

4.10 System Firmware

System firmware consists of two types of firmware images: 1. bootloader image and 2. primary firmware image. The primary firmware image contains the main system software and the features described in this document.

4.10.1 Upgrading System Firmware

The system firmware can be upgraded via Web Interface or via SNMP.

4.10.1.1 Upgrading Firmware via Web Interface

In order to upgrade the firmware via Web Interface, your PC needs to be located in the same IP subnet as the device. When the device is using the default IP address (192.168.1.20), then the connected PC might be configured as follows:

- PC IP address: 192.168.1.1
- PC Netmask: 255.255.255.0

Open your web browser and enter the IP address of the device (default **https://192.168.1.20**) in the browser's address field. You will be asked to enter a username (default: 'webadmin') and a password (default: 'admin'). Then click on **Login** button.

Once logged in choose menu entry **System - Maintenance**. In section **Flash Firmware** you can browse your PC file system for the firmware image by clicking the **Browse...** button.

Concerning device configuration, the following three options are available:

1. **Reset to default configuration**: Device configuration will be reset to its default values.

2. **Keep the current configuration**: Device configuration will not be changed. If the new firmware image provides new configuration items, these will be initialized with their default values.

3. **Apply custom config after upgrade**: See more detailed description below.

After selecting the image file (and the custom configuration file if you have chosen **Apply custom config after upgrade**), proceed to uploading and flashing by clicking the **Flash Firmware** button. A verify page will be displayed with checksum and size information. Click **Proceed** in order to finally start the firmware upgrade process on the device.

When you haven selected **Apply custom config after upgrade**, then the following steps will be processed:

1. Firmware image will be uploaded to the device.

2. Device will be upgraded using new firmware image.

3. Device configuration will be reset to new firmware image default values.

4. Provided custom configuration will then be applied. In order to assert that this custom configuration is valid for the new firmware image, it should best have been exported from a device already using the new firmware image.

4.10.1.2 Upgrading Firmware via SNMP (using TFTP server)

1. Define a valid URL which is accessible by the device. This is done by changing the firmware URL parameter setFwFileUrl in the settings section.

2. Optional: If you want to reset the device to factory settings, set setFwKeepConfig to 'reset(0)'. If you want to use a *custom config* (see paragraph above), define a valid URL in setCfgFileUrl.

3. Writing 'flash(2)' to rpcFwFlash parameter will download and validate the new firmware file. Writing 'download(1)' to rpcFwFlash parameter will only download and validate the new firmware file, but will not flash to the file system. Writing 'flashWithConfig(3)' to rpcFwFlash parameter will download and validate the new firmware file and the custom config file.

4. If the downloaded file is considered a valid firmware for this device, it will be flashed to its file system.

5. Reading rpcFwFlash parameter will report the status of the firmware flash process. A value of 'flash_error(-2)' denotes that the flash process failed during write of the firmware file to the file system. A return value of 'download_error(-1)' indicates an error while the firmware was downloaded or validated. A value of 'flash(2)' means that the device is writing the firmware to the file system.

4.11 Network Configuration Concept

The IP configuration is separated from the interface configuration (Ethernet, Wlan, Vlan, ...) so that there is a single way of how to assign IP addresses to interfaces.

Bridges are able to handle VLANs.

- Untagged frames are internally handled by using VID 0.
- If you need to reach the device over an Ethernet or Wlan interface which is part of a bridge, you need to configure a VLAN and assign an IP address to this VLAN.
- There are 3 different VLAN Modes available: 'trunk', 'access' and 'native untagged'. For more information about VLAN Modes see cfgNetEthVlanMode and cfgNetWlanVlanMode.

As long as an interface is not part of a bridge, you can add an IP address directly to this (Ethernet or Wlan) interface. For more information about adding an IP address to an interface see cfgNetIpInterface.

All IP addresses are configured using Classless Inter-Domain Routing (CIDR) notation (e.g 192.168.1.20/24).

5 Services

5.1 IP Adresses and Network Interfaces

5.1.1 IP Address Settings

IP Addresses are configured under cfgNetIpTable as follows:

- cfgNetIpEnabled: enables (1) or disables (0) this entry
- cfgNetIpAddr: IP address in CIDR notation (e.g. 192.168.1.20/24)
- cfgNetIpProto: selects static (0) or dhcp (1) IP address configuration
- cfgNetIpInterface: Name of the interface on which the IP resides (Examples: br0.vlan0, wlan0, eth0). Possible interface names which can be referenced are defined in cfgNetEthName, cfgNetVlanName and cfgNetWlanName.

5.1.2 Ethernet Network Interface Settings

The network settings are configured under cfgNetEthernetTable as follows:

- cfgNetEthName: name of the Ethernet interface (e.g. eth0, eth1)
- cfgNetEthEnabled: enables (1) or disables (0) the Ethernet interface
- cfgNetEthBridge: if set to -1, interface is not part of a bridge; otherwise it belongs to the bridge configured under the according index (e.g. 0 = br0, 1 = br1, etc.)
- cfgNetEthTrunk: active if cfgNetEthVlanMode is trunk (0) or nativeuntagged (3). Set to -1 to allow all VLANs.
- cfgNetEthTag: active if cfgNetEthVlanMode access (1) or nativeuntagged (3). It specifies which 802.1q VLAN should be used for untagged ingress and egress traffic. Set this entry go -1 to disable it.

- cfgNetEthVlanMode: trunk (0), access (1) or nativeuntagged (3).

5.1.3 Wireless Network Interface Settings

The network settings are configured under cfgNetWlanTable as follows:

- cfgNetWlanName: name of the WLAN interface (e.g. wlan0, wlan1)
- cfgNetWlanEnabled: enables (1) or disables (0) the WLAN interface
- cfgNetWlanBridge: if set to -1, interface is not part of a bridge; otherwise it belongs to the bridge configured under the according index (e.g. 0 = br0, 1 = br1, etc.)
- cfgNetWlanTrunk: active if cfgNetWlanVlanMode is trunk (0) or nativeuntagged (3). Set to -1 to allow all VLANs.
- cfgNetWlanTag: active if cfgNetWlanVlanMode access (1) or nativeuntagged (3). It specifies which 802.1q VLAN should be used for untagged ingress and egress traffic. Set this entry go -1 to disable it.
- cfgNetWlanVlanMode: trunk (0), access (1) or nativeuntagge (3).

5.1.4 VLAN Network Interface Settings

The network settings are configured under cfgNetVlanTable as follows:

- cfgNetVlanName: name of the VLAN interface. The VLAN interface name depends on the value of cfgNetVlanBridge, cfgNetVlanParent and cfgNetVlanVid (e.g. br0.vlan0, eth0.vlan0)
- cfgNetVlanEnabled: enables (1) or disables (0) the VLAN interface
- cfgNetVlanBridge: if set to -1, interface is not part of a bridge; otherwise it belongs to the bridge configured under the according index (e.g. 0 = br0, 1 = br1, etc.)
- cfgNetVlanParent: name of the physical parent interface on which the VLAN resides. This entry is only active when the VLAN interface is not part of a bridge (cfgNetVlanBridge = -1).
- cfgNetVlanVid: ID of the VLAN. Untagged frames are internally handled by using VID 0.

5.2 Wireless

The wireless settings can be divided into three levels:

- **Network interface settings (cfgNetWlanTable)** - such as bridge, VLAN mode, etc.
- **Physical WLAN radio settings (cfgWlanDeviceTable)** - such as frequency and output power
- **Logical WLAN interface settings (cfgWlanInterfaceTable)** - such as operating mode, SSID, encryption and allowed bitrates, up to 16 logical WLAN interfaces can be configured

5.2.1 Physical WLAN Radio Settings

The settings in cfgWlanDeviceTable define the physical level settings for each WLAN radio available in the product. The number of available physical radios is depending on the product variant:

- DT-5302R: radio0 (for communication)
- AP-5312F: radio0 (for communication), radio1 (monitoring only)

Physical settings of a radio are common to all logical WLAN interfaces created on top of it.

The most important settings are explained in the following paragraphs.

5.2.1.0.1 Bandwidth sets the Wireless Bandwidth Mode cfgWlanDevBandwidth by specifying the bandwidth of the channel. Available bandwidths are:

- 0: HT20 20MHz wide channel
- 1: HT40+ 40MHz wide channel with extension channel above primary
- 2: HT40- 40MHz wide channel with extension channel below primary

HT40+ and HT40- can only be used on frequencies where primary and extension channels are fully within the available frequency band. The following table shows examples for valid channels. The full list can be found in IEEE 802.11n Annex J. Depending on the country of operation,not all frequencies may be available. The frequency is set with the cfgWlanDevFrequency parameter in MHz.

Examples:

Band	HT40+	HT40-
2.4 GHz	2412 to 2452	2432 to 2472
5 GHz	5180, 5220, 5260, etc.	5200, 5240, 5280, etc.

Note that the cfgWlanDevFrequency will be overridden when in STA/client operating mode and a frequency list has been specified in cfgWlanIfaceScanList.

5.2.1.0.2 Modulation sets the modulation mode (cfgWlanDevModulation) of the physical wireless radio device. The supported modes are:

- g(2): This modulation mode uses data rates up to 54 MBit/s in the frequency band between 2.4 and 2.4835 GHz. It supports the 802.11g standard. The modulation is either DSSS for the lower rates or OFDM for the higher ones.
- a(4): Mode supports data rates up to 54 MBit/s in the 5GHz frequency band and only OFDM modulation.
- n(8): Mode supports data rates up to 300 MBit/s in the 2.4GHz and 5GHz frequency band and only OFDM modulation. n-rates can not be used standalone but only in combination wit g or a to specify which frequency band shall be used.
- 10(ng): for 2.4GHz
- 12(na): for 5GHz.

In standard applications it is recommended to use the ng or na modes. Legacy modes (a or g) are only usable in application with low throughput requirements. Above that, in mobile environments or under specific conditions, legacy modes in combination with fixed data rates might perform better than in n modes.

5.2.1.0.3 Output Power and Antenna Gain are defining the resulting output power of the physical radio device. cfgWlanDevPower can be used to limit the combined EIRP power of all active TX antenna chains (cfgWlanDevTxAntenna) in dBm including the antenna gain (cfgWlanDevAntennaGain). The antenna gain is the value of the installed antenna in dBi. If multiple antennas with different gains are connected, the value of the antenna with the highest gain shall be configured.

Note that the maximum combined EIRP is limited by local regulations for each country. Please got to the page *Application -> Regulatory Domain Manager* in the graphical user interface (HTTP) to get more information about the maximum achievable RF output power of your device.

5.2.1.0.4 Distance sets the maximum distance (cfgWlanDevDistance) in meters a client can be away from the access point. Even though the distance is set in meters, the slot time settings change in 450m steps. In order to maximize the MAC layer efficiency it is recommended to keep this setting as low as possible.

5.2.1.0.5 Transmission Retries can be set with cfgWlanDevShortRetry and cfgWlanDevLongRetry. The short retry defines the number of retransmissions of the RTS frame if there is no CTS received from the AP, whereas the long retry defines the number of retransmissions for unicast data frames not ACKed by the receiver.

In wireless environments retries on physical level are inevitable. Generally it is recommended to set lower values for UDP traffic and higher values for TCP. If the used channel is overloaded, excessive retransmissions can introduce a negative feedback-loop reducing available bandwidth even further.

5.2.1.0.6 TX and RX Antennas are configured in with cfgWlanDevTxAntenna and cfgWlanDevRxAntenna. The configuration is a bitmask to enable/disable the chains. Depending on the product variant, there are either two or three chains available.

- 1(001) means chain 0 enabled
- 3(011) means chain 0 and 1 enabled
- 7(111) means chain 0, 1 and 2 enabled

The number of enabled chains should match the number of antennas used.

Note, that with one chain enabled only, the 1-stream bitrates (cfgWlanIfaceBitrates) MCS0 to MCS7 can be used. With two chains enabled, the 1- and 2-stream bitrates (cfgWlanIfaceBitrates) MCS0 to MCS15 can be used.

Note, that enabling additional antennas will automatically reduce the output power of each chain as explained in Paragraph Output Power and Antenna Gain.

Also note that if only one antenna is used, the used antenna must be the Antenna 1 (chain 0 i.e. 001).

5.2.2 Logical WLAN Interface Settings

Up to 16 logical interfaces can be configured and enabled simultaneously in cfgWlanInterfaceTable. This table configures the logical WLAN interfaces which can be added on top of the physical radios which were explained in Physical WLAN Radio Settings.

The most important logical WLAN interface setting are explained in the following paragraphs.

5.2.2.0.1 Operating Mode of the WLAN interface can be set with cfgWlanIfaceMode. The supported modes are AP, STA, and MONITOR.

AP is the standard Access Point / Infrastructure mode. This mode is typically used at the infrastructure side in stationary installations. One access point supports up to 200 simultaneous client connections. The AP interface is usually bridged to the Ethernet or to a VLAN directly.

STA is the station/client mode. This mode is typically used at the mobile part of the system. Stations provide a router functionality between the WLAN and Ethernet interface and therefore usually keep the bridging disabled.

The MONITOR mode allows use the interface in a fully passive monitoring mode. It is used to listen to WLAN traffic or scan for wireless interference and off-channel radar signals. Please consult the support for details, if you want to use this mode.

5.2.2.0.2 Service Set Identifier (SSID) of the wireless interface is set with cfgWlanIfaceSsid. SSID is the arbitrary name of the wireless network this interface is part of.

5.2.2.0.3 Encryption can be set with cfgWlanIfaceEncryption. Two encryption modes are currently supported: open(0) and WPA2(3). It it highly recommended that WPA2 encryption is used. The password for the WPA2 can be set with cfgWlanIfacePassword.

5.2.2.0.4 Bitrate Limitations can be set with cfgWlanIfaceBitrates. This setting can be used to set fixed MCS index or range for 802.11n rates. Set to -1 to disable (leave on auto). It is also possible to enter multiple indices divided by a space which are then used in auto rate. This entry is only active when an n-mode is set in cfgWlanDevModulation, and is ignored if g-rates or a-rates are used.

5.2.2.0.5 Enabling Wireless Multimedia Extensions (WME) for the interface is possible with cfgWlanIfaceWmeEnabled. When using legacy rates (a-rates and g-rates), this is optional. When using n-rates, this always has to be enabled. WME uses all parameters in the cfgWlanWmeTable whose cfgWlanWmeId is set to the value in cfgWlanIfaceWmeParameter. For more information about WME tables please check Quality of Service (QoS).

5.2.2.0.6 MAC Address Access Control List (ACL) mode for the interface can be set in cfgWlanIfaceMacaddrAcl. The available modes are:

- 0: Accept unless deny filter - accepts every MAC unless it is on the list defined in cfgWlanAclBlackTable.
- 1: Deny unless accept filter - denies every MAC unless it is on the list defined in cfgWlanAclWhiteTable.
- 2: Use RADIUS to accept/deny clients.

ACL can only be set if the operating mode of the interface is set to AP.

5.2.2.0.7 Scan Channels in station mode are configured with the cfgWlanFreqTable frequency lists. Each of those lists can hold up to 24 entries. Unused entries at the end of the list must be set to 0. In order to assign a frequency list to a WLAN interface, the list index is set in cfgWlanIfaceScanList. As factory default the index 0 (cfgWlanFreqTable.0) includes all 2.4Ghz center frequencies and the index 1 (cfgWlanFreqTable.1) includes all the 5Ghz center frequencies. In order to scan full country code all frequencies of the frequency list must be set to 0.

5.2.2.1 SSID Hide Feature

Service Set Identifier (SSID) specifies the name of a WLAN network. When people want to connect to a WLAN network, they normally check which WLAN networks are available in their neighbourhood, and then they choose the one they want to connect to.

If an Access Point provider does not want that random persons connect to their network, they will normally configure the Access Point so that the SSID is hidden. Then people not knowing the name of the WLAN network (i.e. its SSID) will not try to connect to this WLAN network by accident; but only people who know the name of the WLAN network will connect.

There are two MIB elements available to configure the SSID Hide Feature:

- cfgWlanIfaceIgnoreBroadcastSsid
- cfgWlanIfaceUseVendorSsid

Setting cfgWlanIfaceIgnoreBroadcastSsid to enabled(1) specifies that the SSID will not be announced in the beacon of the Access Point (AP). Additionally, probe request frames that do not specify the full SSID will not be answered by this AP. As a consequence, Clients/Stations need to know the SSID to be able to connect to this WLAN network.

When cfgWlanIfaceIgnoreBroadcastSsid is enabled, a passively scanning Client/Station (forced or because of DFS) has no way of detecting the AP it tries to find. For being able to connect to the WLAN network in these two cases, cfgWlanIfaceUseVendorSsid must be used:

- On an AP: set cfgWlanIfaceUseVendorSsid to enabled(1) so that the hidden SSID is added as vendor element in the AP beacon.
- And on a STA: set cfgWlanIfaceUseVendorSsid to enabled(1) to allow the Client/Station to use the vendor element in the AP beacon.

5.3 Public Wireless Network Access Point

For an initial configuration of an Access Point which is used as public wireless network AP configure at least the following items:

- SSID (cfgWlanIfaceSsid) - example: "wpwnap"
- Wireless password (cfgWlanIfacePassword)
- Wireless mode (cfgWlanDevModulation) - example: 2.4 GHZ = ng(10), 5 GHz = na(12)
- Wireless bandwidth (cfgWlanDevBandwidth) - example: ht20(0) or ht40Plus(1)
- Optionally set system hostname (cfgSysHostname) - example: "AP2G" or "AP5G-HT40+"

5.3.1 Configuration File Example: Access point 2.4GHz

Configuration File Example: Access point 2.4GHz

```
# Config.Format = raw
WESTERMO-SW6-MIB::cfgSysHostname.0 = AP2G
WESTERMO-SW6-MIB::cfgWlanIfaceSsid.0 = wpwnap
```

5.3.2 Configuration File Example: Access point 5GHz

Configuration File Example: Access point 5GHz HT40+

```
# Config.Format = raw
WESTERMO-SW6-MIB::cfgSysHostname.0 = AP5G-HT40+
WESTERMO-SW6-MIB::cfgWlanDevModulation.0 = 12
WESTERMO-SW6-MIB::cfgWlanDevBandwidth.0 = 1
WESTERMO-SW6-MIB::cfgWlanDevFrequency.0 = 5500
WESTERMO-SW6-MIB::cfgWlanIfaceScanList.0 = 1
```

5.4 Bridge Mode (4addr)

Bridge mode or WDS (Wireless Distribution System) mode is a non-standard extension to the wireless 802.11 standard using a 4-address-format to allow transparent ethernet bridging on the STA/client.

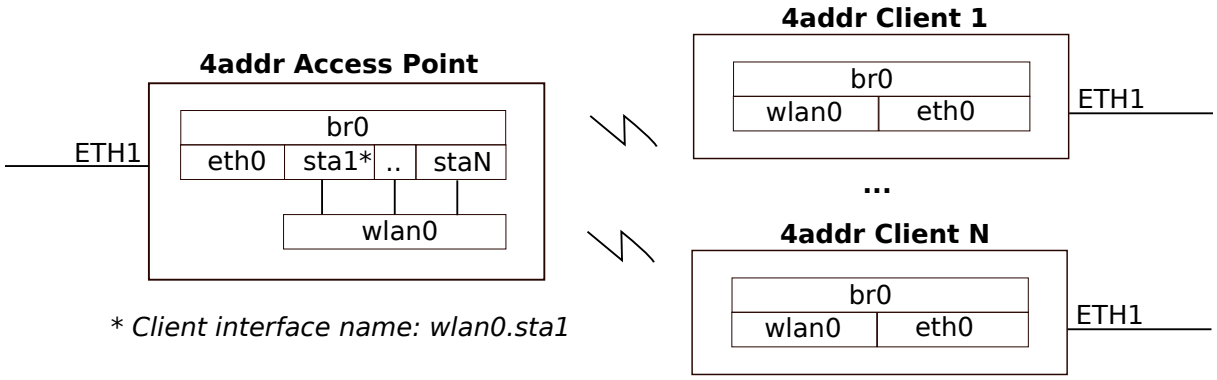


Figure 5.1: *Bridge Mode setup*

Configuration File Example: Access point

```
# Config.Format = raw
WESTERMO-SW6-MIB::cfgWlanIface4addr.0 = 1
```

Configuration File Example: STA/client

```
# Config.Format = raw
WESTERMO-SW6-MIB::cfgNetIpAddr.0 = 192.168.1.30/24
WESTERMO-SW6-MIB::cfgWlanIfaceMode.0 = 1
WESTERMO-SW6-MIB::cfgWlanIface4addr.0 = 1
```

5.5 Client MAC address configuration

It is possible to overwrite the MAC address of the wireless interface in client mode. This might be required to support applications where the MAC address of the client shall be the same as of the device attached to the device. The user can configure the MAC address of the attached wired equipment as the source MAC address of the wireless interface. The cloned address is then used for all wireless communication.

Configuration File Example: Configure new MAC for the wireless radio

```
# Config.Format = raw
WESTERMO-SW6-MIB::cfgWlanIfaceBssid.0 = STRING: 00:11:22:33:44:55
```

5.6 Port-based Network Access Control (802.1X)

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication and authorization mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X authentication involves three parties:

supplicant client device that wishes to attach to the LAN or WLAN (STA)

authenticator network device such as an Ethernet switch or wireless access point through which the supplicant is connected to the network (AP)

authentication server a host running software supporting the RADIUS and EAP protocols (AS)

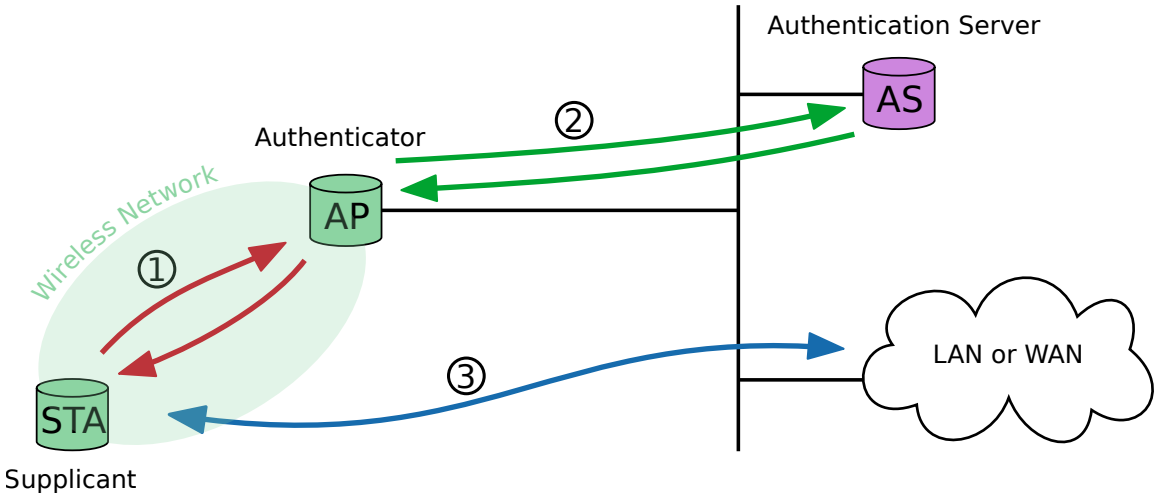


Figure 5.2: *Supplicant authentication using IEEE 802.1X*

The supplicant is not allowed to access through the authenticator to the protected side of the network ③ until the supplicant's identity has been validated and authorized. The authenticator acts like a security guard to a protected network. With IEEE 802.1X port-based authentication, the supplicant provides credentials to the authenticator ①. Accepted credentials can be user name/password or a digital certificate. The authenticator forwards the credentials to the authentication server for verification ②. If the authentication server determines the credentials as valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

The following example shows how to configure SW6 devices as supplicant (STA) and authenticator (AP).

Requirements

- Configured authentication server[1]
- PKI to generate digital certificates, valid client certificate files
- Time server to share time information between the hosts in the network

Wireless access point configuration

The following configuration example configures a device as authenticator:

Configuration File Example: authenticator

```
# Config.Format = raw
# basic AP configuration
WESTERMO-SW6-MIB::cfgSysTimezone.0 = CET-1CEST,M3.5.0,M10.5.0/3
WESTERMO-SW6-MIB::cfgNetIpAddr.0 = 192.168.3.22/24
WESTERMO-SW6-MIB::cfgWlanDevModulation.0 = 12
WESTERMO-SW6-MIB::cfgWlanDevFrequency.0 = 5180
WESTERMO-SW6-MIB::cfgWlanIfaceSsid.0 = radiustesting
WESTERMO-SW6-MIB::cfgWlanIfaceEncryption.0 = 6
WESTERMO-SW6-MIB::cfgWlanGlblCountry.0 = EU
WESTERMO-SW6-MIB::cfgNtpServer1.0 = 192.168.2.2
# IEEE 802.1X related configuration
WESTERMO-SW6-MIB::cfgWlan802dot1xAuthSrvEnabled.0 = 1
WESTERMO-SW6-MIB::cfgWlan802dot1xAuthSrvIpAddr.0 = 192.168.3.2
WESTERMO-SW6-MIB::cfgWlan802dot1xAuthSrvSharedSecret.0 = superSharedSecret
```

The authenticator does not need any certificate information. The shared secret 'superSharedSecret' has to match the authentication server client configuration.

