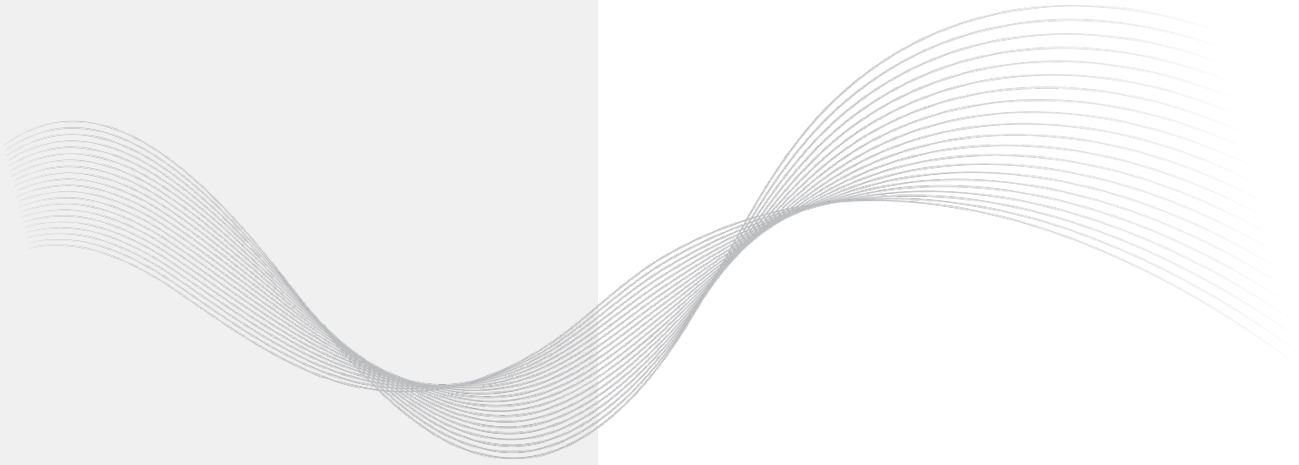


InfiNet Wireless R5000 - Web GUI

Technical User Manual

Table of Contents

Web interface is a friendly management tool of **InfiNet Wireless R5000** unit. Using Web interface, you can easily:

- Monitor device interfaces statistics
- Monitor radio link statistics
- View and change device configuration
- Access the graphical antenna alignment tool
- Run wireless link throughput tests
- Perform device maintenance and support
- Access the Spectrum Analyzer tool
- Access the system log
- Monitor DFS operation.

1 Important Notice

1.1 Legal Rights

1.2 Statement of Conditions

InfiNet Wireless Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this manual or equipment supplied with it.

1.3 Disclaimer

The software is sold on an "AS IS" basis. InfiNet Wireless, its affiliates or its licensors make no warranties, whatsoever, whether express or implied, with respect to the software and the accompanying documentation. InfiNet Wireless specifically disclaims all implied warranties of merchantability and fitness for a particular purpose and non-infringement with respect to the software. Units of product (including all the software) delivered to purchaser hereunder are not fault_ tolerant and are not designed, manufactured or intended for use or resale in applications where the failure, malfunction or inaccuracy of products carries a risk of death or bodily injury or severe physical or environmental damage (“high risk activities”). High risk activities may include, but are not limited to, use as part of on-line control systems in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, life support machines, weapons systems or other applications representing a similar degree of potential hazard. InfiNet Wireless specifically disclaims any express or implied warranty of fitness for high risk activities.

InfiNet Wireless hereby declares that R5000-Omx(b), R5000-Mmx(b), R5000-Smn(c) and R5000-Lmn are in compliance with the essential requirements and other relevant provisions of Directive 1995/5/EC. The declaration of conformity may be consulted at http://infinetwireless.com/products/materials#certifications

1.4 Indication of the countries

InfiNet Wireless equipment has no geographical limitations for selling and can be supplied to any country of the world.

1.5 Limitation of Liability

InfiNet Wireless shall not be liable to the purchaser or to any third party, for any loss of profits, loss of use, interruption of business or for any indirect, special, incidental, punitive or consequential damages of any kind, whether arising under breach of contract, tort (including negligence), strict liability or otherwise and whether based on this agreement or otherwise, even if advised of the possibility of such damages.

To the extent permitted by applicable law, in no event shall the liability for damages hereunder of InfiNet Wireless or its employees or agents exceed the purchase price paid for the product by purchaser, nor shall the aggregate liability for damages to all parties regarding any product exceed the purchase price paid for that product by that party (except in the case of a breach of a party’s confidentiality obligations).

1.6 International Regulatory Information

This equipment has been tested and found to comply with the limits for a Class B digital device.

Hereby, InfiNet Wireless declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

CE	**The CE Marking on this equipment indicates compliance with the following:** **This device conforms to Directive 1999/5/EC on Radio Equipment and Telecommunications Terminal Equipment as adopted by the European Parliament And Of The Council.**

2 About This Manual

This manual provides detailed technical information on the operation of the Web interface (guidelines for the use of all sections and futures) of **InfiNet Wireless R5000** series. The manual provides also step-by-step guides for the routine tasks and basic scenarios like: setting up a basic PtP link, setting the MAC switching options, using "*test*" configuration, firmware upgrade, etc.

This manual is designed for individuals who prefer using a graphical user interface (GUI) for configuring and managing **InfiNet Wireless R5000** series devices. It is intended for the following audiences:

- Customers with technical knowledge of and experience with IP networks
- Network administrators, who install, configure and manage **InfiNet Wireless R5000** series devices.

3 Getting started with InfiNet Wireless R5000 Web GUI

3.1 Document structure

This document consists of the following chapters:

- “Getting started” - This chapter presents the information about this document’s purpose and structure
- “Features set" - This chapter provides descriptions and guidelines for the use of all sections and views of the Web interface
- “Configuration scenarios" - This chapter contains step-by-step guides for the routine tasks and basic scenarios (for example: setting up a basic PtP link, configuration examples, using “test” configuration, firmware upgrade, etc.)

3.2 Abbreviations

The following abbreviations are used in this document:

- ARP - Address Resolution Protocol
- ATPC - Automatic Transmit Power Control
- BS - Base Station
- CINR - Carrier to Interference + Noise Ratio
- CLI - Command Line Interface
- CPE - Customer Premises Equipment
- CPU - Central Processing Unit
- CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
- DFS - Dynamic Frequency Selection
- DHCP - Dynamic Host Configuration Protocol
- DNS - Domain Name System
- DSCP - Differentiated Services Code Point
- EVM - Error Vector Magnitude

- GRE - Generic Routing Encapsulation
- GUI - Graphical User Interface
- HTTPS - HyperText Transfer Protocol Secure
- ICMP - Internet Control Message Protocol
- IGMP - Internet Group Multicast Protocol
- IP - Internet Protocol
- IPIP - IP-in-IP Protocol
- LAG - Link Aggregation Group
- MAC - Media Access Control
- MIB - Management Information Base
- MIMO - Multiple Input Multiple Output
- MINT - Mesh Interconnection Networking Technology
- MISO - Multiple-Input and Single-Output
- NLOS - Non-Line of Sight
- OSPF - Open Shortest Path First
- POSIX - Portable Operating System Interface
- PRF - Pseudo Radio Interface
- PtMP - Point to MultiPoint
- PtP - Point-to-Point
- QoS - Quality of Service
- RSSI - Received Signal Strength Indicator
- RTP - Real Time Protocol
- SID - System Identification Number

- SISO - Single-Input and Single-Output
- SNAP - Standard Network Access Protocol
- SNMP - Simple Network Management Protocol
- SNR - Signal To Noise Ratio
- SNTP - Simple Network Time Protocol
- SSH - Secure Shell
- SSL - Secure Sockets Layer
- STP - Spanning Tree Protocol
- SVI - Switch Virtual Interface
- TAP - Network TAP
- TCP - Transmission Control Protocol
- TDMA - Time Division Multiple Access
- TUN - Network TUNnel
- VLAN - Virtual Local Area Network
- VPN - Virtual Private Network

3.3 Document marks

CAUTION

All caution warnings are marked with a special warning sign. One should pay a great deal of attention to what is written in the Caution section.

NOTE

All notes are marked with a special note sign. Notes usually contain useful comments or hints to the described section of the document.

4 Features set

4.1 InfiNet Wireless R5000 unit access

When you power on the unit, **WANFleX OS** starts automatically and Web management is enabled by default so, in order to access the unit via Web browser (start the graphical user interface), type in the address bar: http://<unit IP address>.