The authenticator will forward incoming client authentication requests to the primary authentication server address (192.168.3.2). More than one authentication server address can be defined by adding more records to the authentication server configuration table.

Configuration File Example: authenticator, second authentication server address

```
# Config.Format = raw
# basic AP configuration
WESTERMO-SW6-MIB::cfgWlan802dot1xAuthSrvEnabled.1 = 1
WESTERMO-SW6-MIB::cfgWlan802dot1xAuthSrvIpAddr.1 = 192.168.3.2
WESTERMO-SW6-MIB::cfgWlan802dot1xAuthSrvSharedSecret.1 = superSharedSecret
```

If the primary authentication server is not reachable, an exponential back off is implemented:

- timeout of first attempt is 3 seconds

[1] FreeRADIUS 4 is used for internal testing, find the project under http://freeradius.org/ (February 2017)

- after each failure the timeout is increased to maximum timeout of 120 seconds
- the authenticator gives up after 10 attempts
- after the fourth attempt, a backup server (secondary, if configured) will be attempted

If none of the configured authentication server is reachable, the supplication will not be authorized to communicate over the access point (authenticator) - no communication is possible.

Wireless station configuration

If encrypted private keys are used for the client, the pass phrase to unlock the key has to be configured before the private key upload. If no matching pass phrase is provided, the client private key file will be rejected by the device.

Use the MIB element cfgWlan802dot1xClientKeyPassword to define the pass phrase and rpcCfgApply to apply the changes.

If the private key is not locked by a pass phrase (unencrypted), this configuration parameter is ignored.

Use the web interface to upload the certificate files: *System -> Certificate Manager -> 802.1X*. Each file is verified before it is stored on the device. The mandatory information can be provided in this files:

client.crt client certificate (public key, PEM or X509 format)

client.key client private key matching the client X509 certificate (RSA)

ca.crt authentication server X509 certificate (public key, PEM or X509 format)

The client private key file may also contain the full CA certificate chain information in PEM format: it can contain client private key and CA certificate chain information (one or multiple certificates) in one single file. Make sure that in this case no separate client certificate file is provided.

Alternatively SNMP can be used to upload the mandatory certificate information to the supplicant. The MIB element setCrtFileSelector is used to define what kind of file should be uploaded and for which interface it should be used. The following file classes are defined:

10x class 100 is used for client certificate files where x is the interface index

20x class 200 is used for client private key files where x is the interface index

30x class 300 is used for CA certificate files where x is the interface index

Client certificate file upload via TFTP:

- WESTERMO-SW6-MIB::setCrtFileSelector.0 100
- WESTERMO-SW6-MIB::setCrtFileUrl.0 tftp://192.168.2.2/client.crt
- WESTERMO-SW6-MIB::rpcCrtFile.0 1

Client private key file upload via TFTP:

- WESTERMO-SW6-MIB::setCrtFileSelector.0 200
- WESTERMO-SW6-MIB::setCrtFileUrl.0 tftp://192.168.2.2/client.key
- WESTERMO-SW6-MIB::rpcCrtFile.0 1

CA certificate file upload via TFTP:

- WESTERMO-SW6-MIB::setCrtFileSelector.0 300
- WESTERMO-SW6-MIB::setCrtFileUrl.0 tftp://192.168.2.2/ca.crt
- WESTERMO-SW6-MIB::rpcCrtFile.0 1

The following configuration example configures a device as supplicant.

Configuration File Example: supplicant

```
# Config.Format = raw
# basic STA configuration
WESTERMO-SW6-MIB::cfgSysTimezone.0 = CET-1CEST,M3.5.0,M10.5.0/3
WESTERMO-SW6-MIB::cfgNetWlanBridge.0 = -1
WESTERMO-SW6-MIB::cfgNetIpEnabled.1 = 1
WESTERMO-SW6-MIB::cfgNetIpAddr.0 = 192.168.2.11/24
WESTERMO-SW6-MIB::cfgNetIpAddr.1 = 192.168.3.11/24
WESTERMO-SW6-MIB::cfgWlanDevModulation.0 = 12
WESTERMO-SW6-MIB::cfgWlanIfaceMode.0 = 1
WESTERMO-SW6-MIB::cfgWlanIfaceSsid.0 = radiustesting
WESTERMO-SW6-MIB::cfgWlanIfaceEncryption.0 = 6
WESTERMO-SW6-MIB::cfgWlanIfaceScanList.0 = 2
WESTERMO-SW6-MIB::cfgWlanGlblCountry.0 = EU
WESTERMO-SW6-MIB::cfgNtpServer1.0 = 192.168.2.2
# IEEE 802.1X related configuration
WESTERMO-SW6-MIB::cfgWlan802dot1xClientKeyPassword.0 = superKeySecret
```

If no certificates are uploaded before applying WPA2-EAP as encryption mode (cfgWlanIfaceEncryption), the configuration apply will fail. NTP has to be enabled on the station (time sync on the access point is optional), make sure that the station shares the same time information and time zone configuration as the authentication server. This is later important for the successful certificate validation.

After applying the described configuration on supplicant (STA) and authenticator (AP), the STA should be successfully authorized. The STA authorization status can be verified using the STA's web interface: (*Status -> Wireless Connections -> Station Dump*).

Supported authentication and encryption algorithms

The TLSv1.2 cipher suites are supported and recommended to use:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384
- DH-DSS-AES256-GCM-SHA384
- DHE-DSS-AES256-GCM-SHA384
- DH-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- DH-RSA-AES256-SHA256
- DH-DSS-AES256-SHA256
- ADH-AES256-GCM-SHA384
- ADH-AES256-SHA256
- ECDH-RSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-SHA384
- AES256-GCM-SHA384
- AES256-SHA256

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256
- DH-DSS-AES128-GCM-SHA256
- DHE-DSS-AES128-GCM-SHA256
- DH-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- DH-RSA-AES128-SHA256
- DH-DSS-AES128-SHA256
- ADH-AES128-GCM-SHA256
- ADH-AES128-SHA256
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-SHA256
- AES128-GCM-SHA256
- AES128-SHA256
- NULL-SHA256

The cipher string format explained for ECDHE-RSA-AES256-GCM-SHA384:

ECDHE key exchange algorithm, Elliptic Curve Diffie-Hellman

RSA authentication algorithm, Rivest-Shamir-Adleman

AES256-GCM cipher algorithm, Advanced Encryption Standard with strength and mode (Galois Counter Mode)

SHA384 MAC or PRF algorithm, Secure Hash Algorithm with strength

5.7 Port management and switching

All Ethernet and one WLAN port on the device are enabled and bridged by default. Ethernet interfaces auto-negotiate speed (10/100/1000 Mbit/s) and duplex mode (half/full) to the best common mode when a physical link is established.

5.8 IP routing

The devices not only provide switch functionality but are also able to route data packages.

5.8.1 Static routing

Using static routing the devices can specify the next hop router to use to reach a given IP subnet, or add additional (directly attached) subnets to a local interface.

The example below shows a static route to the 192.168.11.0/24 subnet using 192.168.1.2 as gateway. A detailed description of all routing related SNMP commands can be found in cfgRouting.

Configuration File Example: Static route

```
# Config.Format = raw
WESTERMO-SW6-MIB::cfgRouteTableEnabled.0 = 1
WESTERMO-SW6-MIB::cfgRouteTableDestinationNetwork.0 = 192.168.11.0/24
WESTERMO-SW6-MIB::cfgRouteTableGateway.0 = 192.168.1.2
WESTERMO-SW6-MIB::cfgRouteTableSource.0 = 192.168.1.20
```

5.9 VLAN

The *Software 6* has built in capability for virtual LANs (VLAN). The devices can be easily integrated into existing network environments where VLANs are in use.

The VLAN configuration is located under cfgNetVlanTable.

5.9.1 Multi SSID and VLAN

The devices support multiple SSIDs one a single radio. It can broadcast up to eight wireless networks with different names (i.e SSIDs). When using Multi SSID, users could also assign different VLAN ID to different wireless network. This makes it possible to get a device work with switches which has VLAN assigned for different access level and authority.

In the following example the Ethernet interfaces (eth0 and eth1) are configured so that either eth0 or eth1 are physically connected, but not both at the same time. The device shall be accessible via Ethernet (eth0 or eth1) for administrative purposes.

The process of configuring VLANs to separate SSIDs and making these networks accessible via Ethernet is as follows:

1. Setup 1st Ethernet interface (eth0) in VLAN 8, 103 and 203 and add it to the bridge (br0)
2. Setup redundant 2nd Ethernet interface (eth1)
3. Setup WLAN physical interface: frequency, power etc.
4. Setup 1st WLAN interface (wlan0) in VLAN 103 and add it to the bridge (br0)
5. Setup 2nd WLAN interface (wlan1) in VLAN 203 and add it to the bridge (br0)
6. Setup Administrative VLAN (VID 8)
7. Setup IP for Administrative VLAN (VID 8)

An example configuration of this kind is shown in Figure 5.3 below.

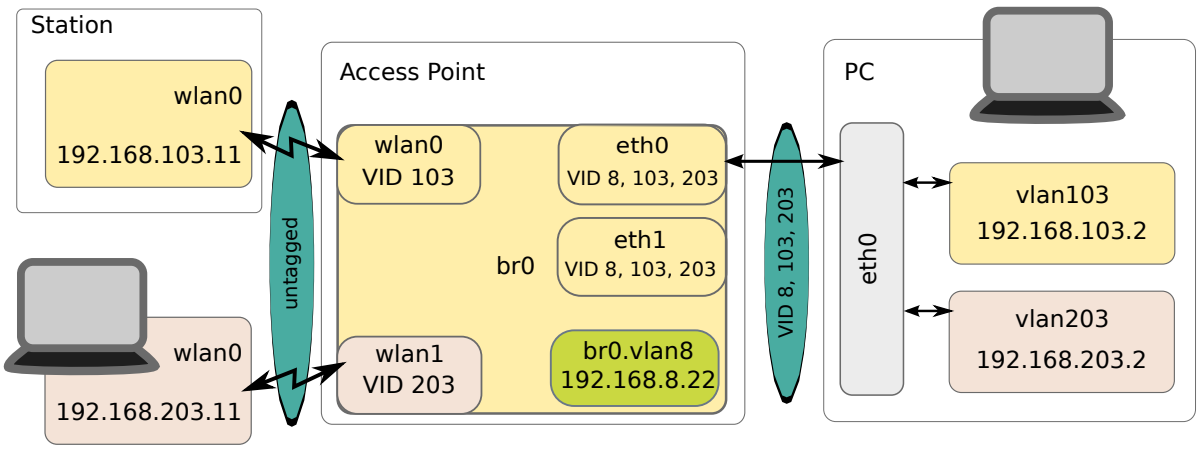


Figure 5.3: *Multi SSID and VLAN example setup*

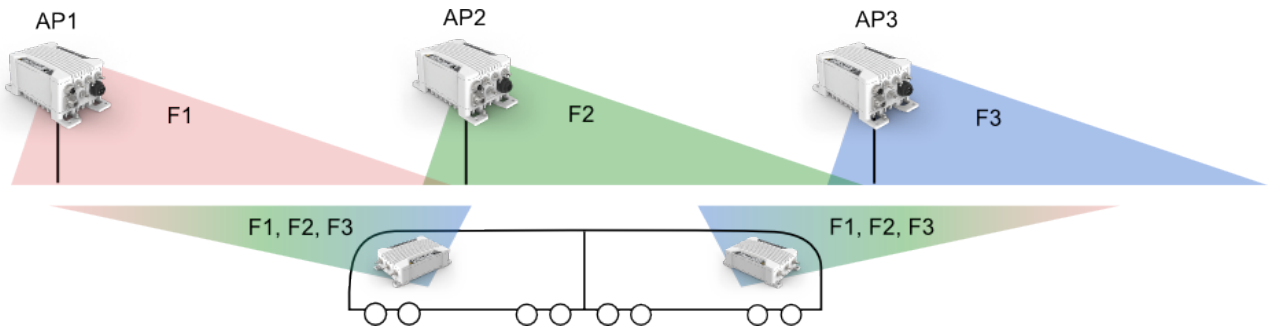
Configuration File Example: Multiple SSID and VLAN

```
# Config.Format = raw
# 1. Setup 1st ethernet interfaces(eth0):
WESTERMO-SW6-MIB::cfgNetEthTrunk.0 = 8,103,203
# 2. Setup 2nd (redundant) ethernet interface (eth1):
WESTERMO-SW6-MIB::cfgNetEthTrunk.1 = 8,103,203
# 4. Setup 1st WLAN interface (wlan0, VID 103):
WESTERMO-SW6-MIB::cfgNetWlanTag.0 = 103
WESTERMO-SW6-MIB::cfgNetWlanVlanMode.0 = 1
WESTERMO-SW6-MIB::cfgWlanIfaceSsid.0 = ssid103
# 5. Setup 2nd WLAN interface (wlan1, VID 203):
WESTERMO-SW6-MIB::cfgNetWlanEnabled.1 = 1
WESTERMO-SW6-MIB::cfgNetWlanBridge.1 = 0
WESTERMO-SW6-MIB::cfgNetWlanTag.1 = 203
WESTERMO-SW6-MIB::cfgNetWlanVlanMode.1 = 1
WESTERMO-SW6-MIB::cfgWlanIfaceDevice.1 = 0
WESTERMO-SW6-MIB::cfgWlanIfaceSsid.1 = ssid203
# 6. Setup Administrator VLAN (VID 8):
WESTERMO-SW6-MIB::cfgNetVlanVid.0 = 8
# 7. Setup IP for Administrative VLAN:
WESTERMO-SW6-MIB::cfgNetIpAddr.0 = 192.168.8.22/24
WESTERMO-SW6-MIB::cfgNetIpInterface.0 = br0.vlan8
```

5.10 Handoff and Mobility

5.10.1 Scan Handoff

The scan handoff is based on a wireless network operating in infrastructure mode. On trackside the modem is configured in Access Point mode where on train in STA (client/station) mode. Each Access Point is autonomously operating based on the configured operating channel where the Access Points can operate on different frequencies.



The mobility is based on the fast handoff and scanning capability of the client. The handoff process is as following:

1. RSSI handoff level defines the level when STA disconnects. The STA constantly observes the signal quality to the AP.

2. STA scans the configured scanning list and chooses the best AP. Please refer to Scan Channels to learn more on how to configure scan lists on STA

3. Connection to the AP is maintained as long as the handoff level is preserved

Handoff performance: 20..80ms depending on the number of channels to be scanned. To achieve maximum handoff performance please refer to handoff parameters in cfgWlanHandoffTable.

For debugging purposes and verification of the system setup it is very important to have the possibility to log signal levels and the handoff process. To serve these needs the STA provides several handoff debug flags (see cfgWlanDbgTable and setWlanDbgTable) which allows to log received RSSI for each beacon and handoff events in the syslog (see Logging Features).

5.10.2 Handoff level configuration

There are two important parameters which define the handoff:

1. Scanning Level cfgWlanHoScanningLevel

2. Recovery time cfgWlanHoRecovery

The following chapter assumes that is always in coverage of overlapping cells of Access Points with same SSID.

The scanning level parameter cfgWlanHoScanningLevel defines the level at which a station (STA) disconnects from an associated Access Point (AP) and proceeds for scanning a new Access Point (AP). The STA after scanning selects AP with the best RSSI. The level has to be selected so that the old AP has RSSI levels lower than potential new AP. Otherwise the STA will reconnect to the old one i.e. do self handoff. When using fixed rates it's important to make levels above sensitivity limits for desired data rate.

The Recovery time parameter cfgWlanHoRecovery is defining the time (ms) after a successful handoff during which no further handoff will be executed. It can be used in situations when RSSI is fluctuating around scan levels and would lead to several self-handoff. This parameter depends also on the speed of moving .

The handoff level parameter is connected to which is relative to the noise floor. The latter is fixed to -95dBm so even when it fluctuates due to environment, one can calculate absolute signal value, which aids planning. RSSI of 8 is then equal -95dBm + 8dB = 87dBm. From sensitivity point of view thist would mean that Modem is still able to maintain low modulation rates MCS 0-2.

For the optimal operation the handoff level must be set as follows:

- Set it to a level where the new Access Point signal is clearly better than the old one, otherwise a self handoff is performed
- Make the level planning (link budget calculations) of the installation so that the required communication speed is possible with the handoff level

5.10.2.1 Good handoff level and level planning

This is example of good handoff level and good level planning. The handoff is done with the RSSI values of approx. -70dBm, which allows the use of high modulation data rates throughout the handoff.

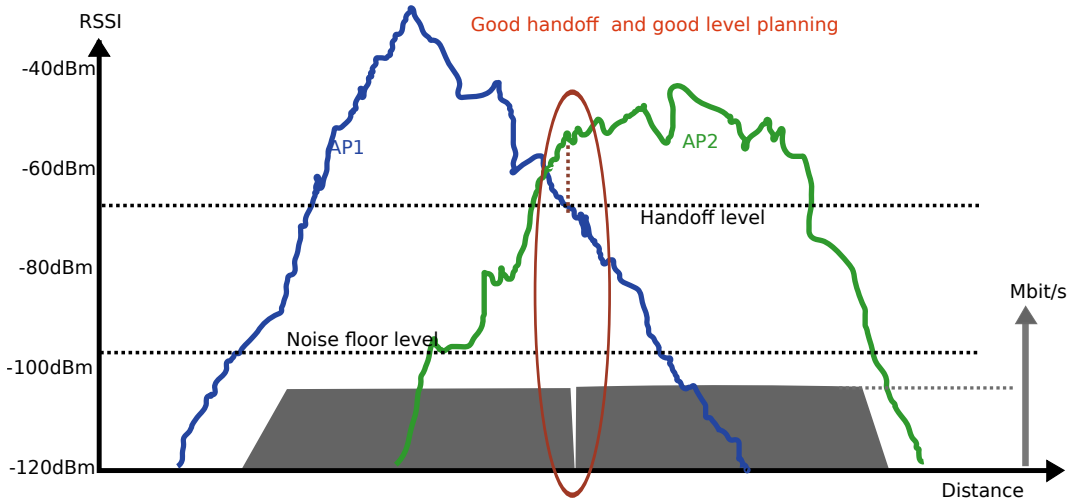


Figure 5.4: *Good handoff level and level planning*

5.10.2.2 Good Handoff level but not optimal level planning

The handoff level is ok and fast handoff is possible. However generally the RSSI levels are too low for high-speed traffic.

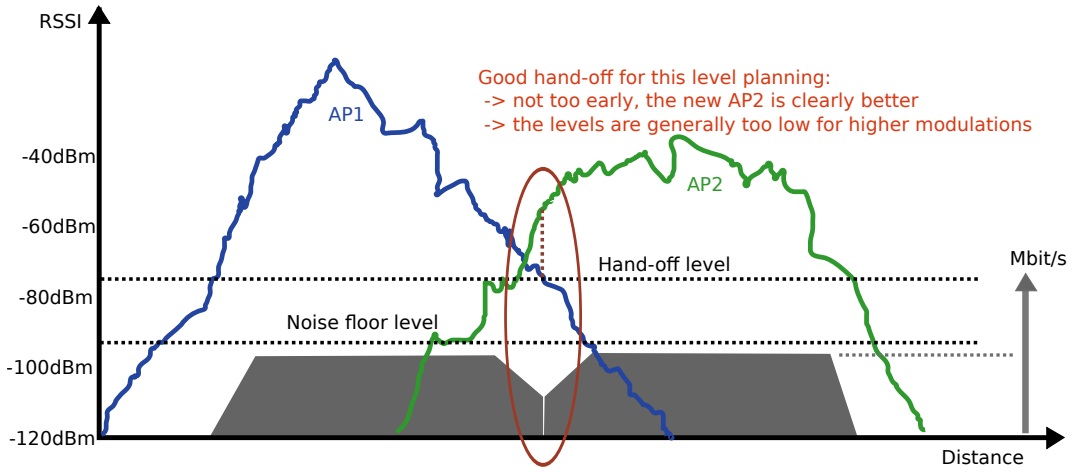


Figure 5.5: *Good handoff level but not optimal level planning*

5.10.2.3 Too high handoff level - self handoff

Here the handoff level is too high for the RSSI levels of AP1 and AP2. The Client will disassociate and re-associate to the AP1 constantly, until AP2 is stronger. The data throughput has gaps because of the self handoff, in order to have the self handoff less frequent one can increase the recovery time parameter.

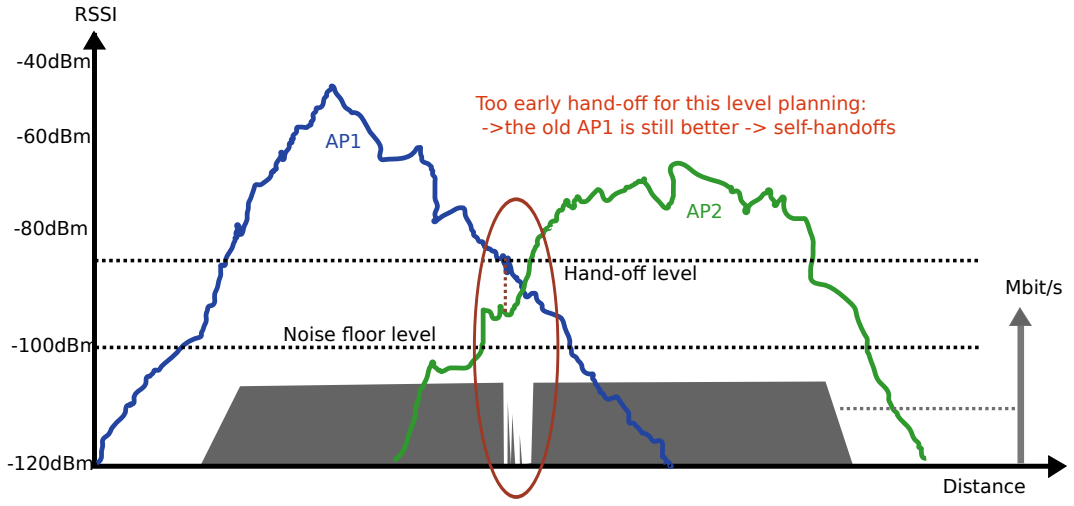


Figure 5.6: *Too high handoff level - self handoff*

5.10.2.4 Too low level planning

Here the level planning is too low (too close to the noise floor and sensitivity limits) to create a good handoff conditions. The low RSSI level of the AP and client is causing connection breaks, regardless

of the handoff level.

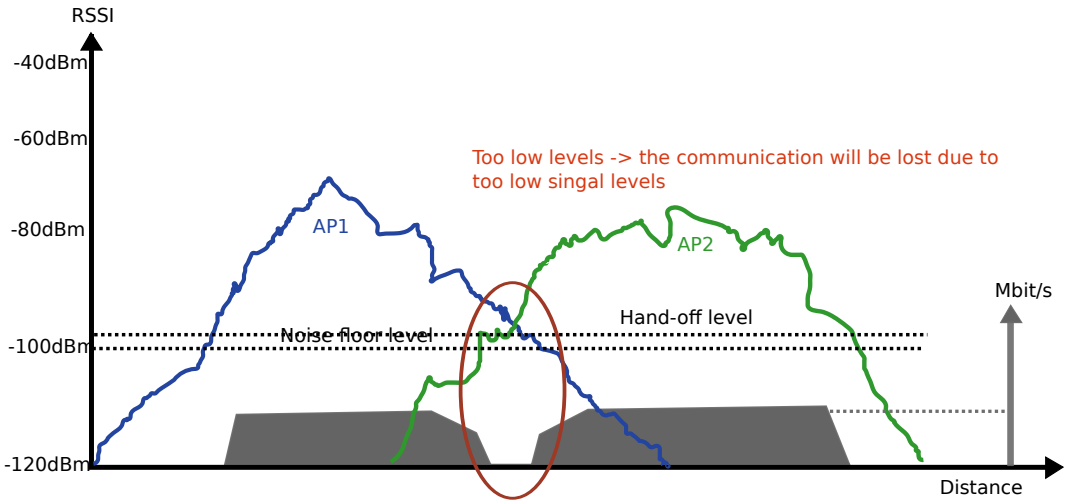


Figure 5.7: *Too low level planning*

5.10.3 Fast BSS Transition (802.11r)

IEEE 802.11r is an amendment to the IEEE 802.11 standard. Fast BSS transition (FT) (802.11r) allows continuous connectivity of wireless devices in motion with fast and secure handoff. It is working for wireless devices in the same Mobility Domain (MD).

If using 802.1X, 802.11r provides a fast and still secure handoff within an MD. Whereas if using 802.1X without 802.11r, the handoff is secure but not fast.

For a simple configuration of the R0- and R1-Key Holder List (R0KH-/R1KH-list), use wildcard entries as given in the following example configuration. The wildcard entry in the R0-KH-list means that all APs of the same MD are allowed as R0-Key Holder. And the wildcard entry in the R1-KH List means, that every AP of the same MD is allowed to request an R1-Key.