NOTE

By default (since v1.90.0), the access to the device is available through "*svi1*" interface at the IP address 10.10.10.1/24 (for further details about SVI interface see section Network settings).

Make sure you have network connectivity to the unit.

NOTE

The system allows concurrent login sessions via Web interface.

On the login page, you can type any username and any password and click Login:

Figure - GUI login

NOTE

Please change the credentials you have just inserted with a permanent username and password for it after the first log in.

The default language is English. After the authentication step, the language can be changed into Russian, French, Italian or Chinese.

You can access the unit via HTTPS (HTTP with SSL only) using InfiNet Wireless self-signed certificate (from the Maintenance menu of Web interface). The «HTTPS Connection» link is available in the right side of the login form:

Figure - HTTPS connection

4.2 Device Status menu

The "Device Status" page is displayed by default after the authentication step. It displays the main parameters of the unit in real-time. You can set the "*Auto Refresh*" option to refresh the statistics automatically. Refresh frequency can be set by the "*Auto Refresh Time*" parameter. The minimal possible value is “0” seconds and it updates the information instantly.

The device statistics can also be refreshed manually by clicking the «**Refresh**» button.

These options are available in the bottom-left side of the "Device Status" screen:

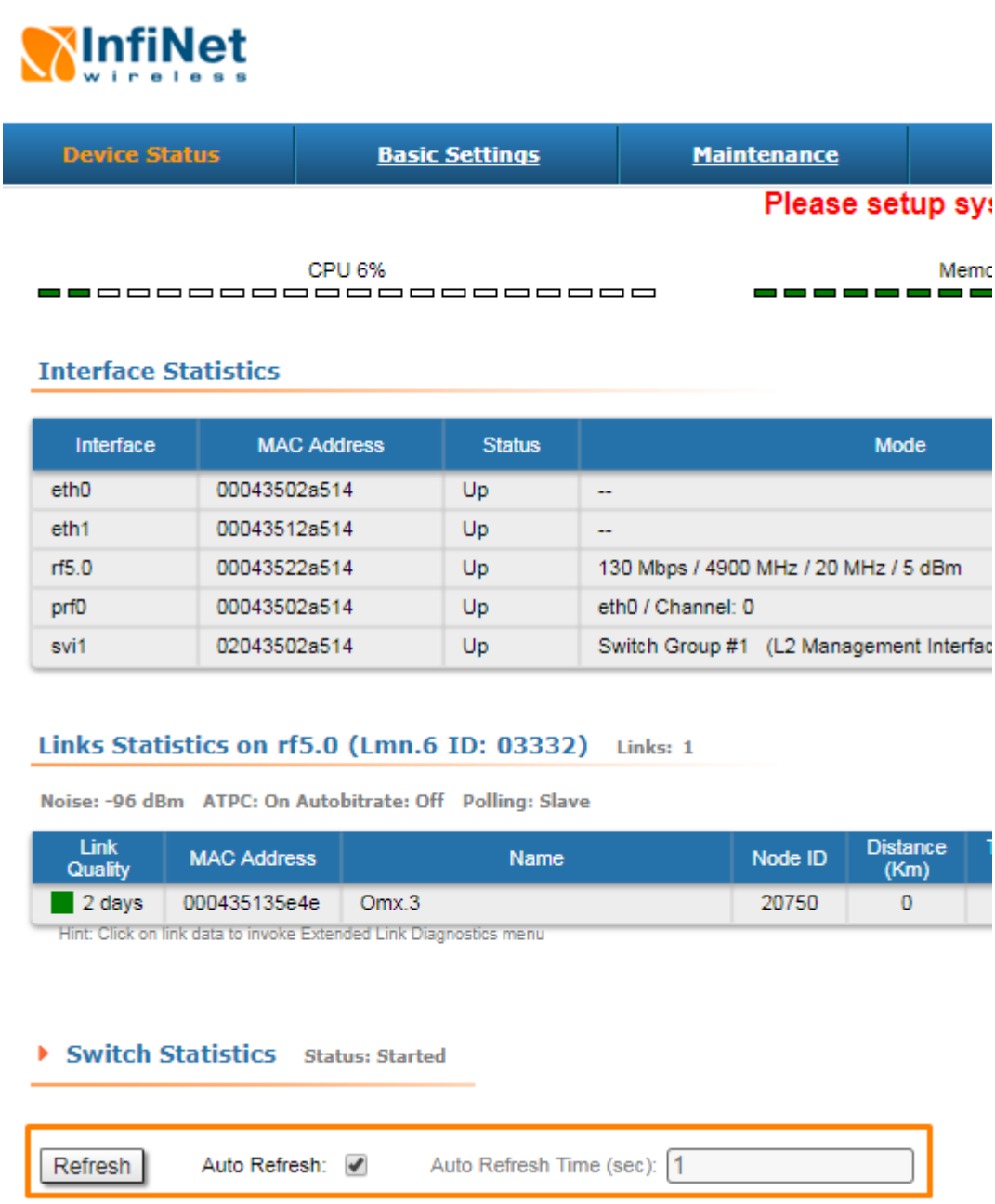


Figure - Refresh option

The "Device Status" page has the following sections:

- "CPU load" - displays the load percentage of the CPU
- "Memory load":
  - Memory (the data stored in volatile memory are valid only during the current session, until the system reset) displays in real-time the total memory available and the used memory by the running processes
  - Flash memory (non-volatile memory) displays in real-time the total memory available and the used memory by the **WANFleX** and configuration files
- "Interface Statistics" - displays the main parameters of all configured interfaces (physical and logical)
- "Wireless Links Statistics" - displays the main parameters of all wireless connections between the device and the neighbor devices
- "Switch Statistics" - displays counters of the frames which have been switched (for example: the number of dropped packets and if they are dropped because of the flood into their reachable destination, because of the firewall, etc).

4.2.1 Interface Statistics

Parameter	Description
Interface	▪ Displays all physical and logical set interfaces
MAC Address	▪ Displays the MAC address of each interface
Status	▪ Displays for each interface whether it is “up and running” or not
Mode	▪ Displays the operation mode of each interface. For example: ○ 10,100 or 1000 Mbps and half or full duplex for the Ethernet interface ○ Bitrate, frequency and bandwidth for the Radio interface ○ Switch Group number for the SVI
Packets	▪ Displays the number of received and transmitted packets for each interface since the unit is operational. The local system packets are counted, too (and not only the ones that are passing through the switching groups - data traffic)
Errors	▪ Displays the number of received and transmitted error packets for each interface since the unit is operational
Load	▪ Displays the packet flow through each interface in real-time (for the system and the data traffic)

Table - Interface Statistics

All these counters can be reset by clicking the **«Reset All Counters»** button:

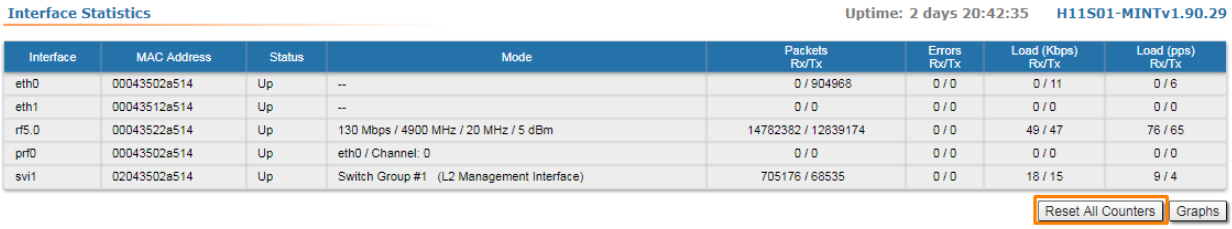


Figure - Counters reset

CAUTION

Clearing these counters by clicking the «**OK**» button in the pop-up page means losing the history data about the functionality of your unit. Avoid this operation unless you are completely sure you don't need these data in the future.

The software version is displayed in the right side of Interface Statistics section (for example: MINTv1.90.5).