5.10.3.1 AP 802.11r configuration

When not using wildcard entries for R0KH-/R1KH-list, then each AP of an MD needs to have one entry for all of the other APs in the same MD. See cfgWlan802dot11rR0KHTable and cfgWlan802dot11rR1KHTable for some more description.

The following configuration example configures an AP for using FT, and using wildcard entry for R0- and R1-Key Holder List:

Configuration File Example: FT AP

```
# Config.Format = raw
# basic 802.11r configuration
WESTERMO-SW6-MIB::cfgWlan802dot11rEnabled.0 = 1
WESTERMO-SW6-MIB::cfgWlan802dot11rMobilityDomain.0 = a1b2
WESTERMO-SW6-MIB::cfgWlan802dot11rPmkR0Lifetime.0 = 10000),
WESTERMO-SW6-MIB::cfgWlan802dot11rPmkR1KeyHolderIdentifier.0 = 000102030405 # i.e. use
    ↪ own MAC
WESTERMO-SW6-MIB::cfgWlan802dot11rR0KHParameter.0 = 0
WESTERMO-SW6-MIB::cfgWlan802dot11rR1KHParameter.0 = 0
# 802.11r R0 key holder list wildcard entry
WESTERMO-SW6-MIB::cfgWlan802dot11rR0KHId.0 = 0
WESTERMO-SW6-MIB::cfgWlan802dot11rR0KHEnabled.0 = 1
WESTERMO-SW6-MIB::cfgWlan802dot11rR0KHDestinationMac.0 = ff:ff:ff:ff:ff:ff
WESTERMO-SW6-MIB::cfgWlan802dot11rR0KHHID.0 = *
WESTERMO-SW6-MIB::cfgWlan802dot11rR0KHKey.0 = 000102030405060708090a0b0c0d0e0f
# 802.11r R1 key holder list wildcard entry
WESTERMO-SW6-MIB::cfgWlan802dot11rR1KHId.0 = 0
WESTERMO-SW6-MIB::cfgWlan802dot11rR1KHEnabled.0 = 1
WESTERMO-SW6-MIB::cfgWlan802dot11rR1KHDestinationMac.0 = 00:00:00:00:00:00
WESTERMO-SW6-MIB::cfgWlan802dot11rR1KHHID.0 = 00:00:00:00:00:00
WESTERMO-SW6-MIB::cfgWlan802dot11rR1KHKey.0 = 000102030405060708090a0b0c0d0e0f
```

The 256-bit R0KH-key cfgWlan802dot11rR0KHKey (000102030405060708090a0b0c0d0e0f in the example above) must match the 256-bit R1KH-key cfgWlan802dot11rR1KHKey. Please use your own key here and not the one which is given here just as an example to demonstrate the format of such a key.

PMK-R0 Key Holder ID (cfgWlan802dot11rPmkR0KeyHolderIdentifier) is configurable via cfgWlan802dot1xNasId. See also 5.6.

5.10.3.2 STA (client/station) 802.11r configuration

The following configuration example configures a STA for using FT:

Configuration File Example: FT STA

```
# Config.Format = raw
WESTERMO-SW6-MIB::cfgWlanHoProfile.0 = 2 # t2gv2(2)
WESTERMO-SW6-MIB::cfgWlan802dot11rEnabled.0 = 1
```

5.11 Quality of Service (QoS)

The *Software 6* and devices supports Wireless Multimedia Extensions (WME) based on the IEEE 802.11e standard. WME provides basic Quality of service (QoS) features to IEEE 802.11 networks. The WME settings are configured on the Access Point only. Connecting clients are informed upon association what their QoS parameters are. Note that QoS/WME does not provide guaranteed throughput, but it is suitable for well defined applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones (VoWLAN).

The levels of priority in Enhanced Distributed Channel Access (EDCA) are called access categories (ACs). They are used by a WMM-enabled device to control the Arbitration Inter-Frame Space (AIFS), the Contention Window Minimum (CwMin), the Contention Windows Maximum (CwMax), and the Transmit Opportunity (TXOP).

The ACs can be set with cfgWlanWmeAc. The available ACs are:

- background (1)
- besteffort (2)
- video (3)
- voice (4)

A smaller AIFS increases probability of a frame getting a slot on the air to be transmitted. Higher prioritised queues should have smaller AIFS values.

The contention window (CW) can be set with cfgWlanWmeCwMin and cfgWlanWmeCwMax. It has a similar function as the AIFS value, but adds some randomness between CwMin and CwMax. Queues which are expected to transmit large amounts of traffic should have a wider window with higher values to allow more randomness. Similar, queues with fewer high prioritised traffic should have a small window with low values.

The Transmit opportunity specifies how long a given station is allowed to transmit when it has gained access to the medium.

The default values recommended by the WiFi-Alliance are:

AC	AIFS	CwMin	CwMax	TXOP
BK	7	4	10	0
BE	3	4	10	0
VI	2	3	4	94
VO	2	2	3	47

By default the *Software 6* maps the class selector of the DSCP field in the IP header to the AC classes according to the following table:

DSCP class selector	AC
0	BE
1	BK
2	BK
3	BE
4	VI
5	VI
6	VO
7	VO

The DSCP header consists of 6 bits. Only the upper most 3 bits, the class selector bits, are considered. The lower 3 bits, the drop probability bits, are ignored. Notice that the class selector 0, which is what most IP frames carry in their header without any configuration, maps to the Best Effort queue.

Mapping of the DSCP header to wireless queues is always performed even if a different priority is specified in the 802.1p part of an 802.1q VLAN header.

Non-IP frames with an 802.1q header, are mapped according to the following table:

802.1p	AC
0	BE
1	BK
2	BK
3	BE
4	VI
5	VI
6	VO
7	VO

Non-IP frames without an 802.1q header, are mapped to the Best Effort queue.

5.12 Service indicators and counters

5.12.1 SNMP trap daemon

The WLAN modem provides notifications by means of SNMP Traps.

In order to receive SNMP traps on a trap server the trap daemon of the WLAN modem must be enabled (cfgSnmpTrapEnabled) and the trap destination IP address (cfgSnmpTrapDest) must be set to the IP address of the trap server.

The SNMP traps are defined and described in the NERATEC-TRAP-MIB file, which is part of the delivered software package. The trap message string contains message codes in the form:

```
[ <prio> <code> ] <text message>
```

Please refer to chapter Message Codes for a complete list of all message codes.

5.12.2 Counters and Status

The WLAN modem provides status information and important counters defined and described by the WESTERMO-SW6-MIB.

The status information and counters are logically divided into

- **Hardware status and counters (hardware)** - such as product type, serial number, revision, etc
- **Software status and counters (software)** - such as firmware name, firmware revision, wireless counters etc

5.13 Logging Features

The *Software 6* supports extensive logging features. Logging is possible to local file or to a remote server (syslog).

Log levels can be read using cfgLogFileLevel and cfgLogRemoteLevel.

In order to enable/disable logging to local file use cfgLogFileEnabled.

For enabling/disabling remote server logging use cfgLogRemoteEnabled. IP address and port of remote syslog server can be configured using cfgLogRemoteIp and cfgLogRemotePort.

5.14 Inter-Carriage Link (ICL)

The Inter-Carriage Link application (ICL) offers a hands-off approach to connect and bridge carriage networks. Once ICL is enabled and operational on two carriages, the application will do the following:

- Broadcast availability to other ICL capable carriages while outside detection range.
- Automatically form a link on approach.
- Stay linked while the carriages are connected and providing the highest throughput possible.
- Cleanly disconnect on departure and switch back to broadcasting availability.

The ICL application removes the need for a cable connection and is designed to be low maintenance. Using the ICL algorithm combined with suitable antennas ensures proper linking of carriages.

All DT5xxx devices support the Inter-Carriage Link application.

5.14.1 Configuration of the Inter-Carriage Link Application

The ICL application supports two configuration modes:

- A WebGUI as a configuration wizard.
- Configuration through SNMP for full customisation.

5.14.1.1 Configuration with the WebGUI

After logging in (See Web-Based Management how to access), the *Inter-Carriage Link* application is available in the *Applications* menu.

The first step to activate the application is to enable it. Go to *Application -> Inter-Carriage Link -> Configuration*.

You should see a page like the screenshot in figure 5.8.

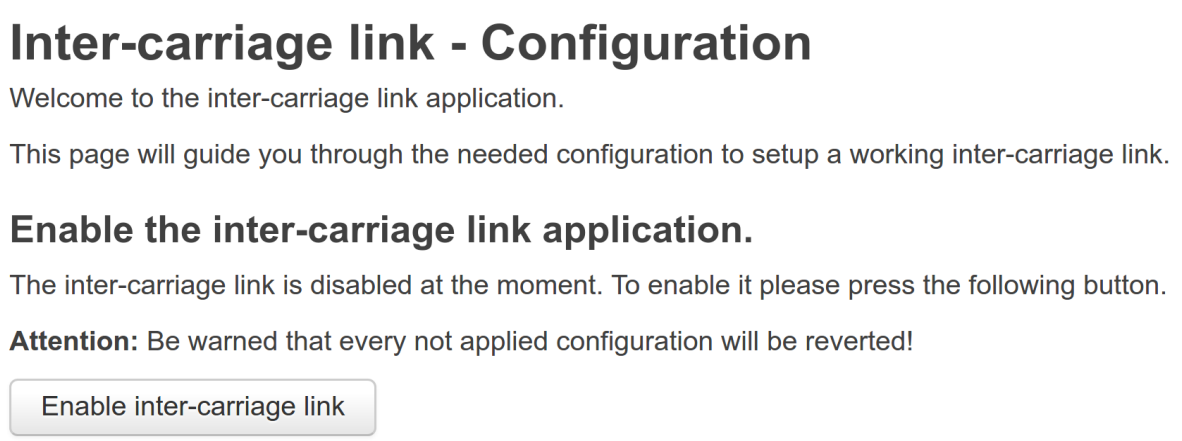


Figure 5.8: *Enable page*

By pressing the enable button the WebGUI wizard will change a number of settings for you. The wizard operates under the assumption that ETH1 is your management interface and ETH2 is your bridge or cable replacement interface. You will be able to adjust various parameters before starting the ICL application.

Once enabled, you will be redirected to the configuration page as shown in figure 5.9 where you will be able to customise a list of settings.

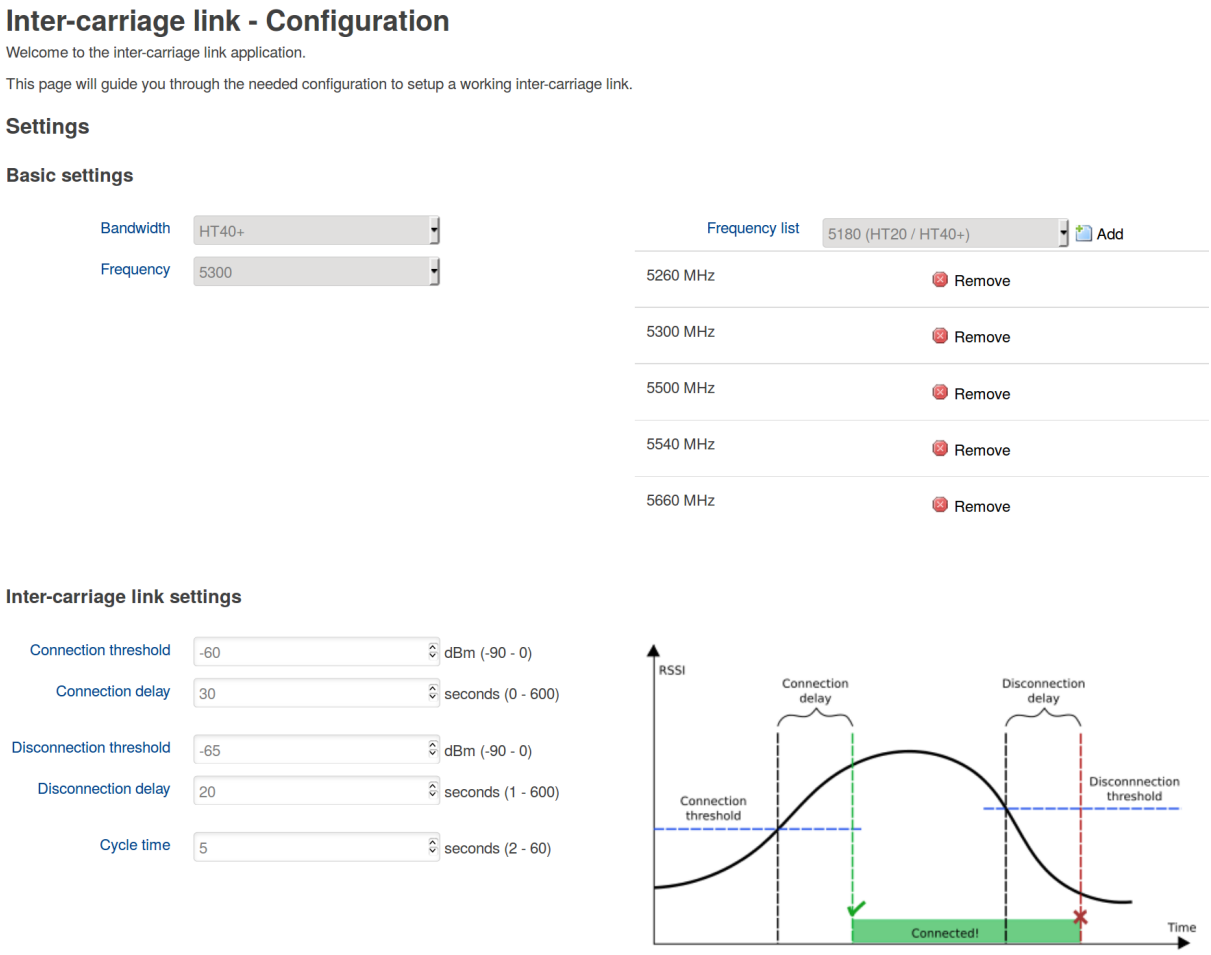


Figure 5.9: *Configuration page*

Bandwidth defines the preferred bandwidth. Options are HT20, HT40+ or HT40-. For more details, see cfgWlanDevBandwidth.

Frequency defines the primary operating frequency and depends on the selected bandwidth. See cfgWlanDevFrequency for more details.

Frequency list contains all frequencies that will be scanned by the Inter-Carriage Link application. It also functions as a list of backup frequencies in case radar is detected on the current operating frequency. This list should include its own frequency the device operates on. Corresponding MIB entries are cfgWlanFFreq0 to cfgWlanFFreq23.

Connection threshold describes the minimum signal level a potential ICL partner needs to reach before it is considered a valid ICL partner. A higher value means the signal needs to be stronger and therefore a potential partner needs to be closer. cfgIclConnectionThreshold is the associated MIB entry.

Connection delay defines how long the Inter-Carriage Link algorithm should evaluate a potential ICL partner. If the connection delay is set to 0 the ICL algorithm will instantly connect to the

very first potential partner circumventing most of the evaluation of the ICL algorithm. See cfgIclConnectionDelay for more details.

Disconnection threshold sets the signal level at which the link disconnection process will be started. For more details, see cfgIclDisconnectionThreshold.

Disconnection delay defines how long the device should wait before scanning for a new partner once the old partner disconnected. It also defines how long a formerly connected partner tries to reconnect if the link is lost for any reason. cfgIclDisconnectionDelay is the corresponding MIB entry.

Cycle time sets the scan interval. Ideally the connection delay time is at least five times the cycle time to allow the ICL algorithm to properly evaluate a candidate. See cfgIclCycleTime for more details. Also consider the size of the Frequency list. A larger list requires more time spend scanning, thus the Cycle time should not be selected too short.

To start the Inter-Carriage Link application press *Apply*. If the application was already running, *Apply* will restart the service with the changed configuration.

Note Configuration with SNMP offers full customisation should the WebGUI not satisfy your configuration needs.

The status page as in figures 5.10, 5.11 and 5.12 shows all important status information regarding the Inter-Carriage Link. This page will automatically refresh every two seconds to keep the status up-to-date.

Figure 5.10: *Status page: Scanning for an ICL partner*

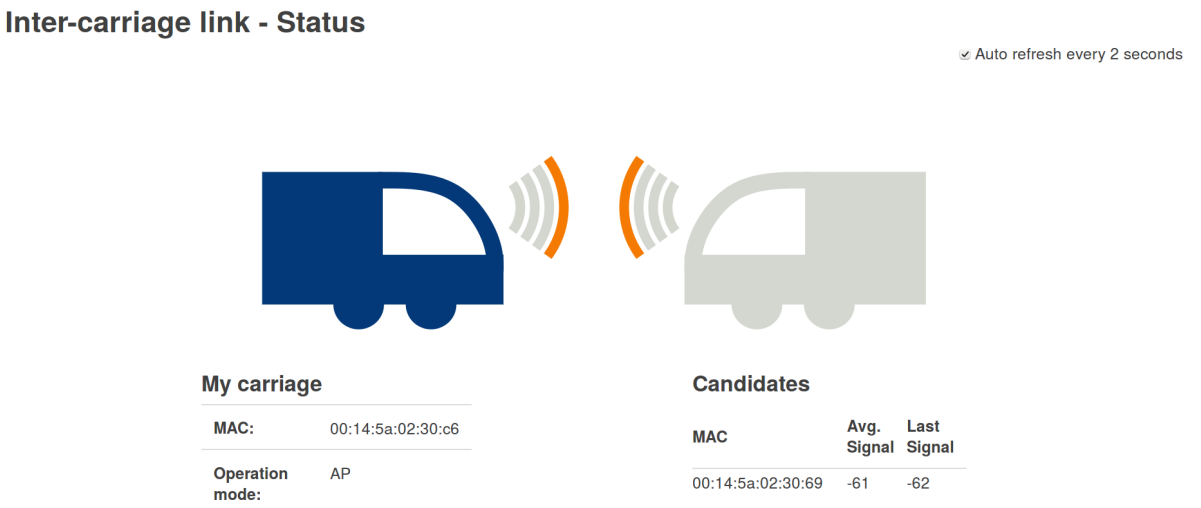


Figure 5.11: *Status page: Evaluating one or more ICL partners*

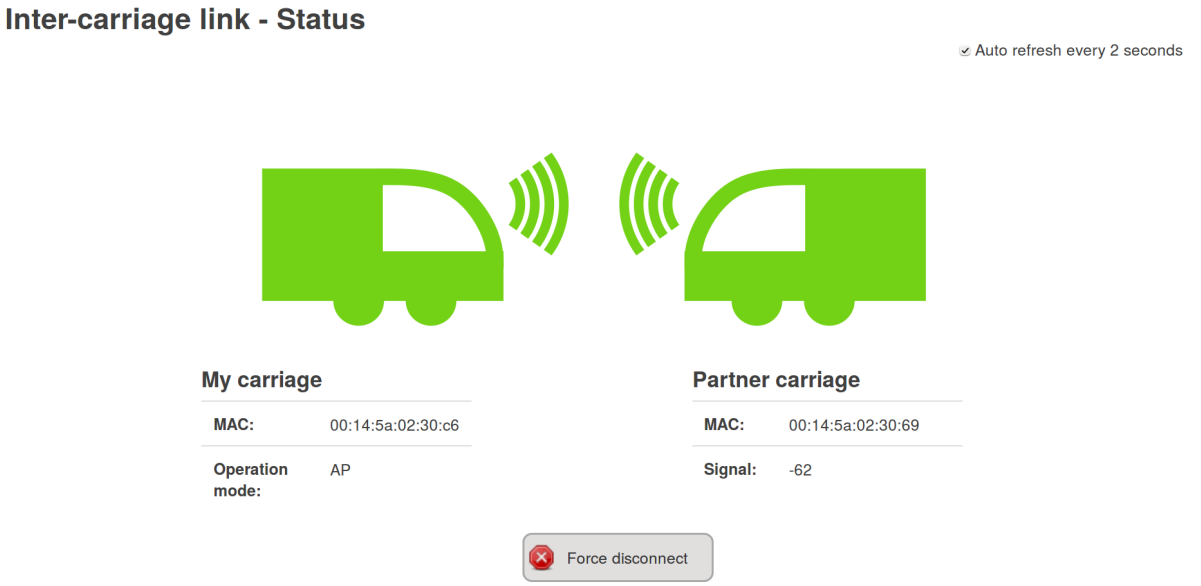


Figure 5.12: *Status page: Link established*

In the unlikely case the displayed connection is not the desired connection, the link can be dropped using the *Force disconnect* button. The current ICL partner will then be added to a blacklist to prevent reconnecting to the same device for the next ten minutes.

5.15 Wireless Manager (NWM)

The Wireless Manager (NWM) offers advanced features for wireless access point operation

- Usable frequency list to support advanced frequency planning
- Background channel availability check (CAC) for DFS channel to support seamless operation in case of radar detection
- Available channel list in non-volatile memory for fast recovery after reboot
- Interference reports

The Wireless Manager (NWM) is only available on RT-370 devices since it requires two radios.

The first radio (antenna ports A1 and A2) is the so called communication interface providing the AP functionality. The second radio (antenna port A3) is responsible to make Channel Availability Checks on channels which are not yet available. During periods where no further CACs are required, the second radio can be used to do scan the environment for interferences as described in section 5.16

Antenna port A3 is used for CAC and Off-Channel-CAC. Therefore you need to assert that you have an antenna connected at antenna port A3.

The NWM can store the list of available DFS channels in a non-volatile memory. Thus, when the channel is once marked as available it will be instantly available after a device reboot. When the non-volatile memory option is enabled (see cfgChMgrDfsUseNvram), an Operator is responsible to reset the list of available DFS channel by setting rpcNvramFreqStatesReset.0 to zero at installation or re-installation of the device.

The NWM depends on following sub-features:

- Channel Manager: The Channel Manager is responsible to perform CACs on usable DFS channels. Its goal is to make all DFS channels available. Further, it proposes the wireless channel to be used by the NWM.
- Scan Worker: The Scan Worker manages the second radio of the RT-370 device. On request it performs scan work jobs like CAC or wireless interference scans. The Channel Manager makes use of the Scan Worker to do the CACs on DFS channels.

5.15.1 Configuration with the WebGUI

The *Wireless Manager* can be configured with the WebGUI (See Web-Based Management how to access).

The NWM is a so called application. You will find it in the *Applications* menu.

The first step to activate the application is to enable it. Go to *Application -> Wireless Manager -> Configuration*.

You should see a page like the screenshot in figure 5.13.

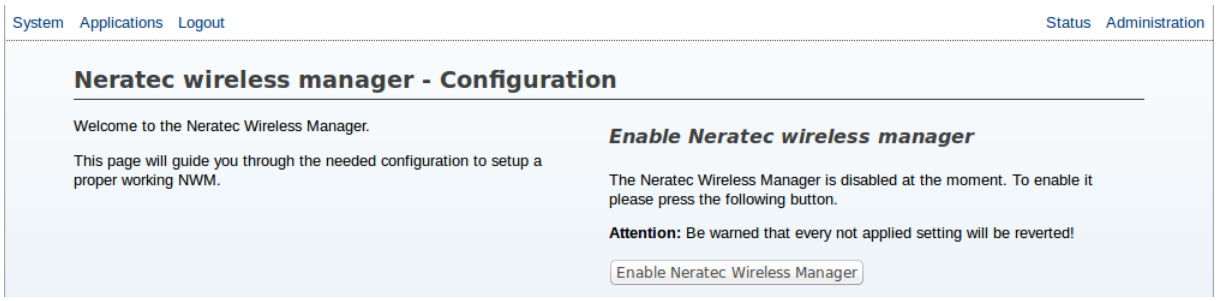


Figure 5.13: *Enable page*

By pressing the enable button the following settings will be changed and the NWM started.

Setting	Value
cfgNwmEnabled.0	1
cfgScnWrkEnabled.0	1
cfgChMgrEnabled.0	1
cfgWlanDevModulation.0	12
cfgWlanDevFrequency.0	5260
cfgWlanDevBandwidth.0	0
cfgWlanIfaceScanList.0	0
cfgNetWlanEnabled.0	1
cfgNetWlanEnabled.1	1
cfgWlanIfaceMode.1	2
cfgChMgrUsableFrequencyList.0	0
cfgWlanFFreq0.0	5260
cfgWlanFFreq1.0	5280
cfgWlanFFreq2.0	5300
cfgWlanFFreq3.0	5320
cfgWlanFFreq4.0	5500
cfgWlanFFreq5.0	5520
cfgWlanFFreq6.0	5540
cfgWlanFFreq7.0	5560
cfgWlanFFreq8.0	5580
cfgWlanFFreq9.0	5660
cfgWlanFFreq10.0	5700

Table 5.1: *Default values for the NWM*

It takes some time to enable the NWM. If the NWM could be successfully started, the configuration page as in figure 5.14 should be shown.

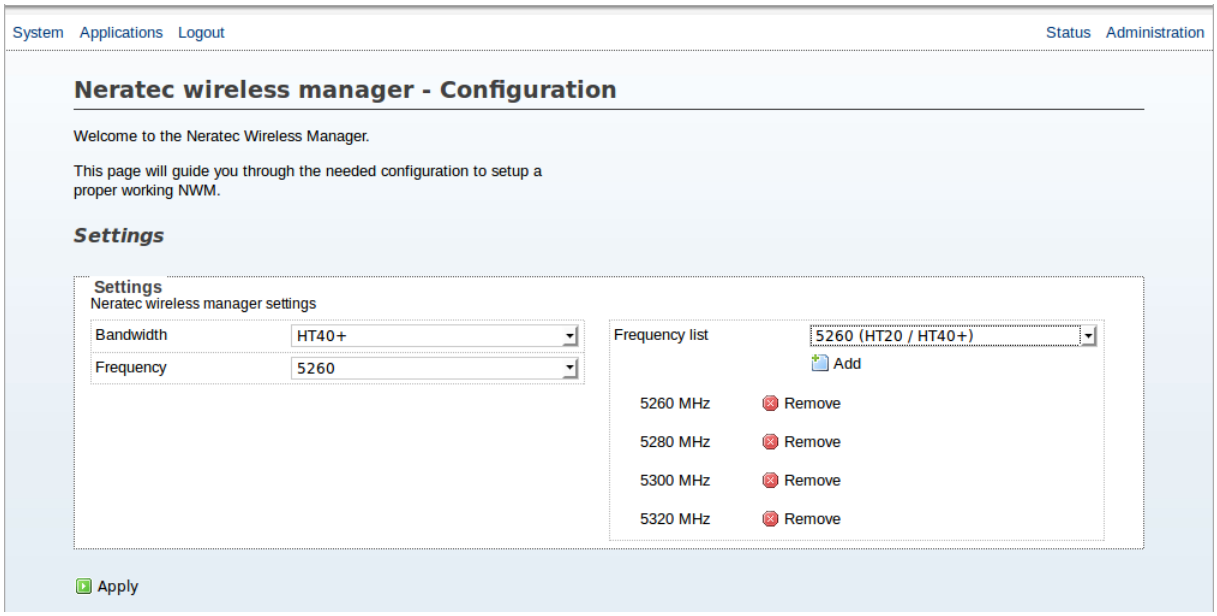


Figure 5.14: *Configuration page*

Bandwidth This define the prefered bandwidth. You can choose HT20, HT40+ or HT40-.

Frequency This define the prefered frequency to use. This depend on the selected bandwidth.

Frequency list The frequencies in this list are used as avoiding-possibility if a radar was detected on your prefered frequency.
In HT40+/HT40- you should always add the frequency and the extended frequency: For HT40+, 5300MHz you should add 5300MHz and 5320MHz.

Attention: If the frequency list is empty, all available frequencies will be used. The available frequencies depend on your country code.

To change the configuration and restart the services press *Apply*.

The status page as in figure 5.15 shows all important status informations about the NWM. The page will be automatically refreshed so you will always see the actual status.

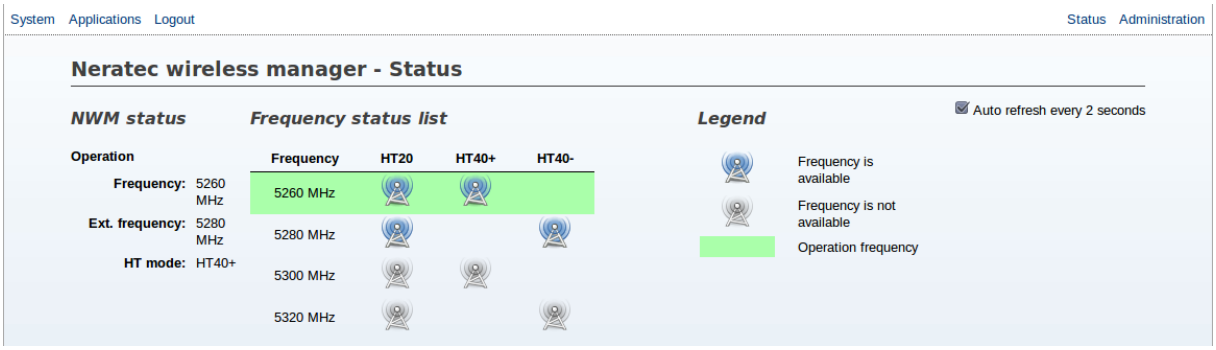


Figure 5.15: *Status page*

5.15.2 Configuration through SNMP

To use the NWM feature, you have to enable and configure all the sub-features.

5.15.2.1 Enable sub-features Scan Worker, Channel Manager and NWM

- Set cfgScnWrkEnabled.0 to enabled(1)
- Set cfgChMgrEnabled.0 to enabled(1)
- Set cfgNwmEnabled.0 to enabled(1)

5.15.2.2 Configure sub-features

Configure usable (Operational Frequency Plan) frequency lists:

- Set cfgChMgrUsableFrequencyList.0 to 1 (pointing to frequency list 1, see Frequency lists)

The NWM supports HT20 and HT40 channels. Define prefered channel for HT20:

1. Set cfgWlanDevModulation.0 to INTEGER: na(12) (i.e. wireless mode 11na (5GHz))
2. Set cfgWlanDevFrequency.0 to 5500 (i.e. using 5500 as starting operation frequency)

or define prefered channel for HT40:

1. Set cfgWlanDevModulation.0 to INTEGER: na(12) (i.e. wireless mode 11na (5GHz))

2. Set cfgWlanDevFrequency.0 to 5500 (i.e. using 5500 as starting operation frequency)
3. Set cfgWlanDevBandwidth.0 to 1 (i.e. using HT40+)

Configure first WLAN interface (Access Point Mode):

- Set cfgWlanIfaceMode.0 to INTEGER: ap(0) (i.e. Access Point Mode)
- Set cfgWlanIfaceScanList.0 to INTEGER: 1 (i.e. use frequency list 1, see Frequency lists)
- Set cfgNetWlanEnabled.0 to INTEGER: enabled(1) (i.e. enable wlan0 interface)

Configure second WLAN interface (Monitor Mode):

- Set cfgWlanIfaceMode.1 to INTEGER: monitor(2) (i.e. Monitor Mode)
- Set cfgNetWlanEnabled.1 to INTEGER: enabled(1)

As the last step the new configuration has to be applied:

- Set rpcCfgApply.1 to INTEGER: all(1)

5.15.2.3 Frequency lists

If needed it is possible to change the default frequency lists; or add an additional frequency list.

Up to 24 frequency lists can be defined. Where each frequency list defines exactly 24 channels.

Setting the frequency to 0 denotes an unused frequency in a frequency list. I.e. if you need a frequency list with just one frequency, set freq0 to the needed frequency (e.g. 5300), and the remaining non used frequencies must be set to 0.

As default, 2 frequency lists are defined. Frequency list 0 defines 2.4 GHz channels (no DFS), frequency list 1 defines 5GHz channels.

If a list is empty and this list is set for cfgWlanIfaceScanList, all available frequencies will be used. The available frequencies depend on your country code.

Example of a frequency list 1:

1. Set cfgWlanFFreq0.1 = INTEGER: 5180
2. Set cfgWlanFFreq1.1 = INTEGER: 5200
3. Set cfgWlanFFreq2.1 = INTEGER: 5220

4. Set cfgWlanFFreq3.1 = INTEGER: 5240
5. Set cfgWlanFFreq4.1 = INTEGER: 5260
6. Set cfgWlanFFreq5.1 = INTEGER: 5280
7. Set cfgWlanFFreq6.1 = INTEGER: 5300
8. Set cfgWlanFFreq7.1 = INTEGER: 5320
9. Set cfgWlanFFreq8.1 = INTEGER: 5500
10. Set cfgWlanFFreq9.1 = INTEGER: 5520
11. Set cfgWlanFFreq10.1 = INTEGER: 5540
12. Set cfgWlanFFreq11.1 = INTEGER: 5560
13. Set cfgWlanFFreq12.1 = INTEGER: 5580
14. Set cfgWlanFFreq13.1 = INTEGER: 5660
15. Set cfgWlanFFreq14.1 = INTEGER: 5680
16. Set cfgWlanFFreq15.1 = INTEGER: 5700
17. Set cfgWlanFFreq16.1 = INTEGER: 0
18. Set cfgWlanFFreq17.1 = INTEGER: 0
19. Set cfgWlanFFreq18.1 = INTEGER: 0
20. Set cfgWlanFFreq19.1 = INTEGER: 0
21. Set cfgWlanFFreq20.1 = INTEGER: 0
22. Set cfgWlanFFreq21.1 = INTEGER: 0
23. Set cfgWlanFFreq22.1 = INTEGER: 0
24. Set cfgWlanFFreq23.1 = INTEGER: 0

To ease the configuration of DFS, Westermo Teleindustri ABcan provide a sample configuration file which can easily be imported (through Web- or SNMP-interface).

5.16 Interference Detection Function (IDF)

Each wireless device (AP and STA) has the functionality to analyze the operation frequency in use. Those values can be read out at any time on any device via SNMP.

In RT-370 products, the IDF functionality supports JSON reports which can be sent to a configured URL (cfgHttpRprtServerUrl) at a configured interval (cfgIdfInterval).

IDF is (currently) only available on RT-370 devices since it uses the second radio (i.e. wlan1) interface.

Please note that the second radio is also used for DFS as described in section 5.15

Basic IDF configuration:

- Set cfgIdfEnabled.0 to INTEGER: enabled(1)
- Set cfgHttpRprtServerUrl.0 to STRING: http://192.168.1.1:8000/json
- Set cfgScnWrkEnabled.0 to INTEGER: enabled(1) (i.e. enable Scan Worker, IDF depends on Scan Worker)

Configure second WLAN interface (Monitor Mode):

- Set cfgWlanIfaceMode.1 to INTEGER: monitor(2) (i.e. Monitor Mode)
- Set cfgNetWlanEnabled.1 to INTEGER: enabled(1)

Example IDF task configuration (scan frequency 5500, wifi data collection):

- Set cfgIdfScanWorkFreq.0 to INTEGER: 5500
- Set cfgIdfScanWorkAction.0 to INTEGER: wifi(4)
- Set cfgIdfScanWorkSeconds.0 to INTEGER: 1

All actions according to the IDF task list (cfgIdfScanWorkTable) are processed sequentially. The whole process is repeated endlessly. The time per action can be configured (cfgIdfScanWorkSeconds) in seconds.

For a complete list of IDF configuration elements see also cfgIdf.

5.17 Http Report

The HTTP Report interface is used by several services and provides a simple way of status reporting to a standard HTTP server.

- Protocol: HTTP POST
- Content-type: application/json
- Servers URL: Can be configured by cfgHttpRprtServerUrl

5.17.1 NWM and ChannelManager Report

For more information about the current status of the NWM and the Channel Manager (see section 5.15) it is possible to request HTTP reports via SNMP.

Nwm 'status' report: Set rpcNwmHttpReport.0 to 1

```
{
  "report": "NwmStatus",
  "epoch": 1436275841,
  "data": {
    "name": "Nwm",
    "nominal_freq": { "freq": 5300, "ext_freq": 5320, "htmode": 1 },
    "opfreq": { "freq": 5300, "ext_freq": 5320, "htmode": 1 }
  }
}
```

Nwm 'frequency state' report: Set rpcNwmHttpReport.0 to 2

```
{
  "report": "NwmFreqState",
  "epoch": 1436277622,
  "data": {
    "name": "Nwm",
    "freq_state_list": [
      [ 5180, 1 ],
      [ 5200, 1 ],
      [ 5220, 1 ],
      [ 5240, 1 ],
      [ 5260, 1 ],
      [ 5280, 1 ],
      [ 5300, 1 ],
      [ 5320, 1 ]
```

```
    ]
  }
}
```

Channel Manager 'frequency state' report: Set rpcChMgrHttpReport.0 to 1

```
{
  "report": "ChMgrFreqState",
  "epoch": 1436277622,
  "data": {
    "freq_state_list": [
      [ 5180, 1 ],
      [ 5200, 1 ],
      [ 5220, 1 ],
      [ 5240, 1 ],
      [ 5260, 1 ],
      [ 5280, 1 ],
      [ 5300, 1 ],
      [ 5320, 1 ]
    ]
  }
}
```

Channel Manager 'channels' report: Set rpcChMgrHttpReport.0 to 2

```
{
  "report": "ChMgrChannels",
  "epoch": 1436277864,
  "data": {
    "chan_nom": { "freq": 5300, "ext_freq": 5320, "htmode": 1 },
    "proposed_chan": { "freq": 5300, "ext_freq": 5320, "htmode": 1 },
    "chans_ht20": {
      "all": [ 5180, 5200, 5220, 5240, 5260, 5280, 5300, 5320 ],
      "available": [ 5180, 5200, 5220, 5240, 5260, 5280, 5300, 5320 ],
      "htmode": 0
    },
    "chans_ht40m": {
      "all": [ 5200, 5240, 5280, 5320 ],
      "available": [ 5200, 5240, 5280, 5320 ],
      "htmode": 2
    },
    "chans_ht40p": {
      "all": [ 5180, 5220, 5260, 5300 ],
      "available": [ 5180, 5220, 5260, 5300 ],
      "htmode": 1
    }
  }
```

```
}
```

5.17.2 IDF Report

An IDF report contains the scan results of all results available in the scan result buffer at the end of the cfgIdfInterval (i.e. at the time the IDF report is sent).

Please refer to section 5.16 for more information on how to configure the IDF

Elements of the IDF Report are:

- data.wlan_stats will only be present if cfgIdfScanWorkAction = wifi(4)
- data.wlan_stats.domest_fstats, data.wlan_stats.alien_fstats and data.wlan_stats.alien_mac might not be sent in each report
- data.radar_reports will only be present if cfgIdfScanWorkAction = radar(3)
- data.spectral_reports will only be present if cfgIdfScanWorkAction = spectral(2)

General elements of the IDF Report wlan_stats element are:

- epoch: UNIX time stamp
- freq: frequency in MHz
- bandwidth: bandwidth in MHz
- window_time: window time in milliseconds
- busy_time: busy time value in milliseconds
- rx_time: rx time value in milliseconds
- tx_time: tx time value in milliseconds

Elements of the IDF Report data.wlan_stats.domest_fstats and data.wlan_stats.alien_fstats element are:

- frame_cnt: frame counter
- frame_size: minimum, average and maximum frame length counter

- frame_total: bytes counter
- rssi: minimum, average and maximum frame RSSI

Elements of the IDF Report data.wlan_stats.alien_mac (list of alien MAC addresses found) element are:

- mac: MAC address
- frame_total: frame counter
- rssi_max: maximum frame RSSI
- rssi_avg: average frame RSSI

Elements of an IDF Report radar_reports element are:

- epoch: UNIX time stamp
- freq: Frequency in MHz
- radar_detected: radar counter
- seconds: observation time

Elements of an IDF Report spectral_reports element are:

- epoch: UNIX time stamp
- freq: Frequency in MHz
- num_samples: Number of FFT data processed
- seconds: observation time
- stats: minimum, average and maximum (all in dBm) of bin0, bin1, bin3, ..., bin55

Example of an IDF Report:

```
{
  "report": "IDF",
  "epoch": 1418301089,
  "data": {
    "name": "IDF",
    "wlan_stats" : [
      {
```

```
      "epoch" : 1315522477,
      "freq" : 5500,
      "bandwidth" : 20,
      "window_time" : 60,
      "busy_time" : 15,
      "rx_time" : 12,
      "tx_time" : 0,
      "domest_fstats" : {
        "frame_cnt" : 100,
        "frame_size" : [100, 200, 300],
        "frame_total" : 20153,
        "rssi" : [ 35, 45, 50 ]
      },
      "alien_fstats" : {
        "frame_cnt" : 10,
        "frame_size" : [ 50, 300, 500 ],
        "frame_total" : 4598,
        "rssi" : [ 15, 35, 50 ]
      },
      "alien_mac" : [
        {
          "mac" : "00:00:00:00:00:01",
          "frame_total" : 2856,
          "rssi_max" : 50,
          "rssi_avg" : 50
        }
      ]
    }
  ],
  "radar_reports": [
    {
      "epoch": 1315528096,
      "freq": 5700,
      "radar_detected": 2,
      "seconds": 60
    }
  ],
  "spectral_reports": [
    {
      "epoch": 1315522405,
      "freq": 5500,
      "num_samples": 14438,
      "seconds": 60,
      "stats": [
        [-159, -107, -91],
        [-154, -106, -92],
        [-157, -106, -91],
```

```
          ..
          [-157, -107, -92]
        ]
      }
    ]
  }
}
```

5.18 Firewall

The *Software 6* uses the well known *netfilter* to filter or mangle network traffic. The configuration is done by the *iptables* application. Most terms are based on these software components.

To use the firewall it has to be enabled. Otherwise no feature described below will work. To enable the feature the cfgFwEnabled flag has to be enabled.

In the following sections you can define multiple rules. Please keep in mind that the order of the rules is important! This means the rule with the index 2 will be processed before the rule with the index 3.

5.18.1 Port forward

Port forwarding can be used to forward network traffic to another destination. This is also know as *Destination Network Address Translation (DNAT)*.

To illustrate how to configure the port forward, we setup a port forward to a web server and a database server which are common use cases. The goal is to connect from Radio Modem 1 (RM1), through the wireless link to RM2, to the web server or the database server.

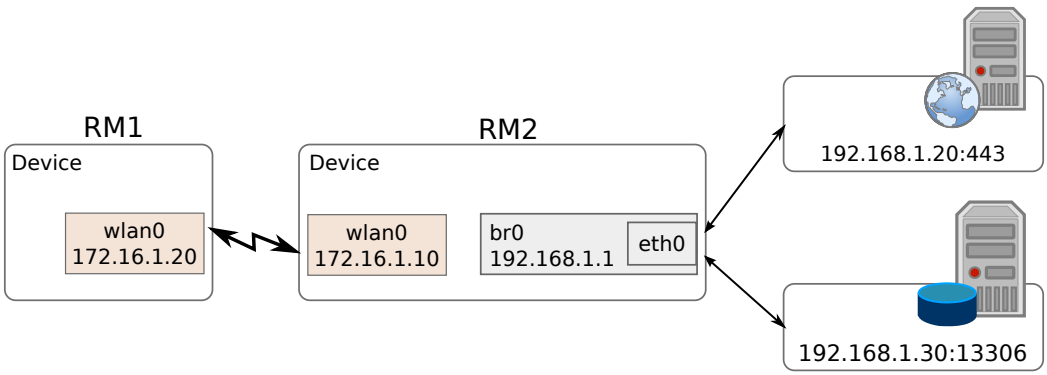


Figure 5.16: *Port forward to servers behind an device*

To forward the network traffic to the web server and the database server we add two new *rules* to the port forward rules table:

1. For the web server we only want to forward tcp traffic to port 443.

2. For the database server we want to forward tcp and udp traffic for the port range 2000 - 2100 to illustrate port ranges. In addition we want to accept traffic to the wlan from anywhere.

Configuration File Example: Port forward

```
# Config.Format = raw
WESTERMO-SW6-FIREWALL-MIB::cfgFwEnabled.0 = 1
# Port forward to the web server
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdEnabled.0 = 1
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdInterface.0 = wlan0
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdProtocol.0 = 2
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdDestinationAddress.0 = 172.16.1.0/24
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdDestinationPortStart.0 = 443
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdDestinationPortEnd.0 = -1
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdRedirectDestinationAddress.0 = 192.168.1.20
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdRedirectDestinationPort.0 = 443
# Port forward to the database server
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdEnabled.1 = 1
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdInterface.1 = wlan0
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdProtocol.1 = 3
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdDestinationAddress.1 = 0.0.0.0/0
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdDestinationPortStart.1 = 2000
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdDestinationPortEnd.1 = 2100
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdRedirectDestinationAddress.1 = 192.168.1.20
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdRedirectDestinationPort.1 = 13306
```

5.18.2 Outbound NAT

With the outbound NAT the device can control how traffic leaving the device will be translated. It's also known as Source NAT (SNAT) and used in the most home routers to rewrite the source address to the address of the WAN interface of the router so the traffic finds the way back home.

The SNAT can be done by simple masquerade, means take the address of the network interface or by defining the source address/port.

As for the port forward we use a simple example to illustrate the functionality as shown in Figure 5.17. The goal is to connect from a Laptop, through RM1 to the web interface of RM2. For this example the Laptop use RM1 as default gateway and the wlan0 interface of RM1 has a dynamic address.

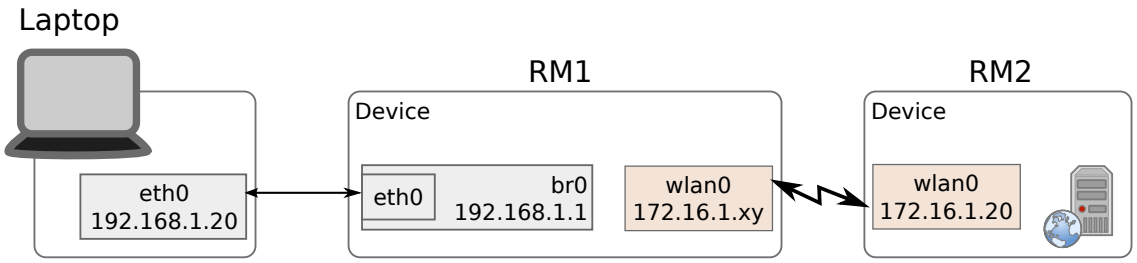


Figure 5.17: *Example for outbound NAT on a device*

At this point we will only describe the steps to configure the outbound NAT. Following example enables the first rule, set the output interface to *wlan0* and applies to TCP traffic only.

Configuration File Example: Outbound NAT

```
# Config.Format = raw
WESTERMO-SW6-FIREWALL-MIB::cfgFwEnabled.0 = 1
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatOutEnabled.0 = 1
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatOutInterface.0 = wlan0
WESTERMO-SW6-FIREWALL-MIB::cfgFwNatPrtFwdProtocol.0 = 2
```

With this configuration you should be able to connect from the laptop to 172.16.1.20, to the web interface of RM2.

For all possible configurations please see firewall in the MIB reference.

6 Default values

The following table shows all configuration parameter and there status if supported or not supported by software 6.8.3. Additionally the default values are shown.

Network Settings:

cfgNetIpAddr	192.168.1.20/24
cfgNetIpProto	static(0)
cfgNetIpInterface	br0.vlan0
cfgNetEthBridge	br0(0)
cfgNetWlanBridge	br0(0)
cfgNetVlanBridge	br0(0)
cfgNetVlanVid	0

WLAN physical device Settings:

cfgWlanDevModulation	ng(10)
cfgWlanDevBandwidth	HT20(0)
cfgWlanDevFrequency	2412
cfgWlanDevPower	9
cfgWlanDevTxAntenna	3 (011)
cfgWlanDevRxAntenna	3 (011)

WLAN logical interface Settings:

cfgWlanIfaceMode	AP(0)
cfgWlanIfaceSsid	Rmodem1
cfgWlanIfaceEncryption	WPA2(3)
cfgWlanIfacePassword	password
cfgWlanIfaceBitrates	Auto(-1)
cfgWlanIfaceScanList	0

Routing settings:

cfgRouteDefGateway	0.0.0.0 (disabled)

7 WESTERMO-SW6-MIB

7.0.1 configuration

7.0.1.1 cfgSystem

7.0.1.1.1 cfgSysHostname

The hostname of the device.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.1.1

7.0.1.1.2 cfgSysTimezone

POSIX timezone string.

For more strings also see http://wiki.openwrt.org/doc/uci/system#time_zones

Example

Europe/Zurich: CET-1CEST,M3.5.0,M10.5.0/3

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.1.2

7.0.1.2 cfgSsh

7.0.1.2.1 cfgSshEnabled

SSH disabled or enabled.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.10.1

7.0.1.2.2 cfgSshPort

SSH port.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.10.2

7.0.1.3 cfgCli

7.0.1.3.1 cfgCliEnabled

CLI feature support configuration.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.100.1

7.0.1.3.2 cfgCliUsername

CLI username.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 31
OID	1.3.6.1.4.1.16177.1.400.1.1.100.2

7.0.1.3.3 cfgCliPassword

CLI password.

For SSH, a password is mandatory. Accessing the device via telnet without using a password is done by setting the password to an empty string (zero string).

Access	readwrite
Status	current
Type	DisplayString
Range	0 - 63
OID	1.3.6.1.4.1.16177.1.400.1.1.100.3

7.0.1.3.4 cfgCliTelnetEnabled

CLI telnet support configuration.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.100.4

7.0.1.3.5 cfgCliTelnetPort

CLI telnet port (default: 23).

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.100.5

7.0.1.3.6 cfgCliSshEnabled

CLI SSH support configuration.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.100.6

7.0.1.3.7 cfgCliSshPort

CLI SSH port (default: 22).

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.100.7

7.0.1.4 cfgLogging

7.0.1.4.1 cfgLogFile

7.0.1.4.1.1 cfgLogFileEnabled

Log messages to file.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.11.1.1

7.0.1.4.1.2 cfgLogFileLevel

Log only messages with higher or equal log level.

Applies to AP and STA.

Enumeration	emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), debug (7)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.11.1.2

7.0.1.4.1.3 cfgLogFileName

Log file.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.11.1.3

7.0.1.4.1.4 cfgLogFileSize

Maximum size of log buffer or log file in KB.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.11.1.4

7.0.1.4.2 cfgLogRemote

7.0.1.4.2.1 cfgLogRemoteTable

List of syslog destinations.

Applies to AP and STA.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1

7.0.1.4.2.2 cfgLogRemoteEnabled

Log messages to file.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.2

7.0.1.4.2.3 cfgLogRemoteLevel

Log only messages with equal or higher priority than prio N (0-7).

Applies to AP and STA.

Enumeration	emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), debug (7)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.3

7.0.1.4.2.4 cfgLogRemoteProtocol

Protocol to send log messages. The udp(0) protocol complies with the standard syslog protocol.

Applies to AP and STA.

Enumeration	udp (0), tcp (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.4

7.0.1.4.2.5 cfgLogRemoteIp

Remote IP address.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.5

7.0.1.4.2.6 cfgLogRemotePort

Remote port.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.6

7.0.1.5 cfgSnmp

7.0.1.5.1 cfgSnmpd

7.0.1.5.1.1 cfgSnmpdLocation

SNMP system location.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.1

7.0.1.5.1.2 cfgSnmpdCommunity

cfgSnmpdComAdmin
Password for the administrator.

This is the community or the passphrase for the user administrator depending on the cfgSnmpdVersion:

- **v2c:** community string for administrator
- **v3usm:** passphrase for authentication and privacy for user admin

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.100.1

cfgSnmpdComMaintainer
Password for the maintainer.

This is the community or the passphrase for the user maintainer depending on the cfgSnmpdVersion:

- **v2c:** community string for maintainer
- **v3usm:** passphrase for authentication and privacy for user maintainer

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.100.2

cfgSnmpdComMonitor
Password for the monitor.

This is the community or the passphrase for the user monitor depending on the cfgSnmpdVersion:

- **v2c:** community string for monitor
- **v3usm:** passphrase for authentication and privacy for user monitor

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.100.3

cfgSnmpdContact
SNMP contact.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.2

cfgSnmpdVersion
SNMP version, either **v2c(0)** or **v3usm(1)**, for the users admin, maintainer and monitor.

Please refer to the user guide for more information about the access rights of the three predefined users.

The User-based Security Model (USM), which is the default Security Module for SNMPv3, with the authentication type SHA and the privacy protocol AES is implemented and can be chosen by setting this value to **v3usm(1)**.

Setting **v3usm(1)** disables access to the device via SNMPv2.

SNMPv3 USM configuration:

- **User:** admin, maintainer or monitor
- **Authentication Protocol:** SHA
- **Privacy Protocol:** AES

Applies to AP and STA.

Enumeration	v2c (0), v3usm (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.3

cfgSnmpdName
SNMP node name often used in NMS.

By convention, this is the node's fully-qualified domain name.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.4

7.0.1.5.2 cfgSnmpTrap

7.0.1.5.2.1 cfgSnmpTrapEnabled
Enable sending of SNMP traps.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.12.10.1

7.0.1.5.2.2 cfgSnmpTrapVersion
SNMP version with which traps are sent.

Applies to AP and STA.

Enumeration	v1 (0), v2c (1), v3usm (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.12.10.2

7.0.1.5.2.3 cfgSnmpTrapCommunity

SNMP community if SNMP v2c is used.

If SNMP v3 is used the community string is the password.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.12.10.3

7.0.1.5.2.4 cfgSnmpTrapDest

IP address of the trap receiver. Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.12.10.4

7.0.1.6 cfgDhcp

7.0.1.6.1 cfgDhcpGlobal

7.0.1.6.1.1 cfgDhcpGlobalEnabled

Enable DHCP server functionality.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.13.1.1

7.0.1.6.1.2 cfgDhcpDnsmasqTable

DHCP Dnsmasq instances.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.13.2

7.0.1.6.1.3 cfgDhcpDnsmasqScopeParameter

Parameter to set which scope ID to use for the DHCP server.

This is used in conjunction with the scope ID parameter (see cfgDhcpScopeId).

Access	readwrite
Status	current
Range	0 - 8
OID	1.3.6.1.4.1.16177.1.400.1.1.13.2.1.2

7.0.1.6.1.4 cfgDhcpScopeTable

DHCP instance configs.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3

7.0.1.6.1.5 cfgDhcpScopeId

Several scopes can share the same ID.

This is used in conjunction with the DHCP parameter (see cfgDhcpDnsmasqScopeParameter).

Access	readwrite
Status	current
Range	0 - 8
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.2

7.0.1.6.1.6 cfgDhcpScopeInterface

Network interface (ETH, VLAN, WLAN) on which the DHCP server runs. If the interface is part of a bridge, the server will run on that bridge.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.3

7.0.1.6.1.7 cfgDhcpScopeStart

Specifies the offset from the network address of the underlying interface to calculate the minimum address that may be leased to clients. It may be greater than 255 to span subnets.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.4

7.0.1.6.1.8 cfgDhcpScopeLimit

Specifies the maximum allowable address that may be leased to clients, calculated as network address + 'start' + 'limit'.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.5

7.0.1.6.1.9 cfgDhcpScopeLeasetime

Specifies the lease time of addresses handed out to clients, e.g. 12h or 30m.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.6

7.0.1.6.1.10 cfgDhcpScopeGateway

Specifies the gateway address handed out to clients. A value of 0.0.0.0 means not used.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.7

7.0.1.6.1.11 cfgDhcpScopeDnsServer1

Specifies the primary DNS server address handed out to clients. A value of 0.0.0.0 means not used.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.8

7.0.1.6.1.12 cfgDhcpScopeDnsServer2

Specifies the secondary DNS server address handed out to clients. If the first DNS server is not used, this server will also be ignored. A value of 0.0.0.0 means not used.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.9

7.0.1.7 cfgNtp

7.0.1.7.1 cfgNtpEnabled

Synchronize the system time with given server.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.14.1

7.0.1.7.2 cfgNtpServer1

NTP server 1.

If the IP is set to 0.0.0.0 the NTP client will only listen to broadcast packages.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.14.2

7.0.1.7.3 cfgNtpServer2

NTP server 2.

Used as fallback if server 1 cannot be reached.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.14.3

7.0.1.8 cfgHttp

7.0.1.8.1 cfgHttpUser

Web administrator username.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.15.1

7.0.1.8.2 cfgHttpPassword

Web administrator password.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	5 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.15.2

7.0.1.8.3 cfgHttpRedirectEnabled

Configure if by default all access to the HTTP server on port 80 shall be redirected to HTTPS. This does not disable HTTPS.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.15.4

7.0.1.9 cfgLldp

7.0.1.9.1 cfgLldpEnabled

Enable LLDP.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.16.1

7.0.1.10 cfgMdns

7.0.1.10.1 cfgMdnsEnabled

Enable mDNS.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.17.1

7.0.1.10.2 cfgMdnsNetwork

Space separated list of mDNS aware network interfaces

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.17.2

7.0.1.11 cfgNetwork

7.0.1.11.1 cfgNetEthernetTable

Ethernet Network Interfaces.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1

7.0.1.11.2 cfgNetEthTrunk

This entry is active when cfgNetEthVlanMode is set to **trunk(0)** or **native-untagged(3)**. It specifies which 802.1q VLANs are accepting ingress and egress on the respective port. All unspecified VLANs are dropped. Set this entry to -1 to allow all VLANs. Untagged traffic is considered to be VLAN 0.

The format of this entry is a space or comma-separated list. E.g. '0,12,24,69' or '7 56 127' or '0, 84, 99, 2000'

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 32767
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.10

7.0.1.11.3 cfgNetEthTag

This entry is active when cfgNetEthVlanMode is set to access (1) or native-untagged (3). It specifies which 802.1q VLAN should be used for untagged ingress and egress traffic. Set this entry to -1 to disable it.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.11

7.0.1.11.4 cfgNetEthVlanMode

This entry specifies how the port should behave.

trunk(0)

A trunk port carries packets on one or more specified VLANs specified in the cfgNetEthTrunk entry. A packet that ingresses on a trunk port is in the VLAN specified in its 802.1q header, or VLAN 0 if the packet has no 802.1q header (untagged frame). A packet that egresses through a trunk port will have an 802.1q header if it has a nonzero VLAN ID. Frames egressing on VLAN 0 have their tag stripped (egress untagged). Any packet that ingresses on a trunk port tagged with a VLAN that the port does not trunk is dropped.

access(1)

An access port carries packets on exactly one VLAN specified in cfgNetEthTag. Packets egressing on an access port have no 802.1q header (egress untagged). Any packet with an 802.1q header with

a nonzero VLAN ID that ingresses on an access port is dropped, regardless of whether the VLAN ID in the header is the access port's VLAN ID or not.

nativeuntagged(3)

A native-untagged port resembles a trunk port, with the exception that a packet without an 802.1q header (ingress untagged) is automatically in the native VLAN specified in cfgNetEthTag. Frames egressing in the native VLAN are automatically untagged (egress untagged).

Applies to AP and STA.

Enumeration	trunk (0), access (1), nativeuntagged (3)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.12

7.0.1.11.5 cfgNetEthName

Name of the ethernet interface.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.2

7.0.1.11.6 cfgNetEthEnabled

Ethernet interface disabled or enabled.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.3

7.0.1.11.7 cfgNetEthBridge

If set to other than -1 the interface is part of bridge:

- -1: none
- 0: br0
- 1: br1

- X: brX

Bridges with an index >=100 are special bridges which forward link local traffic. This can be used for wireless links in 4addr mode which should act as a cable-replacement.

Notice: Such a bridge may only contain 2 interfaces!

Example

- wlan0 and eth0 in br100, with eth1 as management interface.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.7

7.0.1.11.8 cfgNetEthAutoneg

Enables or disables auto negotiation of the PHY.

forced(0)

Forces the speed and duplex defined by cfgNetEthSpeed. Only 10Mbit and 100Mbit rates are allowed in forced mode. 1000Mbit requires the mode to be auto.

auto(1)

Advertises the supported auto negotiation defined by cfgNetEthSpeed.

Applies to AP and STA.

Enumeration	forced (0), auto (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.8

7.0.1.11.9 cfgNetEthSpeed

Defines a bitmask containing the possible speed/duplex combinations.

- 0x01 (1) = 10Mbit/Half
- 0x02 (2) = 10Mbit/Full
- 0x04 (4) = 100Mbit/Half
- 0x08 (8) = 100Mbit/Full

- 0x20 (32) = 1000Mbit/Full

When cfgNetEthSpeed is forced(0) only a single bit may be active. Only 10Mbit and 100Mbit rates are allowed in forced mode. 1000Mbit requires the mode to be auto. When cfgNetEthSpeed is auto(1) multiple bits may be set which are used to advertise the supported speed/duplex. 1000Mbit/Half is not supported.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.2.1.1.9

7.0.1.11.10 cfgNetWlanTable

WLAN Network Interfaces.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2

7.0.1.11.11 cfgNetWlanTrunk

This entry is active when cfgNetWlanVlanMode is set to 0 (trunk) or 3 (native-untagged). It specifies which 802.1q VLANs are accepted ingress and egress on the respective port. All unspecified VLANs are dropped. Set this entry to -1 to allow all VLANs. Untagged traffic is considered to be VLAN 0.

The format of this entry is a space or comma-separated list.

Examples

‘0,12,24,69’ or ‘7 56 127’ or ‘0, 84, 99, 2000’

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 32767
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2.1.10

7.0.1.11.12 cfgNetWlanTag

This entry is active when cfgNetWlanVlanMode is set to access (1) or native-untagged (3). It specifies which 802.1q VLAN should be used for untagged ingress and egress traffic. Set this entry to -1 to disable it.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2.1.11

7.0.1.11.13 cfgNetWlanVlanMode

This entry specifies how the port should behave.

trunk(0)

A trunk port carries packets on one or more specified VLANs specified in the cfgNetWlanTrunk entry. A packet that ingresses on a trunk port is in the VLAN specified in its 802.1q header, or VLAN 0 if the packet has no 802.1q header (untagged frame). A packet that egresses through a trunk port will have an 802.1q header if it has a nonzero VLAN ID. Frames egressing on VLAN 0 have their tag stripped (egress untagged). Any packet that ingresses on a trunk port tagged with a VLAN that the port does not trunk is dropped.

access(1)

An access port carries packets on exactly one VLAN specified in the cfgNetWlanTag. Packets egressing on an access port have no 802.1q header (egress untagged). Any packet with an 802.1q header with a nonzero VLAN ID that ingresses on an access port is dropped, regardless of whether the VLAN ID in the header is the access port's VLAN ID.

nativeuntagged(3)

A native-untagged port resembles a trunk port, with the exception that a packet without an 802.1q header (ingress untagged) is automatically in the native VLAN specified in cfgNetWlanTag. Frames egressing in the native VLAN are automatically untagged (egress untagged).

Applies to AP and STA.

Enumeration	trunk (0), access (1), nativeuntagged (3)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2.1.12

7.0.1.11.14 cfgNetWlanName

Name of the wireless interface.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2.1.2

7.0.1.11.15 cfgNetWlanEnabled

Wireless interface disabled or enabled.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2.1.3

7.0.1.11.16 cfgNetWlanBridge

If set to other than -1 the interface is part of bridge:

- -1: none
- 0: br0
- 1: br1
- X: brX

Bridges with an index >=100 are special bridges which forward link local traffic. This can be used for wireless links in 4addr mode which should act as a cable-replacement.

Notice: such a bridge may only contain 2 interfaces!

Example

wlan0 and eth0 in br100, with eth1 as managment interface.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.2.2.1.7

7.0.1.11.17 cfgNetVlanTable

VLAN Network Interfaces.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3

7.0.1.11.18 cfgNetVlanName

Name of the VLAN interface.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.2

7.0.1.11.19 cfgNetVlanEnabled

VLAN interface disabled or enabled.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.3

7.0.1.11.20 cfgNetVlanBridge

The number of the bridge the VLAN interface is applied to. VLAN interfaces are always of type access.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.7

7.0.1.11.21 cfgNetVlanParent

Name of the physical parent interface on which the VLAN resides. This entry is only active when the VLAN interface is not part of a bridge (cfgNetVlanBridge = -1).

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.8

7.0.1.11.22 cfgNetVlanVid

ID of the VLAN.

Applies to AP and STA.

Access	readwrite
Status	current
Range	0 - 4094
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.9

7.0.1.11.23 cfgNetIpTable

IP address.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.6

7.0.1.11.24 cfgNetIpEnabled

IP disabled or enabled.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.6.1.3

7.0.1.11.25 cfgNetIpAddr

The IPv4 address (using CIDR notation) of the interface specified in cfgNetIpInterface.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	9 - 19
OID	1.3.6.1.4.1.16177.1.400.1.1.2.6.1.4

7.0.1.11.26 cfgNetIpProto

This parameter defines which protocol is used to get the IPv4 settings for this interface.

static(0)

Indicates that the address is manually configured to a specified address given by the IPv4 address parameter of this interface configuration.

dhcp(1)

Indicates that an IPv4 address will be obtained by the DHCP client. In case the DHCP client is unable to get a valid IPv4 address the static IP address will be used as a fallback.

linkLocal(4)

Indicates that an IPv4 link local address (an address in the range of 169.254.0.1 to 169.254.255.254, randomly chosen by the system) will be used on this interface. cfgNetIpAddr is then not used for the interface. Note: Only one interface of the device can use a link local protocol.

For wireless interfaces, the following additional modes are available:

dhcpForceRenew(2)

Indicates that an IPv4 address will be obtained by the DHCP client. In case the DHCP client is unable to get a valid IPv4 address the static IP address will be used as a fallback. On a STA this mode will perform a DHCP RENEW after every connection to an AP. This is useful if the device is roaming between different DHCP servers.

dhcpForceRelease(3)

Indicates that an IPv4 address will be obtained by the DHCP client. In case the DHCP client is unable to get a valid IPv4 address, the static IP address will be used as a fallback. On a STA this mode will perform a DHCP RELEASE followed by a DHCP DISCOVER after every connection to an AP. This is useful if the device is roaming between different DHCP servers which don't send NAK to an unknown device sending RENEW.

Applies to AP and STA.

Enumeration	static (0), dhcp (1), dhcpForceRenew (2), dhcpForceRelease (3), linkLocal (4)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.2.6.1.6

7.0.1.11.27 cfgNetIpInterface

Name of the interface on which the IP resides.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.2.6.1.8

7.0.1.12 cfgWireless

7.0.1.12.1 cfgWlanDeviceTable

Wireless Hardware Modules.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1

7.0.1.12.2 cfgWlanDevDistance

Maximum distance in meters a client can be apart from the access point. Even though the distance is set in meters, the slot time settings change in 450ms steps.

Applies to AP and STA.

Access	readwrite
Status	current
Range	0 - 114750
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.10

7.0.1.12.3 cfgWlanDevRts

Frames equal or longer than this value require a RTS/CTS handshake.

RTS/CTS is used in hidden node situations. In 11bg and b mode, these frames are sent in DSSS modulation at 11b data rates. Otherwise (pure-g and a) OFDM rates are used.

The following settings are special:

- **-1** disable value, RTS/CTS is disabled.
- **0** minimum value, RTS/CTS is always used.
- **2346** maximum value legacy-rates, RTS/CTS is enabled for maximum sized frames.
- **65535** maximum value n-rates, RTS/CTS is enabled for maximal aggregate sized frames.

Notice: It is not recommended to use RTS/CTS in AP mode.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 65535
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.11

7.0.1.12.4 cfgWlanDevFragments

Frames longer than this threshold will be fragmented.

Fragmentation can be used to reduce the number of retransmissions. The following settings are special

- **-1** disable value, fragmentation is disabled
- **256** minimum value, frames above 256 are fragmented.
- **2346** maximum value, essentially the same as disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 2346
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.12

7.0.1.12.5 cfgWlanDevShortRetry

Number of times the transmission of the RTS frame will be retried if there is no CTS received from the AP.

Applies to AP and STA.

Access	readwrite
Status	current
Range	1 - 10
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.13

7.0.1.12.6 cfgWlanDevLongRetry

Number of times the unicast data frames will be retried if there is no ACK from the receiver.

Applies to AP and STA.

Access	readwrite
Status	current
Range	1 - 10
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.14

7.0.1.12.7 cfgWlanDevAntennaGain

Antenna gain in dBi.

If multiple antennas with different gains are connected, the value of the antenna with the highest gain shall be configured.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.15

7.0.1.12.8 cfgWlanDevTxAntenna

Configure the number of wireless transmission antennas.

This is a bitmask to enable/disable the chains.

Example

- 1(001) = A1 (chain 0) enabled
- 3(011) = A1 and A2 (chain 0 and 1) enabled
- 7(111) = A1, A2 and A3 (chain 0, 1 and 2) enabled

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.16

7.0.1.12.9 cfgWlanDevRxAntenna

Configure the number of wireless receiver antennas.

This is a bitmask to enable/disable the chains.

Example

- 1(001) = A1 (chain 0) enabled
- 3(011) = A1 and A2 chain 0 and 1) enabled
- 7(111) = A1, A2 and A3 (chain 0, 1 and 2) enabled

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.17

7.0.1.12.10 cfgWlanDevPhy

The map between physical device and radio.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.18

7.0.1.12.11 cfgWlanDevName

Name of the wireless device.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.2

7.0.1.12.12 cfgWlanDevHtCapabilities

HT capability flags:

- [LDPC] = 1 Enable support for LDPC coding
- [SHORT-GI-20] = 32 Allow short GI for 20 MHz
- [SHORT-GI-40] = 64 Allow short GI for 40 MHz
- [TX-STBC] = 128 Enable support for TX-STBC
- [RX-STBC1] = 256 Enable support for RX-STBC1
- [DSSS_CCK-40] = 4096 Enable support for DSSS/CCK Mode in 40 MHz
- [40-INTOLERANT] = 16384 Advertise 40 MHz intolerance

Applies to AP.

Access	readwrite
Status	current
Range	0 - 65535
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.24

7.0.1.12.13 cfgWlanDevRfOutput

Ability to disable transmission of RF signal.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.3

7.0.1.12.14 cfgWlanDevModulation

The modulation modes of the physical wireless device are:

g(2)

This modulation mode uses OFDM data rates up to 54 MBit/s in the frequency band between 2.4 and 2.4835 GHz. It supports the 802.11g standard.

bg(3)

This modulation mode uses data rates up to 54 MBit/s in the frequency band between 2.4 and 2.4835 GHz. It supports the 802.11bg standard. The modulation is either DSSS for the slower rates or OFDM for the faster ones.

a(4)

Mode supports data rates up to 54 MBit/s in the 5GHz frequency band and only OFDM modulation.

n(8)

Mode supports data rates up to 300 MBit/s in the 2.4GHz and 5GHz frequency band and only OFDM modulation. This mode (n) cannot be used as such. It has to be combined with g or a to specify which frequency band shall be used.

ng(10)

For 2.4GHz

na(12)

For 5GHz.

Applies to AP and STA.

Enumeration	a (4), ng (10), bg (3), na (12), g (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.4

7.0.1.12.15 cfgWlanDevBandwidth

Wireless Bandwidth Mode specifies the Bandwidth of the Channel.

- **ht20(0)** for HT20 20MHz wide channel.
- **ht40Plus(1)** for HT40+ 40MHz wide channel with the side channel on the top.
- **ht40Minus(2)** for HT40- 40MHz wide channel with the side channel on the bottom.
- **quarter(3)** for 5MHz wide channel (quarter rate).
- **half(4)** for 10MHz wide channel (half rate).

HT40+ and HT40- may not be usable on all channels. The following table shows examples of which channels may be used. The full list can be found in IEEE 802.11n Annex J. Depending on the country, not all frequencies may be available

Examples

freq	HT40+	HT40-
2.4 GHz	2412 to 2452	2432 to 2472
5 GHz	5180, 5220, 5260, etc.	5200, 5240, 5280, etc.

Applies to AP and STA.

Enumeration	ht20 (0), ht40Plus (1), ht40Minus (2), quarter (3), half (4)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.5

7.0.1.12.16 cfgWlanDevFrequency

Wireless Frequency in MHz.

In AP mode, setting the wireless frequency to zero(0) enables the automatic channel selection (ACS) feature. This forces the AP to choose the best channel for operation.

In STA mode, the cfgWlanIfaceScanList is used to configure which frequencies are to be used.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.6

7.0.1.12.17 cfgWlanDevPower

Wireless output power as combined power of all chains in dBm including antenna gain. (EIRP).

Notice: For a setup with two antennas, the transmission power on each antenna port is approximately 3dB lower than combined transmission power.

Applies to AP and STA.

Access	readwrite
Status	current
Range	6 - 50
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.8

7.0.1.12.18 cfgWlan802dot1xTable

Wireless 802dot1x.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10

7.0.1.12.19 cfgWlan802dot1xIdentity

The identity string for EAP.

Applies to STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.10

7.0.1.12.20 cfgWlan802dot1xClientKeyPassword

The password to unlock the private key.

This is only required if the key is encrypted.

Applies to STA.

Access	readwrite
Status	current
Type	DisplayString
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.17

7.0.1.12.21 cfgWlan802dot1xName

Name of the virtual wireless interface.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.2

7.0.1.12.22 cfgWlan802dot1xOwnIpAddr

The own IP address of the access point (used as NAS-IP-Address).

Applies to AP.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.3

7.0.1.12.23 cfgWlan802dot1xAuthServerParameter

Reference ID to the radius auth server table. Uses all parameters in the cfgWlan802dot1xAuthServerTable which have as cfgWlan802dot1xAuthSrvId the value set here.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.4

7.0.1.12.24 cfgWlan802dot1xAcctServerParameter

Reference ID to the radius acct server table. Uses all parameters in the cfgWlan802dot1xAcctServerTable which have as cfgWlan802dot1xAcctSrvId the value set here.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.5

7.0.1.12.25 cfgWlan802dot1xRetryPrimaryInterval

Retry interval for trying to return to the primary RADIUS server (in seconds). RADIUS client code will automatically try to use the next server when the current server is not replying to requests. If this interval is set, primary server will be retried after configured amount of time even if the currently used secondary server is still working. Set to 0 to disable.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 86400
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.6

7.0.1.12.26 cfgWlan802dot1xInterimAccountingInterval

Interim accounting update interval

If this is set (larger than 0) and acct_server is configured, hostapd will send interim accounting updates every N seconds. Set to 0 to disable.

Notice: If set, this overrides possible Acct-Interim-Interval attribute in Access-Accept message. Thus, this value should not be configured in hostapd.conf if RADIUS server is used to control the interim interval. This value should not be less 600 (10 minutes) and must not be less than 60 (1 minute).

Applies to AP.

Access	readwrite
Status	current
Range	0 - 86400
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.7

7.0.1.12.27 cfgWlan802dot1xNasId

Optional NAS identifier string for RADIUS messages. When used, this should be unique to the NAS

within the scope of the RADIUS server. For example, a fully qualified domain name can be used here. When using IEEE 802.11r, nas_identifier must be set and must be between 1 and 48 octets long.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 48
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.8

7.0.1.12.28 cfgWlan802dot1xEapType

Specify the EAP type.

Applies to STA.

Enumeration	tls (0), peap (1), ttls (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.9

7.0.1.12.29 cfgWlan802dot1xAuthServerTable

Wireless 802dot1x AuthServer.

Applies to AP.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.11

7.0.1.12.30 cfgWlan802dot1xAuthSrvEnabled

Enable this entry in the auth server list.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.11.1.2

7.0.1.12.31 cfgWlan802dot1xAuthSrvId

ID of the authorisation server table. The configuration item cfgWlan802dot1xAuthServerParameter references to this ID.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.11.1.3

7.0.1.12.32 cfgWlan802dot1xAuthSrvIpAddr

IP of the RADIUS server against which will be authenticated.

Applies to AP.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.3.11.1.4

7.0.1.12.33 cfgWlan802dot1xAuthSrvPort

Port of the RADIUS server against which will be authenticated.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.11.1.5

7.0.1.12.34 cfgWlan802dot1xAuthSrvSharedSecret

Password to connect to the specified RADIUS server.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.11.1.6

7.0.1.12.35 cfgWlan802dot1xAcctServerTable

Wireless 802dot1x AcctServer.

Applies to AP.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.12

7.0.1.12.36 cfgWlan802dot1xAcctSrvEnabled

Enable this entry in the acct server list.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.12.1.2

7.0.1.12.37 cfgWlan802dot1xAcctSrvId

ID of the accounting server table. The configuration item cfgWlan802dot1xAcctServerParameter refers to this ID.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.12.1.3

7.0.1.12.38 cfgWlan802dot1xAcctSrvIpAddr

IP of the RADIUS accounting server. Set to 0.0.0.0 to disable.

Applies to AP.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.3.12.1.4

7.0.1.12.39 cfgWlan802dot1xAcctSrvPort

Port of the RADIUS accounting server.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.12.1.5

7.0.1.12.40 cfgWlan802dot1xAcctSrvSharedSecret

Password to connect to the specified RADIUS accounting server.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.12.1.6

7.0.1.12.41 cfgWlan802dot11rTable

Wireless 802dot11r.

Applies to AP.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13

7.0.1.12.42 cfgWlan802dot11rR0KHParameter

Reference ID to the R0KH parameter table. Uses all parameters in the cfgWlan802dot11rR0KHTable which have as cfgWlan802dot11rR0KHTblId the value set here.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.10

7.0.1.12.43 cfgWlan802dot11rR1KHParameter

Reference ID to the R1KH parameter table. Uses all parameters in the cfgWlan802dot11rR1KHTable which have as cfgWlan802dot11rR1KHTblId the value set here.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.11

7.0.1.12.44 cfgWlan802dot11rName

Name of the virtual wireless interface.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.2

7.0.1.12.45 cfgWlan802dot11rEnabled

Enable usage of 802.11r on this device.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.3

7.0.1.12.46 cfgWlan802dot11rMobilityDomain

Mobility Domain identifier (dot11FTMobilityDomainID, MDID) MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. 2-octet identifier as a hex string.

Example

mobility_domain=a1b2

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	4 - 4
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.4

7.0.1.12.47 cfgWlan802dot11rPmkR0KeyHolderIdentifier

PMK-R0 Key Holder identifier (dot11FTR0KeyHolderID).

Configure this in the field cfgWlan802dot1xNasId.

Applies to AP.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 48
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.5

7.0.1.12.48 cfgWlan802dot11rPmkR0Lifetime

Default lifetime of the PMK-RO in minutes (dot11FTR0KeyLifetime).

Applies to AP.

Access	readwrite
Status	current
Range	1 - 65535
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.6

7.0.1.12.49 cfgWlan802dot11rPmkR1KeyHolderIdentifier

PMK-R1 Key Holder identifier (dot11FTR0KeyHolderID).

6-octet identifier as a hex string. This may be the same as the local MAC address. Default magic number 000102030405 means use own mac address (bssid).

Format: `020102030405`

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	12 - 12
OID	1.3.6.1.4.1.16177.1.400.1.1.3.13.1.7

7.0.1.12.50 cfgWlan802dot11rR0KHTable

Wireless 802dot11r R0KH.

List of R0KHs in the same Mobility Domain. This list is used to map R0KH-ID (NAS Identifier) to a destination MAC address when requesting PMK-R1 key from the R0KH that the STA used during the Initial Mobility Domain Association.

Format: <128-bit key as hex string>

Example

```
r0kh=02:01:02:03:04:05 r0kh-1.example.com 000102030405060708090a0b0c0d0e0f
r0kh=02:01:02:03:04:06 r0kh-2.example.com 00112233445566778899aabbccddeeff
```

Applies to AP.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.14

7.0.1.12.51 cfgWlan802dot11rR0KHId

ID of the R0KH table.

The configuration item cfgWlan802dot11rR0KHParameter references to this ID.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.14.1.2

7.0.1.12.52 cfgWlan802dot11rR0KHEnabled

Enable this entry in the R0KH list.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.14.1.3

7.0.1.12.53 cfgWlan802dot11rR0KHDestinationMac

MAC addresses of all possible R0KHs from which PMK-R1 can be requested.

Format: `02:01:02:03:04:05`

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	17 - 17
OID	1.3.6.1.4.1.16177.1.400.1.1.3.14.1.4

7.0.1.12.54 cfgWlan802dot11rR0KHHID

NAS Identifier of all R0KHs to map to the MAC address.

See the field: cfgWlan802dot11rPmkR0KeyHolderIdentifier.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 48
OID	1.3.6.1.4.1.16177.1.400.1.1.3.14.1.5

7.0.1.12.55 cfgWlan802dot11rR0KHKey

Static Key of the R0KH.

Connecting R1KHs need to have this key configured.

Format: `000102030405060708090a0b0c0d0e0f`

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	32 - 32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.14.1.6

7.0.1.12.56 cfgWlan802dot11rR1KHTable

Wireless 802dot11r R1KH.

List of R1KHs in the same Mobility Domain This list is used to map R1KH-ID to a destination MAC address when sending PMK-R1 key from the R0KH. This is also the list of authorized R1KHs in the MD that can request PMK-R1 keys.

Format: <128-bit key as hex string>

Example

```
r1kh=02:01:02:03:04:05 02:11:22:33:44:55 000102030405060708090a0b0c0d0e0f
r1kh=02:01:02:03:04:06 02:11:22:33:44:66 00112233445566778899aabbccddeeff
```

Applies to AP.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.15

7.0.1.12.57 cfgWlan802dot11rR1KHId

ID of the R1KH table.

The configuration item cfgWlan802dot11rR1KHParameter references to this ID.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.15.1.2

7.0.1.12.58 cfgWlan802dot11rR1KHEnabled

Enable this entry in the R1KH list.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.15.1.3

7.0.1.12.59 cfgWlan802dot11rR1KHDestinationMac

MAC addresses of all R1KHs which can reqest PMK-R1 from the local R0KH.

Format: `02:01:02:03:04:05`

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	17 - 17
OID	1.3.6.1.4.1.16177.1.400.1.1.3.15.1.4

7.0.1.12.60 cfgWlan802dot11rR1KHHID

PMK-R1 Key Holder identifier (dot11FTR1KeyHolderID)

6-octet identifier as a hex string to map to the MAC. This may be the same as the destination MAC. See the field cfgWlan802dot11rPmkR1KeyHolderIdentifier.

Format: `02:01:02:03:04:05`

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	17 - 17
OID	1.3.6.1.4.1.16177.1.400.1.1.3.15.1.5

7.0.1.12.61 cfgWlan802dot11rR1KHKey

Static Key of the R0KH.

These keys are used wenn sending updates to R1KHs from the local R0KH. The respective key has to match the respective entry on the target in the field cfgWlan802dot11rR0KHKey.

Format: `000102030405060708090a0b0c0d0e0f`

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	32 - 32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.15.1.6

7.0.1.12.62 cfgWlanInterfaceTable

Wireless Virtual Interfaces.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2

7.0.1.12.63 cfgWlanIfaceDtim

This attribute shall specify the number of beacon intervals that shall elapse between transmission of beacons frames containing a TIM element whose DTIM count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.10

7.0.1.12.64 cfgWlanIfaceBitrates

Fixed MCS index for 802.11n rates.

Set to -1 to disable (leave on auto). Allows for entering multiple indices divided by a space which are then used in auto rate. This entry is only active when an n-rate is set in cfgWlanDevModulation (not only g-rate or only a-rate).

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.11

7.0.1.12.65 cfgWlanIfaceBeaconInterval

Time in kus (1.024 ms) between the sending of beacon frames.

Applies to AP.

Access	readwrite
Status	current
Range	15 - 1000
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.12

7.0.1.12.66 cfgWlanIfaceWmeParameter

Reference ID to the WME parameter table.

Uses all parameters in the cfgWlanWmeTable which have as cfgWlanWmeId the value set here.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.13

7.0.1.12.67 cfgWlanIfaceWmeEnabled

Enables usage of the WME parameter table.

When using legacy rates (a-rates and g-rates) this is optional. When using n-rates this has to be enabled at all times.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.14

7.0.1.12.68 cfgWlanIfaceScanList

Index to specify a frequency list with frequencies to be scanned when in STA mode. To only scan the frequency defined in cfgWlanDevFrequency set to -1. To scan all frequencies allowed by the configured country code set to -2.

Applies to STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.15

7.0.1.12.69 cfgWlanIfaceIgnoreBroadcastSsid

Send empty SSID in beacons and ignore probe request frames that do not specify the full SSID, i.e., require stations to know SSID.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.16

7.0.1.12.70 cfgWlanIfaceMacaddrAcl

Mode of the MAC access control list.

acceptunlessdeny(0)

Accept unless deny filter. Accept every MAC unless it is on the list defined in cfgWlanAclBlackTable.

denyunlessaccept(1)

Deny unless accept filter. Deny every MAC unless it is on the list defined in cfgWlanAclWhiteTable.

radius(2)

Use RADIUS to accept/deny clients.

Applies to AP.

Enumeration	acceptunlessdeny (0), denyunlessaccept (1), radius (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.17

7.0.1.12.71 cfgWlanIfaceMaxNumSta

Maximum number of allowed stations which can connect to this AP.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.18

7.0.1.12.72 cfgWlanIfaceBssid

BSSID of AP.

Set 00:00:00:00:00:00 to use the MAC address stored in the flash of the wireless card itself. If this is the second virtual AP on this card it will automatically set the locally assigned bit. If there are more than 2 virtual APs on a single card this field MUST be set. Shall be in the format: 00:14:5a:02:10:42

When the device is operating in STA mode the MAC address of the wireless interface can be configured.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	17 - 17
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.19

7.0.1.12.73 cfgWlanIfaceName

Name of the virtual wireless interface.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.2

7.0.1.12.74 cfgWlanIfaceLegacyRates

Wireless legacy data rates:

- **11b:** 1, 2, 5.5, 11 Mbps
- **11a/g:** 6, 9, 12, 18, 24, 36, 48, 54 Mbps

The values are interpreted as flags:

- auto(0), 1Mbps(1), 2Mbps(2), 5.5Mbps(4), 6Mbps(8), 9Mbps(16),
- 11Mbps(32), 12Mbps(64), 18Mbps(128), 24Mbps(256), 36Mbps(512),
- 48Mbps(1024), 54Mbps(2048)

When cfgWlanDevBandwidth is equal 3 (quarter rates) the rate is quarter i.e. 36Mbps becomes 9MBps. When cfgWlanDevBandwidth is equal 4 (half rates) the rate is halved i.e. 36Mbps becomes 18MBps. This entry is only active when g-rates or a-rates are selected in cfgWlanDevModulation (disabled with n-rates).

Applies to AP and STA.

Access	readwrite
Status	current
Range	0 - 2048
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.20

7.0.1.12.75 cfgWlanIface4addr

This option allows to bridge the STA side.

When used on the STA, the corresponding AP has to enable this feature as well.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.21

7.0.1.12.76 cfgWlanIfaceInactivityTimeout

If a station does not send anything in ap_max_inactivity seconds, an empty data frame is sent to it in order to verify whether it is still in range. If this frame is not ACKed, the station will be disassociated and then deauthenticated. This feature is used to clear the station table of old entries when the STAs move out of range.

Applies to AP.

Access	readwrite
Status	current
Range	15 - 65535
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.23

7.0.1.12.77 cfgWlanIfaceUseVendorSsid

When cfgWlanIfaceIgnoreBroadcastSsid is enabled, a passively scanning STA (forced or because of DFS) has no way of detecting the AP it tries to find. On an AP this options adds the hidden SSID as vendor element. On a STA this options allows it to use the vendor element in the beacon.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.26

7.0.1.12.78 cfgWlanIfaceDevice

Maps the virtual wireless interface to the radio device.

Applies to AP and STA.

Enumeration	radio0 (0), radio1 (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.3

7.0.1.12.79 cfgWlanIfaceIeee80211w

Controls usage of 802.11w Management Frame Protection (MFP) mechanism. If set to optional on AP, MFP will be enabled only for clients which have it also enabled. If set to required, only MFP enabled clients will be able to connect.

Applies to AP and STA.

Enumeration	disabled (0), optional (1), required (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.30

7.0.1.12.80 cfgWlanIfaceIeee80211wMaxTimeout

802.11w Management Frame Protection (MFP)

Association SA query maximum timeout (in TU = 1.024 ms; for MFP) (maximum time to wait for a SA query response)

Applies to AP.

Access	readwrite
Status	current
Range	1 - 4000
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.31

7.0.1.12.81 cfgWlanIfaceIeee80211wRetryTimeout

802.11w Management Frame Protection (MFP)

Association SA query retry timeout (in TU = 1.024 ms; for MFP) (time between two subsequent SA query requests)

Applies to AP.

Access	readwrite
Status	current
Range	1 - 4000
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.32

7.0.1.12.82 cfgWlanIfaceMode

Wireless Operation Mode.

Allowed modes are:

- **ap(0)** defines the interface as Access Point (AP)
- **sta(1)** defines the interface as Station (STA)
- **monitor(2)** defines the interface as Monitor (MON)

Enumeration	ap (0), sta (1), monitor (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.4

7.0.1.12.83 cfgWlanIfaceAcsList

Index to specify a frequency list for Automated Channel Selection (ACS) support when in AP mode. To disable set to -1.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.40

7.0.1.12.84 cfgWlanIfaceSsid

The Service Set Identifier (SSID) of the wireless interface is the arbitrary name of the wireless network this interface is part of.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.5

7.0.1.12.85 cfgWlanIfaceEncryption

Wireless Encryption Mode.

Three encryption modes are supported: **open(0)**, **wpa2(3)** and **wpa2eap(6)**. WPA2 EAP enables 802.1X support.

Applies to AP and STA.

Enumeration	open (0), wpa2 (3), wpa2eap (6)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.6

7.0.1.12.86 cfgWlanIfacePassword

Wireless password if an encryption is in use.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	8 - 63
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.7

7.0.1.12.87 cfgWlanIfacePassiveScanning

Wireless Scanning Mode:

If the scanning mode is set to active(0) the station will send a probe request to detect available access points if it's allowed by the country code.

If the scanning mode is set to passive(1) the station will always perform passive scanning to detect available access points.

Applies to STA.

Enumeration	active (0), passive (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.8

7.0.1.12.88 cfgWlanIfaceBeaconMiss

Number of misses on consecutive beacons before the station will disconnect from the associated access point.

Applies to STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.9

7.0.1.12.89 cfgWlanHandoffTable

Wireless handoff parameters.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3

7.0.1.12.90 cfgWlanHoScanRateLimitTime

Time in ms (jiffy steps) in which a number of attempts to connect to an AP can be tried.

Applies to STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.12

7.0.1.12.91 cfgWlanHoScanRateLimitTries

Number of attempts to connect to an AP before the AP is blacklisted and ignored. The AP is removed from the blacklist after cfgWlanHoScanRateLimitTime since the first attempt.

Applies to STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.13

7.0.1.12.92 cfgWlanHoPassiveChanTime

Time in ms (jiffy steps) we stay on a channel during passive scanning and wait for beacons.

Applies to STA.

Access	readwrite
Status	current
Range	1 - 65535
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.16

7.0.1.12.93 cfgWlanHolfaceName

Name of the virtual wireless interface.

Applies to STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.2

7.0.1.12.94 cfgWlanHoProfile

Handoff profile.

- **t2gv1(1):** Train to Ground v1
- **t2gv2(2):** Train to Ground v2

Applies to STA.

Enumeration	t2gv1 (1), t2gv2 (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.3

7.0.1.12.95 cfgWlanHoScanningLevel

When the RSSI level of the currently connected access point drops below the value configured in this parameter, the STA will scan for better access points on all frequencies specified by the scan list configured in cfgWlanIfaceScanList and cfgWlanFreqTable.

Applies to STA.

Access	readwrite
Status	current
Range	0 - 95
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.5

7.0.1.12.96 cfgWlanHoBeacons

Number of beacons which have to be received from an AP before a decision about handoff is allowed. Essentially forces the STA to stay on a given AP for before doing another handoff. Applies to STA.

Access	readwrite
Status	current
Range	4 - 20
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.6

7.0.1.12.97 cfgWlanHoRecovery

Recovery time [ms] after a successful handoff.

During this time no further handoff will be executed.

Applies to STA.

Access	readwrite
Status	current
Range	0 - 2000
OID	1.3.6.1.4.1.16177.1.400.1.1.3.3.1.7

7.0.1.12.98 cfgWlanFreqTable

Frequency list entry.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4

7.0.1.12.99 cfgWlanFFreq8

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.10

7.0.1.12.100 cfgWlanFFreq9

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.11

7.0.1.12.101 cfgWlanFFreq10

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.12

7.0.1.12.102 cfgWlanFFreq11

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.13

7.0.1.12.103 cfgWlanFFreq12

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.14

7.0.1.12.104 cfgWlanFFreq13

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.15

7.0.1.12.105 cfgWlanFFreq14

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.16

7.0.1.12.106 cfgWlanFFreq15

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.17

7.0.1.12.107 cfgWlanFFreq16

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.18

7.0.1.12.108 cfgWlanFFreq17

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.19

7.0.1.12.109 cfgWlanFFreq0

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.2

7.0.1.12.110 cfgWlanFFreq18

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.20

7.0.1.12.111 cfgWlanFFreq19

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.21

7.0.1.12.112 cfgWlanFFreq20

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.22

7.0.1.12.113 cfgWlanFFreq21

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.23

7.0.1.12.114 cfgWlanFFreq22

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.24

7.0.1.12.115 cfgWlanFFreq23

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.25

7.0.1.12.116 cfgWlanFFreq1

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.3

7.0.1.12.117 cfgWlanFFreq2

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.4

7.0.1.12.118 cfgWlanFFreq3

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.5

7.0.1.12.119 cfgWlanFFreq4

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.6

7.0.1.12.120 cfgWlanFFreq5

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.7

7.0.1.12.121 cfgWlanFFreq6

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.8

7.0.1.12.122 cfgWlanFFreq7

Frequency, 0 is interpreted as empty.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.4.1.9

7.0.1.12.123 cfgWlanWmeTable

Wireless Multimedia Extensions (WME) based on the IEEE 802.11e standard. It provides basic Quality of Service (QoS) features to IEEE 802.11 networks.

The levels of priority in EDCA are called access categories (ACs). The contention window (CW) can be set according to the traffic expected for each access category, with a wider window needed for categories with heavier traffic.

Applies to AP.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5

7.0.1.12.124 cfgWlanWmeApAifs

Arbitration inter-frame space.

Is used on the AP itself.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.10

7.0.1.12.125 cfgWlanWmeApBurst

Maximum length for bursting (equivalent to TxOpLimit).

This value is in units of 32us. Is used on the AP itself.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.11

7.0.1.12.126 cfgWlanWmeId

ID of the WME parameter table. The virtual wireless interface references to this ID.

Applies to AP.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.2

7.0.1.12.127 cfgWlanWmeAc

Access category.

Applies to AP.

Enumeration	none (0), background (1), besteffort (2), video (3), voice (4)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.3

7.0.1.12.128 cfgWlanWmeCwMin

Contention window minimum in exponential form.

Is used on STAs connected to this AP: `Real value = (2^n)-1`

Applies to AP.

Access	readwrite
Status	current
Range	0 - 12
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.4

7.0.1.12.129 cfgWlanWmeCwMax

Contention window maximum in exponential form.

Is used on STAs connected to this AP: `Real value = (2^n)-1`

Applies to AP.

Access	readwrite
Status	current
Range	0 - 12
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.5

7.0.1.12.130 cfgWlanWmeAifs

Arbitration inter-frame space.

Is used on STAs connected to this AP.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.6

7.0.1.12.131 cfgWlanWmeTxOpMax

A Transmit Opportunity (TXOP) is a bound time interval during which a station can send as many frames as possible (as long as the duration of the transmissions does not exceed the maximum duration of the TXOP). A value of 0 indicates that a single MSDU or MMPDU in addition to a possible RTS/CTS or CTS to itself may be transmitted at any PHY rate for each TXOP. This value is in units of 32 us. Is used on STAs connected to this AP.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.7

7.0.1.12.132 cfgWlanWmeApCwMin

Contention window minimum.

Allowed values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.

Is used on the AP itself.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 1023
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.8

7.0.1.12.133 cfgWlanWmeApCwMax

Contention window maximum.

Allowed values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023

cwMax has to be greater or equal cwMin. Is used on the AP itself.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 1023
OID	1.3.6.1.4.1.16177.1.400.1.1.3.5.1.9

7.0.1.12.134 cfgWlanDbgTable

Wireless Handoff Debug Parameters.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6

7.0.1.12.135 cfgWlanDbgRatelimit

Persistent default value to enable/disable the rate limiter messages in syslog. These log messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.10

7.0.1.12.136 cfgWlanDbgLinkmonitor

Periodically sends a trap containing link information of all connected devices on this interface.

Applies to both AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.11

7.0.1.12.137 cfgWlanDbgIfaceName

Name of the virtual wireless interface.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.2

7.0.1.12.138 cfgWlanDbgHandoff

Persistent default value to enable/disable the handoff messages in syslog. These log messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.3

7.0.1.12.139 cfgWlanDbgScan

Persistent default value to enable/disable the scan messages in syslog. These log messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.4

7.0.1.12.140 cfgWlanDbgMlme

Persistent default value to enable/disable the MLME messages in syslog. These log messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.5

7.0.1.12.141 cfgWlanDbgEvents

Persistent default value to enable/disable the events messages in syslog. These log messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.6

7.0.1.12.142 cfgWlanDbgBeaconrssi

Persistent default value to enable/disable the beacon RSSI messages in syslog. These log messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.7

7.0.1.12.143 cfgWlanDbgAckrssi

Persistent default value to enable/disable the ACK RSSI messages in syslog. These log messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.8

7.0.1.12.144 cfgWlanDbgBeaconfiltered

Persistent default value to enable/disable the beacon filtered RSSI messages in syslog. These log

messages are subject to change. DO NOT PARSE!

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.6.1.9

7.0.1.12.145 cfgWlanAclWhiteTable

Wireless MAC Access Control Whitelist

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.7

7.0.1.12.146 cfgWlanAclWhiteEnabled

Enable this entry in the ACL.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.7.1.2

7.0.1.12.147 cfgWlanAclWhiteInterface

Name of the virtual wireless interface on which this entry is active.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.7.1.3

7.0.1.12.148 cfgWlanAclWhiteAddr

MAC address in the ACL.

Shall be in the format: 00:14:5a:02:10:42

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	17 - 17
OID	1.3.6.1.4.1.16177.1.400.1.1.3.7.1.4

7.0.1.12.149 cfgWlanAclWhiteMask

Mask of the MAC address to specify ranges of MAC addresses. To be used like CIDR notation of IP addresses.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 48
OID	1.3.6.1.4.1.16177.1.400.1.1.3.7.1.5

7.0.1.12.150 cfgWlanAclBlackTable

Wireless MAC Access Control Blacklist.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.8

7.0.1.12.151 cfgWlanAclBlackEnabled

Enable this entry in the ACL.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.3.8.1.2

7.0.1.12.152 cfgWlanAclBlackInterface

Name of the virtual wireless interface on which this entry is active.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.8.1.3

7.0.1.12.153 cfgWlanAclBlackAddr

MAC address in the ACL.

Shall be in the format: 00:14:5a:02:10:42

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	17 - 17
OID	1.3.6.1.4.1.16177.1.400.1.1.3.8.1.4

7.0.1.12.154 cfgWlanAclBlackMask

Mask of the MAC address to enable the use of ranges of MAC addresses. To be used like CIDR notation of IP addresses.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 48
OID	1.3.6.1.4.1.16177.1.400.1.1.3.8.1.5

7.0.1.12.155 cfgWlanGlobal

7.0.1.12.155.1 cfgWlanGlblCountry

Wireless country code.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.9.1

7.0.1.12.155.2 cfgWlanGlblLinkmonitorInterval

LinkMonitor interval.

A new trap is sent every milliseconds.

Notice: A short interval and/or numerous connections may affect system performance negatively.

Access	readwrite
Status	current
Range	200 - 60000
OID	1.3.6.1.4.1.16177.1.400.1.1.3.9.2

7.0.1.13 cfgRouting

7.0.1.13.1 cfgRouteDefault

7.0.1.13.1.1 cfgRouteDefGateway

The default gateway defines the node on an IP network that serves as a router for any other network which is not defined in the routing table.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.4.1.1

7.0.1.13.1.2 cfgRouteDefGwOverride

Override a default gateway previously received via DHCP with the value in cfgRouteDefGateway. If this is disabled and a default gateway already exists it will not be changed.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.4.1.2

7.0.1.13.1.3 cfgRouteTable

Static routes

Applies to AP and STA.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.4.2

7.0.1.13.1.4 cfgRouteTableEnabled

Enable/Disable this route entry. Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.4.2.1.2

7.0.1.13.1.5 cfgRouteTableDestinationNetwork

Destination network in CIDR notation.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
OID	1.3.6.1.4.1.16177.1.400.1.1.4.2.1.3

7.0.1.13.1.6 cfgRouteTableGateway

Gateway to destination network.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.4.2.1.5

7.0.1.13.1.7 cfgRouteTableSource

Source for traffic to destination network.

Optional. Use only if you have multiple possible sources.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.4.2.1.6

7.0.1.13.1.8 cfgMRouteTable

Static multicast routes.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3

7.0.1.13.1.9 cfgMRouteTableEnabled

Enable/Disable this multicast route entry.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.2

7.0.1.13.1.10 cfgMRouteTableInput

Input interface.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.3

7.0.1.13.1.11 cfgMRouteTableSource

Unicast source address to listen to.

If it is set to 0.0.0.0 all multicast traffic will be forwarded.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.4

7.0.1.13.1.12 cfgMRouteTableGroup

Multicast group to forward.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.5

7.0.1.13.1.13 cfgMRouteTableOutput

Output interface(s).

Can be a list of interface names separated by spaces.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.6

7.0.1.14 cfgIpTables

7.0.2 rpc

7.0.2.1 rpcConfiguration

7.0.2.1.1 rpcCfgRevert

In case there are any changes in the configuration section, which are not applied yet, they can be all reverted by writing **all(1)** to this parameter.

Reading this parameter will show the status of the last RPC. A value less than 0 means an error occurred. A value of 0 is returned if the revert process was successful.

Applies to AP and STA.

Enumeration	nop (0), all (1), allError (-1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.1.1

7.0.2.1.2 rpcCfgApply

All changes to any parameter in the configuration section have to be applied before they come into operation. To apply all new parameters to the device, set this parameter to **all(1)**.

Reading this parameter will show the status of the apply process. A value less then 0 indicates that an error occurred during the last apply process, **nop(0)** means no operation and indicates that no apply process is in operation and no error has occurred. The return value all(1) means the apply process is still running.

Applies to AP and STA.

Enumeration	nop (0), all (1), allError (-1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.1.2

7.0.2.1.3 rpcCfgReset

Reset configuration to default values.

Reading this parameter will show the status of the process. A value less than 0 indicates that an error occurred during the last apply process, **nop(0)** means no operation and indicates that no process is in operation and no error has occurred. A return value greater than 0 means the process is still running.

Applies to AP and STA.

Enumeration	nop (0), all (1), allError (-1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.1.3

7.0.2.1.4 rpcCfgFile

Export or import a configuration to or from a file respectively.

Please refer to setCfgFileUrl for more information on how to set the configuration file.

Reading this parameter will show the status of the process. A value less than 0 indicates the occurrence of an error during the last process, **nop(0)** means no operation and indicates that no process is in operation and no error has occurred. A return value greater than 0 means the process is still running.

Applies to AP and STA.

Enumeration	nop (0), export (1), import (2), errorImport (-2), errorExport (-1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.1.4

7.0.2.2 rpcFirmware

7.0.2.2.1 rpcFwFlash

Start download/flash of a new firmware.

To flash a new firmware to the device, define a valid URL accessible by the device. Change the firmware URL parameter setFwFileUrl in the settings section, if needed.

Writing **flash(2)** to this parameter will download and validate the new firmware file. if the downloaded file is recognized as a valid firmware for this device, it will be flashed to the file system of the device.

Writing **flashWithConfig(3)** to this parameter will download the firmware and the custom config defined with setCfgFileUrl and validate the new firmware file. If the download is recognized as a valid firmware for this device, it will be written to the file system of the device. The supplied custom config will be applied after the upgrade.

Reading this parameter will return the status of the firmware flash process. A value of **flashError(-2)** indicates that the flash process failed during writing. A return value of **downloadError(-1)** indicates the occurrence of an error during download or validation of the firmware/config. A value of **flash(2)** indicates that the device is currently writing the firmware to the file system.

Applies to AP and STA.

Enumeration	nop (0), download (1), flash (2), flashWithConfig (3), flashError (-2), downloadError (-1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.2.1

7.0.2.3 rpcSystem

7.0.2.3.1 rpcSysReboot

Reboot system after n seconds.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.3.3.1

7.0.2.3.2 rpcSysFactoryReset

Perform a factory reset (i.e. reset device configuration, including administrator password and HTTPS/802.1x certificates, to its default state).

Notice: You will not be able to communicate with the device until the factory reset has finished and the device has booted again.

Applies to AP and STA.

Enumeration	nop (0), reset (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.3.2

7.0.2.3.3 rpcSysErrorReset

Writing **reset(1)** to this parameter will reset all logged warning and errors of the system. The device LEDs will indicate normal operating state after result.

Applies to AP and STA.

Enumeration	nop (0), reset (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.3.3

7.0.2.3.4 rpcSysKernelLogReset

Writing **reset(1)** to this parameter will clear all kernel logs.

Reading this parameter will show the status of the process. A **nop(0)** means no operation and points out that there is no process in operation. In case the return value is greater then 0 the process is still running.

Applies to AP and STA.

Enumeration	nop (0), reset (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.3.4

7.0.2.4 rpcCertificate

7.0.2.4.1 rpcCrtFile

Import or export a HTTPS/802.1X certification/key to or from a file respectively.

Please refer to setCrtFileUrl for more information on how to set the certification/key file URL.

Reading this parameter will show the status of the process. A value less than 0 indicates that an error has occurred during the last process, **nop(0)** means no operation and points out that there is no process in operation and no error has occurred. A return value greater than 0 means the process is still running.

Applies to AP and STA.

Enumeration	nop (0), import (1), export (2), delete (3), importerror (-1), validateerror (-4), deleteerror (-3), exporterror (-2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.4.1

7.0.2.5 rpcDriver

7.0.2.5.1 rpcDrvTable

RPC driver module

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.6.1

7.0.2.5.2 rpcDrvName

Name of the radio device

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.3.6.1.1.2

7.0.2.5.3 rpcDrvDfsSimulateRadar

Simulate a radar detection on the current channel

Enumeration	nop (0), fire (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.3.6.1.1.5

7.0.3 settings

7.0.3.1 setConfiguration

7.0.3.1.1 setCfgFileUrl

The configuration file URL defines to or from which location the configuration file will be exported or imported. At the moment only TFTP protocol is supported.

Example

- tftp://192.168.1.1/device.cfg

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.4.1.1

7.0.3.2 setWireless

7.0.3.2.1 setWlanDeviceTable

Wireless hardware modules.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1

7.0.3.2.2 setWlanDevName

Name of the wireless device.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1.1.2

7.0.3.2.3 setWlanDevRfOutput

Enable/disable RF output.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1.1.3

7.0.3.2.4 setWlanDevFrequency

Wireless frequency.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1.1.6

7.0.3.2.5 setWlanDevPower

Wireless output power.

Applies to AP and STA.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1.1.8

7.0.3.2.6 setWlanDbgTable

Wireless handoff debug parameters.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6

7.0.3.2.7 setWlanDbgIfaceName

Name of the virtual wireless interface.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.2

7.0.3.2.8 setWlanDbgHandoff

Volatile setting to enable/disable the handoff messages in syslog.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.3

7.0.3.2.9 setWlanDbgScan

Volatile setting to enable/disable the scan messages in syslog.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.4

7.0.3.2.10 setWlanDbgMlme

Volatile setting to enable/disable the MLME messages in syslog.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.5

7.0.3.2.11 setWlanDbgEvents

Volatile setting to enable/disable the Events messages in syslog.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.6

7.0.3.2.12 setWlanDbgBeaconrssi

Volatile setting to enable/disable the Beacon RSSI messages in syslog.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.7

7.0.3.2.13 setWlanDbgAckrssi

Volatile setting to enable/disable the ACK RSSI messages in syslog.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.8

7.0.3.2.14 setWlanDbgBeaconfiltered

Volatile setting to enable/disable the Beacon filtered RSSI messages in syslog.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.3.6.1.9

7.0.3.3 setConfmgmtd

7.0.3.3.1 setCfgdLogLevel

Log message level, N = 0-8.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.4.4.1

7.0.3.4 setFirmware

7.0.3.4.1 setFwFileUrl

Download firmware from this URL.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.4.5.1

7.0.3.4.2 setFwKeepConfig

Try to import configuration from the previous firmware version.

Applies to AP and STA.

Enumeration	reset (0), keep (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.5.2

7.0.3.5 setCertificate

7.0.3.5.1 setCrtFileUrl

The certification/key (for HTTPS/802.1X) file-URL defines the location of the certification/key file where it will be downloaded from or uploaded to. At the moment only the TFTP protocol is supported.

Example

- tftp://192.168.1.1/sw6-uttpd.crt

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.4.6.1

7.0.3.5.2 setCrtFileSelector

Set this field to select which file should be downloaded/uploaded via the rpcCrtFile.

To disable the CA certificate verification on 802.1X write the following string into this file:

```
DISABLE CA CERTIFICATE VERIFICATION. THIS WILL ALLOW A 3RD PARTY TO CAPTURE MY PASSWORD.
```

Applies to AP and STA.

Enumeration	legacyhttps (0), httpscrt (1), httpskey (2), wlan0crt (100), wlan1crt (101), wlan0key (200), wlan1key (201), wlan0ca (300), wlan1ca (301)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.4.6.2

7.0.4 hardware

7.0.4.1 hwSystem

7.0.4.1.1 hwSysProduct

Product type.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.1.1

7.0.4.1.2 hwSysSerial

Serial number of the product.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.1.2

7.0.4.1.3 hwSysRevision

ERP revision of the product.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.1.3

7.0.4.1.4 hwSysVersion

Version of the product.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.1.4

7.0.4.2 hwBaseBoard

7.0.4.2.1 hwBbType

Product type of the base board.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.10.1

7.0.4.2.2 hwBbSerial

Serial number of the base board.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.10.2

7.0.4.2.3 hwBbRevision

ERP revision of the base board.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.10.3

7.0.4.2.4 hwBbVersion

Version of the base board.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.10.4

7.0.4.2.5 hwBbPcbId

Hardware assembly ID.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.10.5

7.0.4.2.6 hwBbAssemblyId

Hardware assembly ID.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.10.6

7.0.4.3 hwIfaceBoard

7.0.4.3.1 hwIfBrdAssembled

Interface board present or not.

Applies to AP and STA.

Enumeration	inexistent (0), present (1)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.5.11.1

7.0.4.3.2 hwIfBrdType

Product type of the interface board.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.11.2

7.0.4.3.3 hwIfBrdSerial

Serial number of the interface board.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.11.3

7.0.4.3.4 hwIfBrdRevision

ERP Revision of the interface board.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.11.4

7.0.4.3.5 hwIfBrdVersion

Version of the interface board.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.11.5

7.0.4.3.6 hwIfBrdPcbId

Hardware assembly ID.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.11.6

7.0.4.3.7 hwIfBrdAssemblyId

Hardware assembly ID.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.11.7

7.0.4.4 hwNetwork

7.0.4.4.1 hwNetEthernetTable

Ethernet network interfaces

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.5.2.1

7.0.4.4.2 hwNetEthName

Name of the ethernet interface.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.2.1.1.2

7.0.4.4.3 hwNetEthAssembled

Ethernet interface present or not.

Applies to AP and STA.

Enumeration	inexistent (0), present (1)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.5.2.1.1.3

7.0.4.4.4 hwNetEthMacAddress

Ethernet MAC address..

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.2.1.1.4

7.0.4.4.5 hwNetEthOperation

Ethernet interface plugged or unplugged.

Applies to AP and STA.

Enumeration	down (0), up (1)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.5.2.1.1.5

7.0.4.4.6 hwNetEthSpeed

Ethernet speed.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.2.1.1.6

7.0.4.4.7 hwNetEthHwIndex

The physical address of the Ethernet interface of the base board, since not all products are assembled the same way this is to describe how the wiring is done.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.2.1.1.7

7.0.4.5 hwSensor

7.0.4.5.1 hwSensorTable

Hardware sensor information table.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.5.21.1

7.0.4.5.2 hwSensorName

Name of the hardware sensor.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.21.1.1.2

7.0.4.5.3 hwSensorUnit

Unit of the hardware sensor.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.21.1.1.3

7.0.4.5.4 hwSensorValue

Value of the hardware sensor.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.21.1.1.4

7.0.4.6 hwWireless

7.0.4.6.1 hwWlanDeviceTable

Hardware information of the wireless LAN devices.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1

7.0.4.6.2 hwWlanDevAntennaProfileId

Antenna profile ID.

Please check the user manual for antenna details.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.10

7.0.4.6.3 hwWlanDevAntennaGain

Antenna gain in dBi.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.11

7.0.4.6.4 hwWlanDevCableLoss

Cable loss in dB.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.12

7.0.4.6.5 hwWlanDevAssembled

Wireless device present or not.

Applies to AP and STA.

Enumeration	inexistent (0), present (1)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.2

7.0.4.6.6 hwWlanDevType

Type of the wireless device.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.3

7.0.4.6.7 hwWlanDevSerial

Serial number / customer field.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.4

7.0.4.6.8 hwWlanDevRevision

ERP revision of the RF board.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.5

7.0.4.6.9 hwWlanDevVersion

Version of the RF board.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.6

7.0.4.6.10 hwWlanDevPcbId

Hardware assembly ID.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.7

7.0.4.6.11 hwWlanDevAssemblyId

Hardware assembly ID.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.8

7.0.4.6.12 hwWlanDevMacAddress

MAC address.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.3.1.1.9

7.0.4.6.13 hwWlanGlobal

7.0.4.6.13.1 hwWlanGlblRegulatoryRegionId

Regulatory region ID.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.5.3.2.2

7.0.5 software

7.0.5.1 swFirmware

7.0.5.1.1 swFwName

Firmware name.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.2.1

7.0.5.1.2 swFwVersion

Firmware name.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.2.2

7.0.5.1.3 swFwRevision

Firmware name.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.2.3

7.0.5.2 swBootloader

7.0.5.2.1 swBootName

Name of the bootloader.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.20.1

7.0.5.2.2 swBootVersion

Version of the bootloader.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.20.2

7.0.5.2.3 swBootBuildDate

Date when the bootloader was built.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.20.3

7.0.5.3 swSystem

7.0.5.3.1 swSysRebootReason

Reason for the reboot of the system.

Applies to AP and STA.

Enumeration	coldstart (0), unknown (9), watchdog (2), oops (3), warmstart (1)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.6.3.1

7.0.5.3.2 swSysMessageTable

System messages (e.g. errors, warnings).

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.6.3.100

7.0.5.3.3 swSysMsgPriority

Message priority/level.

Applies to AP and STA.

Enumeration	emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), debug (7)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.1.6.3.100.1.2

7.0.5.3.4 swSysMsgCode

Message code.

Applies to AP and STA.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.3.100.1.3

7.0.5.3.5 swSysMsgText

Message.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.3.100.1.4

7.0.5.4 swConfiguration

7.0.5.4.1 swCfgChangesCount

Number of not yet applied device configuration changes.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.30.1

7.0.5.5 swOperatingSystem

7.0.5.5.1 swOsName

Operating system name.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.4.1

7.0.5.5.2 swOsVersion

Operating system version.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.4.2

7.0.5.5.3 swOsRevision

Operating system revision.

Applies to AP and STA.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.4.3

7.0.5.5.4 swOsUptime

Up time of the operating system.

Applies to AP and STA.

Access	readonly
Status	current
Type	TimeTicks
OID	1.3.6.1.4.1.16177.1.400.1.6.4.4

7.0.5.6 swDriver

7.0.5.6.1 swDrvDfsTable

DFS driver statistics

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.6.5.1

7.0.5.6.2 swDrvDfsName

Name of the wireless device.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.5.1.1.2

7.0.5.6.3 swDrvDfsPulsesDetected

Pulses detected by the wireless device.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.1.1.3

7.0.5.6.4 swDrvDfsPulsesProcessed

Pulses processed by the wireless device.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.1.1.4

7.0.5.6.5 swDrvDfsRadarDetected

Radar sequences detected by the wireless device.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.1.1.5

7.0.5.6.6 swDrvCntWlanMacTable

Wireless MAC layer statistics.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4

7.0.5.6.7 swDrvCntWlanMacRxHandlersDrop

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.10

7.0.5.6.8 swDrvCntWlanMacRxHandlersQueued

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.11

7.0.5.6.9 swDrvCntWlanMacRxHandlersDropNullfunc

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.12

7.0.5.6.10 swDrvCntWlanMacRxHandlersDropDefrag

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.13

7.0.5.6.11 swDrvCntWlanMacRxHandlersDropShort

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.14

7.0.5.6.12 swDrvCntWlanMacTxExpandSkbHead

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.15

7.0.5.6.13 swDrvCntWlanMacTxExpandSkbHeadCloned

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.16

7.0.5.6.14 swDrvCntWlanMacRxExpandSkbHead

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.17

7.0.5.6.15 swDrvCntWlanMacRxExpandSkbHead2

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.18

7.0.5.6.16 swDrvCntWlanMacRxHandlersFragments

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.19

7.0.5.6.17 swDrvCntWlanMacName

Name of the wireless device.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.2

7.0.5.6.18 swDrvCntWlanMacTxstatusDrop

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.20

7.0.5.6.19 swDrvCntWlanMacTxHandlersDrop

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.3

7.0.5.6.20 swDrvCntWlanMacTxHandlersQueued

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.4

7.0.5.6.21 swDrvCntWlanMacTxHandlersDropUnencrypted

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.5

7.0.5.6.22 swDrvCntWlanMacTxHandlersDropFragment

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.6

7.0.5.6.23 swDrvCntWlanMacTxHandlersDropWep

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.7

7.0.5.6.24 swDrvCntWlanMacTxHandlersDropNotAssoc

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.8

7.0.5.6.25 swDrvCntWlanMacTxHandlersDropUnauthPort

MAC debug entry.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.4.1.9

7.0.5.6.26 swDrvCntWlanWmmTable

WMM statistics.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.6.5.6

7.0.5.6.27 swDrvCntWlanWmmName

Name of the queue.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.5.6.1.2

7.0.5.6.28 swDrvCntWlanWmmTx

Number of frames sent in this queue.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.6.1.3

7.0.5.6.29 swDrvCntWlanWmmRx

Number of frames received in this queue.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.6.1.4

7.0.5.6.30 swDrvCntWlanWmmShortRetries

Number of retries for frames shorter than RTS.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.6.1.5

7.0.5.6.31 swDrvCntWlanWmmLongRetries

Number of retries for frames longer than RTS.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.6.1.6

7.0.5.6.32 swDrvCntWlanWmmExceededRetries

Number of failed transmissions due to exceeding of the retry limit.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.6.1.7

7.0.5.6.33 swDrvConStatWlanIf

WLAN interface selector for swDrvConStatTable

Access	readwrite
Status	current
Type	DisplayString
Range	4 - 5
OID	1.3.6.1.4.1.16177.1.400.1.6.5.7

7.0.5.6.34 swDrvConStatTable

Connection Status Information.

Status	current
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8

7.0.5.6.35 swDrvConStatTxBrType

Station tx bitrate type.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.10

7.0.5.6.36 swDrvConStatTxBrValue

Station tx bitrate value.

Multiplied by 10 if swDrvConStatTxBrType is ‘legacy’.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.11

7.0.5.6.37 swDrvConStatTxBytes

Station tx bytes.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.12

7.0.5.6.38 swDrvConStatTxPackets

Station tx packets.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.13

7.0.5.6.39 swDrvConStatSigChain0

Station signal chain 0.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.14

7.0.5.6.40 swDrvConStatSigChain1

Station signal chain 1.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.15

7.0.5.6.41 swDrvConStatSigChain2

Station signal chain 2.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.16

7.0.5.6.42 swDrvConStatSigAvgChain0

Station signal average chain 0.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.17

7.0.5.6.43 swDrvConStatSigAvgChain1

Station signal average chain 1.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.18

7.0.5.6.44 swDrvConStatSigAvgChain2

Station signal average chain 2.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.19

7.0.5.6.45 swDrvConStatWlanName

WLAN interface name.

Access	readonly
Status	current
Type	DisplayString
Range	4 - 5
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.2

7.0.5.6.46 swDrvConStatTxRetries

Station tx retries.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.20

7.0.5.6.47 swDrvConStatTxFailed

Station tx failed.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.21

7.0.5.6.48 swDrvConStatCacheNo

Station Dump Cache Access Number.

The cache gets refreshed if it is older than 5 seconds.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.22

7.0.5.6.49 swDrvConStatMacName

Station MAC address.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 17
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.3

7.0.5.6.50 swDrvConStatRxBrExtra

Station rx bitrate extra.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.4

7.0.5.6.51 swDrvConStatRxBrType

Station rx bitrate type.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.5

7.0.5.6.52 swDrvConStatRxBrValue

Station rx bitrate value.

Multiplied by 10 if swDrvConStatRxBrType is ‘legacy’.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.6

7.0.5.6.53 swDrvConStatRxBytes

Station rx bytes.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.7

7.0.5.6.54 swDrvConStatRxPackets

Station rx packets.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.8

7.0.5.6.55 swDrvConStatTxBrExtra

Station tx bitrate extra.

Access	readonly
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.1.6.5.8.1.9

7.0.5.7 swRdm

7.0.5.7.1 swRdmMaxEirp

Maximal equivalent isotropically radiated power (EIRP) in dBm.

This value shows the maximal aggregated transmit power over all configured chains.

Applies to AP.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.6.1

7.0.5.7.2 swRdmMaxApp

Maximal antenna port power in dBm.

This value shows the maximal transmit power of a single chain.

Applies to AP.

Access	readonly
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.1.6.6.2

8 WESTERMO-SW6-FIREWALL-MIB

8.0.1 firewall

8.0.1.1 configuration

8.0.1.1.1 cfgFwEnabled

Firewall disabled or enabled.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.1.1.1

8.0.1.1.2 cfgFwNat

8.0.1.1.2.1 cfgFwNatPortForwardTable

Firewall port forward rules table.

Status	current
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1

8.0.1.1.2.2 cfgFwNatPrtFwdDestinationPortEnd

Destination end port to redirect.

When forwarding multiple port, this value is the end of the range. Set to -1 if no range is forwarded. Can only be used with TCP, UDP or TCP/UDP.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 65535
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.10

8.0.1.1.2.3 cfgFwNatPrtFwdRedirectDestinationAddress

Redirect traffic to this redirection destination address.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.11

8.0.1.1.2.4 cfgFwNatPrtFwdRedirectDestinationPort

Redirect traffic to this destionation port.

Can only be used with TCP, UDP or TCP/UDP.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 65535
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.12

8.0.1.1.2.5 cfgFwNatPrtFwdEnabled

Disable or enable the rule.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.2

8.0.1.1.2.6 cfgFwNatPrtFwdInterface

Name of the network interface on which the rule applies.

Defines on which interface traffic is comming in. Groups of interfaces can be matched by adding the character '+' at the end. E.g. eth+ to match the interfaces eth0, eth1 and eth2. To match all interfaces

use the character '+' alone.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.3

8.0.1.1.2.7 cfgFwNatPrtFwdProtocol

Choose which IP protocol the rule matches.

Allowed protocols are:

- **any(0):** Any ip protocol.
- **udp(1):** Only UDP protocol.
- **tcp(2):** Only TCP protocol.
- **udptcp(3):** UDP and TCP protocol.

Applies to AP and STA.

Enumeration	any (0), udp (1), tcp (2), udptcp (3)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.4

8.0.1.1.2.8 cfgFwNatPrtFwdSourceAddress

Source address to match.

This can be a specific ip address or a range in CIDR notation. Set to 0.0.0.0/0 to match all inbound traffic. Set to 172.17.29.7/32 to match the specific IP 172.17.29.7 You can use ! to invert the sense of the rule: E.g. !192.168.0.0/24

Notice: Usually you want 0.0.0.0/0.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	9 - 19
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.5

8.0.1.1.2.9 cfgFwNatPrtFwdSourcePortStart

Source start port to match.

Specify the port or start of a port range from which a connection originates. Can only be used with TCP, UDP or TCP/UDP. Leave this on -1 to disable. You can use ! to invert the sense of the rule: E.g. !80. When used in a range, the inversion applies to the range.

Notice: Usually you want this disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 6
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.6

8.0.1.1.2.10 cfgFwNatPrtFwdSourcePortEnd

Destination end port to match.

When matching multiple port, this value is the end of the range. Set to -1 if no range is to be matched. Can only be used with TCP, UDP or TCP/UDP.

Notice: Usually you want this disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 65535
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.7

8.0.1.1.2.11 cfgFwNatPrtFwdDestinationAddress

Destination address to redirect.

This can be a specific ip address or a range in CIDR notation. Set to 0.0.0.0/0 to match all inbound traffic on the interface specified in cfgFwNatPrtFwdInterface. You can use ! to invert the sense of the rule: E.g. !192.168.0.0/24. When using static IPs set this to the configured address of the respective interface or alias you want to forward.

Be aware, that setting 0.0.0.0/0 will redirect everything arriving on the configured interface, even if not sent to the device itself.

Notice: Leave this on 0.0.0.0/0 when using DHCP.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	9 - 19
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.8

8.0.1.1.2.12 cfgFwNatPrtFwdDestinationPortStart

Destionation start port to redirect.

Specify the port or start of a port range for the destination. You can use ! to invert the sense of the rule: E.g. !80. When used in a range, the inversion applies to the range. Can only be used with TCP, UDP or TCP/UDP.

Applies to AP and STA.

Access	readwrite
Status	current
Range	0 - 65535
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.9

8.0.1.1.2.13 cfgFwNatOutboundTable

Firewall outbound NAT rules table

Status	current
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2

8.0.1.1.2.14 cfgFwNatOutDestinationPortEnd

Destination end port to match.

When forwarding multiple port, this value is the end of the range. Set to -1 if no range is forwarded. Can only be used with TCP, UDP or TCP/UDP.

Notice: Usually you want this disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 65535
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.10

8.0.1.1.2.15 cfgFwNatOutSourceRewriteAddress

Redirect traffic to this redirection destination address.

Set the address with which outbound traffic shall be rewritten. In case you are using DHCP leave this on 0.0.0.0.

Notice: If you are not rewriting the source to a specific aliases you can leave this on 0.0.0.0 as well to automatically rewrite to the configured main address of the interface.

Applies to AP and STA.

Access	readwrite
Status	current
Type	IpAddress
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.11

8.0.1.1.2.16 cfgFwNatOutSourceRewritePort

Redirect traffic to this destionation port.

Can only be used with TCP, UDP or TCP/UDP. Set to -1 to disable source port rewrite.

Notice: Usually you want this disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 65535
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.12

8.0.1.1.2.17 cfgFwNatOutEnabled

Disable or enable the rule.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.2

8.0.1.1.2.18 cfgFwNatOutInterface

Name of the network interface on which the rule applies.

Matches traffic leaving on this interface. Needs to be set to an interface name if you are using DHCP. Set to -1 if you don't know on which interface traffic will be leaving. Match the traffic with cfgFwNatOutDestinationAddress instead. You can use ! to invert the sense of the rule. E.g. !wlan0.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.3

8.0.1.1.2.19 cfgFwNatOutProtocol

Choose which IP protocol the rule matches.

Allowed protocols are:

- **any(0):** Any ip protocol.
- **udp(1):** Only UDP protocol.
- **tcp(2):** Only TCP protocol.
- **udptcp(3):** UDP and TCP protocol.

Applies to AP and STA.

Enumeration	any (0), udp (1), tcp (2), udptcp (3)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.4

8.0.1.1.2.20 cfgFwNatOutSourceAddress

Source address to match.

This can be a specific ip address or a range in CIDR notation. Set to 0.0.0.0/0 to match all inbound traffic. Set to 172.17.29.7/32 to match the specific IP 172.17.29.7. You can use ! to invert the sense of the rule: E.g. !192.168.0.0/24.

Notice: Usually you want 0.0.0.0/0.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	9 - 19
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.5

8.0.1.1.2.21 cfgFwNatOutSourcePortStart

Source start port to match.

Specify the port or start of a port range from which a connection originates. Can only be used with TCP, UDP or TCP/UDP. Leave this on -1 to disable. You can use ! to invert the sense of the rule: E.g. !80. When used in a range, the inversion applies to the range.

Notice: Usually you want this disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 6
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.6

8.0.1.1.2.22 cfgFwNatOutSourcePortEnd

Destination end port to match.

When matching multiple port, this value is the end of the range. Set to -1 if no range is to be matched. Can only be used with TCP, UDP or TCP/UDP.

Notice: Usually you want this disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Range	-1 - 65535
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.7

8.0.1.1.2.23 cfgFwNatOutDestinationAddress

Destination address to match.

This can be a specific ip address or a range in CIDR notation. Set to 0.0.0.0/0 to match all outbound traffic on the interface specified in cfgFwNatOutInterface. You can use ! to invert the sense of the

rule: E.g. !192.168.0.0/24.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	9 - 19
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.8

8.0.1.1.2.24 cfgFwNatOutDestinationPortStart

Destionation start port to match.

Specify the port or start of a port range for the destination. Can only be used with TCP, UDP or TCP/UDP. You can use ! to invert the sense of the rule: E.g. !80. When used in a range, the inversion applies to the range.

Notice: Usually you want this disabled.

Applies to AP and STA.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 6
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.9

9 WESTERMO-SW6-ICL-MIB

9.0.1 icl

9.0.1.1 configuration

9.0.1.1.1 cfgIcl

9.0.1.1.1.1 cfgIclEnabled

Enable Inter-Carriage Link application.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.1

9.0.1.1.1.2 cfgIclConnectionDelay

Connection delay after a potential ICL partner was first detected.

This value in conjunction with cfgIclCycleTime defines how extensively a potential ICL partner is monitored and analyzed before a connection is established.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 600
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.2

9.0.1.1.1.3 cfgIclConnectionThreshold

This value defines the minimum signal level necessary for the ICL application to start evaluating a potential ICL partner.

Applies to AP.

Access	readwrite
Status	current
Range	-90 - 0
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.3

9.0.1.1.1.4 cfgIclDisconnectionDelay

Disconnection delay in seconds defines how quickly a connected ICL pair resets to scanning mode after after the current ICL partner reaches a low signal level or gets disconnected.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 600
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.4

9.0.1.1.1.5 cfgIclDisconnectionThreshold

This value defines the minimum signal level necessary for a ICL pair to stay connected. If the singal level drops below this level for longer than in cfgIclDisconnectionDelay specified, the ICL application will revert the device do access point and resume scans for a new partner.

Applies to AP.

Access	readwrite
Status	current
Range	-90 - 0
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.5

9.0.1.1.1.6 cfgIclInterfaceName

This value describes the interface the ICL Application will use for its services.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.6

9.0.1.1.1.7 cfgIclCycleTime

Interval of background scans in seconds.

This value in conjunction with cfgIclConnectionDelay defines how extensively a potential ICL partner is monitored and analyzed before a connection is established.

Applies to AP.

Access	readwrite
Status	current
Range	2 - 60
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.7

9.0.1.1.1.8 cfgIclBlacklistTime

Duration of blacklisting in seconds.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 3600
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.8

9.0.1.2 rpc

9.0.1.2.1 rpcIcl

9.0.1.2.1.1 rpcIclForceDisconnect

Force the device to disconnect from the current ICL partner and resume background scanning for a new partner.

Enumeration	nop (0), disconnect (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.5.3.1.1

9.0.1.2.1.2 rpcIclClearBlacklist

Clear all currently blacklisted entries.

Enumeration	nop (0), clear (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.5.3.1.2

9.0.1.3 software

9.0.1.3.1 swIcl

9.0.1.3.1.1 swIclStatus

Current status of ICL application.

- **scanning(1):** Scanning indicates Access Point mode with background scanning activated.
- **connected(2):** Connected indicates a connection with an ICL partner is established and background scanning is disabled.

Enumeration	disabled (0), scanning (1), connected (2)
Access	readonly
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.5.6.1.1

10 WESTERMO-SW6-NWM-MIB

10.0.1 nwm

10.0.1.1 configuration

10.0.1.1.1 cfgHttpReport

10.0.1.1.1.1 cfgHttpRprtServerUrl

URL of the remote server where DFS / IDF reports are sent to.

Format: http://:/

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.2.3.1.1.1

10.0.1.1.2 cfgScanWorker

10.0.1.1.2.1 cfgScnWrkEnabled

Enable the ScanWorker.

ChannelManager or IDF both depend on ScanWorker.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.1.2.1

10.0.1.1.3 cfgChannelManager

10.0.1.1.3.1 cfgChMgrEnabled

Enable the ChannelManager.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.1.3.1

10.0.1.1.3.2 cfgChMgrUsableFrequencyList

Configure which frequency list is to be used as 'list of usable frequencies' by the ChannelManager. A value of -1 means no list defined using all frequencies available in current country.

Access	readwrite
Status	current
Range	-1 - 23
OID	1.3.6.1.4.1.16177.1.400.2.3.1.3.2

10.0.1.1.3.3 cfgChMgrDfsUseNvram

When 'enabled' the DFS states will be load / stored from / to the non-volatile ram device.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.1.3.3

10.0.1.1.4 cfgNwm

10.0.1.1.4.1 cfgNwmEnabled

Enable the Wireless Manager.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.1.4.1

10.0.1.1.5 cfgIdf

10.0.1.1.5.1 cfgIdfEnabled

Enable Interference Detection Function.

IDF is only supported for devices with two radios.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.1

10.0.1.1.5.2 cfgIdfScanWorkTable

Table of scan works items.

Applies to AP.

Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.10

10.0.1.1.5.3 cfgIdfScanWorkFreq

Center frequency in MHz of the channel to scan.

Set center frequency to 0 to disable this scan work item and all following items.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 6100
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.10.1.2

10.0.1.1.5.4 cfgIdfScanWorkAction

Scan Work Action of the interference function.

The following scan work actions are available:

none(0)

Scan work item and all following items of the table are ignored.

spectral(2)

Spectral data are collected from Antenna port 3 and spectral statistics is generated at the end of the scan work item. During a Spectral Scan Work the raw spectral data can be retrieved from the AP. Please refer to the Software User Manual for more information.

radar(3)

Runs the radar detection engine and counts all radar sequences detected by the monitor wireless device on Antenna port 3.

wifi(4)

Wifi data are collected from Antenna port 3 and wifi statistics is generated at the end of the scan work item.

Applies to AP.

Enumeration	none (0), spectral (2), radar (3), wifi (4)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.10.1.3

10.0.1.1.5.5 cfgIdfScanWorkSeconds

Duration of the Scan Work Item in seconds.

At the end of the Scan Work a JSON formatted Report is generated and buffered. Set scan work time to 0 to disable this scan work item and all following items.

Applies to AP.

Access	readwrite
Status	current
Range	0 - 86400
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.10.1.4

10.0.1.1.5.6 cfgIdfInterval

Report interval in seconds.

This value defines the interval when all available Reports are sent to the URL defined in cfgIdfHttpReportUrl.

Applies to AP.

Access	readwrite
Status	current
Range	1 - 86400
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.3

10.0.1.1.5.7 cfgIdfName

IDF Name.

Can be used to set an unique identifier for the reports.

Applies to AP.

Access	readwrite
Status	current
Type	DisplayString
Range	1 - 255
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.4

10.0.1.1.5.8 cfgIdfTrigger

cfgIdfTrigRadarCntTh

IDF trigger radar_count.

Defines the number of radar events to trigger a report.

Access	readwrite
Status	current
Type	Integer32
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.5.1

cfgIdfTrigChanLoadTh

IDF trigger channel_load.

Defines the channel load ratio in percent to trigger a report.

Access	readwrite
Status	current
Range	0 - 100
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.5.2

cfgIdfTrigAlienLoadTh
IDF trigger alien_load.

Defines the ratio of alien channel load in percent to trigger a report.

Access	readwrite
Status	current
Range	0 - 100
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.5.3

cfgIdfTrigDomLoadTh
IDF trigger domestic_load.

Defines the ratio of domestic channel load in percent to trigger a report.

Access	readwrite
Status	current
Range	0 - 100
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.5.4

cfgIdfTrigAlienMaxRssiTh
IDF trigger alien_avg_rssi.

Defines the average RSSI of alien traffic to trigger a report.

Access	readwrite
Status	current
Range	0 - 127
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.5.5

cfgIdfTrigDomMaxRssiTh
IDF trigger domestic_avg_rssi.

Defines the average RSSI of domestic traffic to trigger a report.

Access	readwrite
Status	current
Range	0 - 127
OID	1.3.6.1.4.1.16177.1.400.2.3.1.5.5.6

10.0.1.2 rpc

10.0.1.2.1 rpcChannelManager

10.0.1.2.1.1 rpcChMgrHttpReport

Requests a HTTP report from the Channel Manager.

Enumeration	nop (0), freqstate (1), channels (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.3.1.1

10.0.1.2.2 rpcNwm

10.0.1.2.2.1 rpcNwmHttpReport

Requests a HTTP report from the Wireless Manager.

Enumeration	nop (0), status (1), freqstate (2)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.3.2.1

10.0.1.2.3 rpcNvram

10.0.1.2.3.1 rpcNvramFreqStatesReset

Resets the state of DFS frequencies in the Available Channel List which is stored in non-volatile memory.

The device performs a reboot after resetting the state of the frequencies. The behaviour is similar to a factory reset but does only reset the Available Channel List.

Enumeration	reset (0)
Access	readwrite
Status	current
OID	1.3.6.1.4.1.16177.1.400.2.3.3.3.1

Message Codes

Variable text, inserted at the time the message is created, is displayed using the place holder '<val>'.

10.0.1.3 [0]

```
INFO 0 <val>
```

Manual or WebGUI Log Reset.

10.0.1.4 [100]

```
ERROR 100 SYS_MON: Voltage sensor '<val>' is out of range <val> / [<val>, <val
    ↪ >]
```

This trap is sent when supply voltage or one of the internal voltages are outside specified limits which are hardware dependent.

10.0.1.5 [101]

```
ERROR 101 SYS_MON: Temperature sensor '<val>' is out of range <val> / [<val>,
    ↪ <val>]
```

This trap is sent when internally measured temperature is outside specified limits which are hardware dependent.

10.0.1.6 [105]

```
CRITICAL 105 SYS_MON: Failure by reading value <val>. This value isn't
    ↪ monitored anymore
```

This trap is sent when internally a value couldn't read.

10.0.1.7 [130]

```
INFO 130 <val>|<val>|<val>||<val>|<val>|<val>|<val>|<val>|<val>||<val>|<val>|<
    ↪ val>|<val>|<val>|<val>|<val>|<val>||<val>|<val>|<val>|<val>
```

This message is sent periodically containing current 'iw <iface> station dump'. Format is 'interface|mac|inactive time||rx bytes|rx packets|tx bytes|tx packets|tx retries|tx failed||signal combined|avg signal combined|signal ch0|avg signal ch0|signal ch1|avg signal ch1|signal ch2|avg signal ch2||rx bitrate mode|rx bitrate value|tx bitrate mode|tx bitrate value'.

10.0.1.8 [131]

```
INFO 131 <val>|<val>|<val>|<val>|<val>|<val>|<val>|<val>|<val>|<val>|<val>
```

This message is sent periodically containing counters of the wireless interface. Format: 'NofStations|TxPackets|RetryCount|6Mbps|9Mbps|..|54Mbps'.

10.0.1.9 [200]

```
NOTICE 200 Device has restarted because of <val>
```

This message is sent at boot-up process. RESET CAUSE can be either coldstart, warmstart, watchdog and oops.

10.0.1.10 [201]

```
NOTICE 201 System startup
```

This message is sent when the system starts up.

10.0.1.11 [202]

```
NOTICE 202 Firmware update started
```

This message is sent when a firmware update is initiated.

10.0.1.12 [203]

```
NOTICE 203 System reboot
```

This message is sent when a system reboot is issued.

10.0.1.13 [204]

```
INFO 204 Reserved
```

10.0.1.14 [205]

```
NOTICE 205 Factory Reset confirmed, System configuration changed
```

This message is sent whenever the system configuration is changed.

10.0.1.15 [206]

```
NOTICE 206 Reserved
```

10.0.1.16 [207]

```
WARNING 207 Invalid upgrade image for this platform.
```

10.0.1.17 [208]

```
ERROR 208 Corrupt firmware package!
```

10.0.1.18 [209]

```
ERROR 209 Transfer firmware to device failed!
```

10.0.1.19 [210]

```
WARNING 210 Decryption of the upgrade image failed!
```

10.0.1.20 [220]

```
NOTICE 220 Start writing device identification memory!
```

10.0.1.21 [221]

```
NOTICE 221 Device identification memory successfully updated!
```

10.0.1.22 [222]

```
CRITICAL 222 Failed to update device identification memory!
```

10.0.1.23 [300]

```
WARNING 300 NTP: time synchronization failed!
```

This message is generated when ntp client is configured in unicast mode and it failed to connect to NTP server.

10.0.1.24 [310]

```
NOTICE 310 Reserved
```

10.0.1.25 [320]

```
ERROR 320 BIST: Daemon '<val>' isn't running, recover it
```

This message is generated when process with name process is not running and has to be restarted by the bist

10.0.1.26 [321]

```
ERROR 321 BIST: Daemon watchdog is not running - force restart
```

This message is generated when watchdog process is not running. System reboots afterwards.

10.0.1.27 [322]

```
CRITICAL 322 Critical hardware failure: <val>
```

This message is generated when a critical hardware failure was detected during boot up. Please read the user manual about the "Support File".

10.0.1.28 [323]

```
ERROR 323 Kernel log(s) found
```

This message is generated when a kernel log(s) was found during boot up. Please read the user manual about the "Support File".

10.0.1.29 [332]

```
INFO 332 BBMON: icmp target <val> is down.
```

This message is generated when the icmp target on the backbone is detected as down.

10.0.1.30 [333]

```
INFO 333 BBMON: icmp target <val> is up.
```

This message is generated when the icmp target on the backbone is detected as up.

10.0.1.31 [400]

```
INFO 400 <val>: Station is associated
```

This message is used to trigger led status

10.0.1.32 [401]

```
INFO 401 <val>: Station is disassociated, Reason: <val>
```

This message is used to trigger led status

10.0.1.33 [402]

```
INFO 402 <val>: Station is authorized
```

This message is used to trigger various daemons.

10.0.1.34 [403]

```
NOTICE 403 WLAN: Authentication failure
```

10.0.1.35 [404]

```
NOTICE 404 WLAN: Association failure
```

10.0.1.36 [405]

```
NOTICE 405 Reserved
```

10.0.1.37 [406]

```
ERROR 406 WLAN: Max number of station exceeded
```

10.0.1.38 [407]

```
ERROR 407 Reserved
```

10.0.1.39 [413]

```
WARNING 413 Switched to secondary SSID |<val>|
```

10.0.1.40 [430]

```
NOTICE 430 TS|<val>|<val>|RSSI_BCN|<val>
```

Format: 'TS|<timestamp>|<bssid>|RSSI BCN|<rssi>'

10.0.1.41 [432]

```
NOTICE 432 Reserved
```

10.0.1.42 [433]

```
INFO 433 WLAN: Low RSSI event: <val>
```

This event is used to trigger various daemons.

10.0.1.43 [435]

```
ERROR 435 Radius <val> server <val>:<val> not available (reason <val>)
```

AP: Radius server not available/invalid shared secret/connection rejected. Format: Radius <authentication, accounting> server <ip>:<port> not available (reason: <not available>, <shared secret>, <rejected>)

10.0.1.44 [436]

```
ERROR 436 (T)TLS Authentication started
```

STA: Full (T)TLS authentication has been started

10.0.1.45 [437]

```
ERROR 437 Certificate <val> is <val>
```

STA: T(TLS) certificate errors. Format: Certificate <ca, client> is <wrong, missing, expired>

10.0.1.46 [438]

```
ERROR 438 TTLS: Invalid username and/or password
```

STA: TTLS Username and/or password is not recognized by radius server

10.0.1.47 [500]

```
CRITICAL 500 CONFIG: Unable to connect to IPC system (ubus)!
```

10.0.1.48 [501]

```
CRITICAL 501 CONFIG: Unable to read from UCI!
```

10.0.1.49 [510]

```
ERROR 510 CONFIG: Invalid configuration, reverting to previous configuration!
```

10.0.1.50 [511]

```
ERROR 511 CONFIG: Unable to save new configuration!
```

10.0.1.51 [512]

```
CRITICAL 512 CONFIG: Unable to apply previous configuration!
```

10.0.1.52 [513]

```
WARNING 513 CONFIG: Unable to set config parameter: <val>
```

Warning for configuration import.

10.0.1.53 [514]

```
ERROR 514 CONFIG: <val>
```

Error detected during configuration validation.

10.0.1.54 [515]

```
ERROR 515 CONFIG: Invalid WLAN operation mode: <val>
```

Some devices may not support all operation modes. Please check the datasheet of the device.

10.0.1.55 [516]

```
WARNING 516 Country code <val> not supported on this product/revision!
```

Use this message when country code has ss control on=false but SS CONTROL is not supported

10.0.1.56 [530]

```
ERROR 530 PENDING CHANGES: <val>
```

10.0.1.57 [531]

```
ERROR 531 System upgrade to a major version other than 6 is not supported.
```

10.0.1.58 [532]

```
ERROR 532 'Keep config' on a system downgrade is not supported.
```

10.0.1.59 [533]

```
CRITICAL 533 Config manipulation for an upgrade failed. This is not
   ↪ correctable situation. Do a factory reset.
```

10.0.1.60 [540]

```
ERROR 540 Failed to verify key or certificate file.
```

10.0.1.61 [580]

```
ERROR 580 CONFIG FILE: Transfer failed!
```

10.0.1.62 [581]

```
WARNING 581 CONFIG FILE: <val>
```

10.0.1.63 [582]

```
ERROR 582 CONFIG FILE: Unable to read or parse!
```

10.0.1.64 [583]

```
ERROR 583 CONFIG FILE: Incorrect encryption key!
```

10.0.1.65 [585]

```
ERROR 585 Certificate import/export failed!
```

10.0.1.66 [605]

```
ERROR 605 <val>: could not send report to <val>
```

10.0.1.67 [700]

```
ERROR 700 NET: Configuration failed!
```

This message is sent if the network couldn't be set up. Possible reason are wrong protocol, missing or invalid netmask or ip address.

10.0.1.68 [701]

```
WARNING 701 NET: Configuration failed, but try to continue anyway.
```

This message is sent if the network couldn't be set up. Possible reason are the interface we try to configure does not exist.

10.0.1.69 [710]

```
ERROR 710 NET: Unable to set the default gateway!
```

This message is sent if the default gateway couldn't be set properly. This happens if the destination can not be reached, or no matching subnet exist.

10.0.1.70 [711]

```
WARNING 711 NET: Unable to set the default gateway!
```

This message is sent if the default gateway couldn't be set properly. This can happen if the default gateway is already set by DHCP.

10.0.1.71 [712]

```
ERROR 712 NET: Unable to set a static route!
```

This message is sent when an static route couldn't be set.

10.0.1.72 [713]

```
WARNING 713 NET: Unable to set a static route!
```

This message is sent when an static route couldn't be set.

10.0.1.73 [720]

```
ERROR 720 NET: Wireless configuration failed!
```

This message is sent when the configuration manager is not able to set up a wireless interface.

10.0.1.74 [721]

```
ERROR 721 NET: A wireless interface can not be bridged to an eth without 4addr
    ↪  mode!
```

This message is sent when the configuration manager is not able to set up a wireless interface because of missing 4addr mode.

10.0.1.75 [730]

```
ERROR 730 NET: Creation of IP address failed! Probably the IP/netmask is
    ↪ invalid.
```

This message is sent if an ip couldn't be set up. Possible reason are missing or invalid netmask or ip address.

10.0.1.76 [731]

```
WARNING 731 NET: The interface <val> to create the IP address on doesn't exist.
    ↪
```

This message is sent if the parent interface for an ip doesn't exist.

10.0.1.77 [732]

```
WARNING 732 NET: The interface <val> is not a valid interface to create an IP
    ↪ address on.
```

This message is sent if the parent interface for an ip is not valid (e.g. it's bridged).

10.0.1.78 [740]

```
ERROR 740 NET: Creation of VLAN failed!
```

This message is sent if the creation of a vlan failed.

10.0.1.79 [741]

```
WARNING 741 NET: Parent interface missing for VLAN.
```

This message is sent if the creation of a vlan failed because the parent doesn't exist.

10.0.1.80 [750]

```
WARNING 750 NET: Adding a QoS rule failed.
```

10.0.1.81 [760]

```
WARNING 760 NET: Bridges which forward link local traffic can not have more
    ↪ than 2 interfaces (bridge index >=100)
```

10.0.1.82 [800]

```
INFO 800 DFS: Starting CAC on <val> MHz.
```

This message is sent when a CAC or Off-Channel CAC is started.

10.0.1.83 [801]

```
INFO 801 DFS: Radar found on <val> MHz.
```

This message is sent when a radar pattern during In-Service Monitoring, CAC or Off-Channel CAC is detected.

10.0.1.84 [802]

```
INFO 802 DFS: Channel on <val> MHz becomes Available.
```

This message is sent when a channel on the given frequency becomes Available after a CAC or Off-Channel CAC.

10.0.1.85 [803]

```
INFO 803 DFS: Channel on <val> MHz becomes Usable again.
```

This message is sent when a channel on the given frequency becomes Usable after the NOP time.

10.0.1.86 [804]

```
INFO 804 DFS: Starting In-Service Monitoring on <val> MHz.
```

This message is sent when the In-Service Monitoring for the Operating Channel on the given frequency.

10.0.1.87 [805]

```
INFO 805 DFS: All initial CACs done.
```

This message is sent when all DFS frequencies have passed the inital CAC.