4.2.2 Links Statistics on rf5.0

This section displays the following information for the radio interface of the unit:

- Node name and ID
- Noise level
- Number of established links
- ATPC status (activated or deactivated)
- Autobitrate status (activated or deactivated)
- Polling mode

Parameter	Description
Link Quality	▪ Gives a color indication for the wireless connection quality with the neighbor unit: ○ Red: poor connection ○ Yellow: good connection ○ Green: excellent connection

Parameter	Description
Link Uptime	▪ Displays the link uptime
Relevance of remote unit firmware **(Optional)**	▪ Idicates that the remote unit has the older firmware than the local one ○ The indicator looks like a "F" symbol after the link uptime
System password of the remote unit **(Optional)**	▪ Idicates that the remote unit has the system password ○ The indicator looks like a "?" symbol after the link uptime
MAC Address	▪ Displays the neighbor’s MAC address
Name	▪ Displays the neighbor’s name
Node ID	▪ Displays the sequential number of the neighboring node
Distance	▪ Displays the calculated (theoretical) distance to the neighbor unit (in Km)
Tx Power	▪ Displays the power level of the Tx and Rx signals of the neighbor unit (in dBm)
Ref. Level	▪ Displays the Tx and Rx signals levels for the minimal available bitrate of the neighbor unit (in dB)
Current Level	▪ Displays the Tx and Rx signals levels for current bitrate of the neighbor unit (in dB)

Parameter	Description
Bitrate	▪ Displays the set bitrate value for the Tx and Rx signals of the neighbor unit
Retries	▪ Displays the percentage of Tx and Rx retries of the neighbor unit
Errors	▪ Displays the percentage of Tx and Rx errors of the neighbor unit
Load	▪ Displays the number of kbps and packets that are going inbound and outbound the radio interface of the neighbor unit (main data)

Table - Wireless Links Statistics

By clicking the "**Route Map**" button you can get the MINT topology schematic map with the visualization of the active and alternative routes to each node.

NOTE

Map is available for H08, H09, H11 hardware platforms.

Schematic topology map allows you to visually determine the network connectivity and complexity and to track the route switching, including mobile objects.

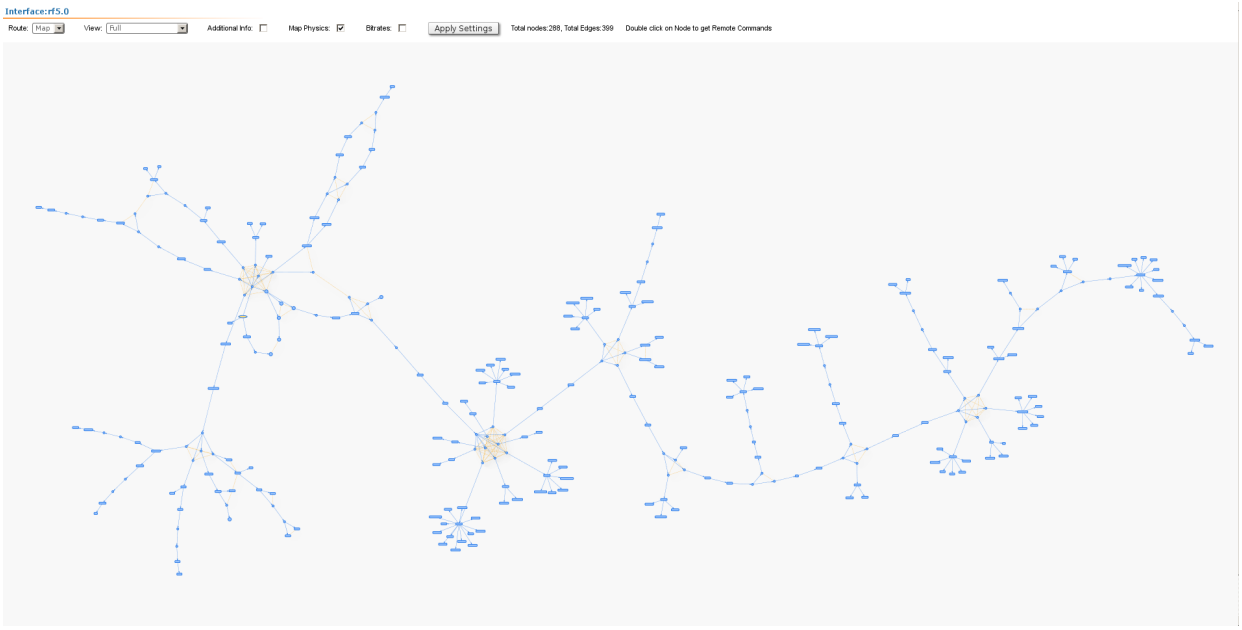


Figure - Schematic map

For additional information on each node, double click on it to get remote commands (rcmd).

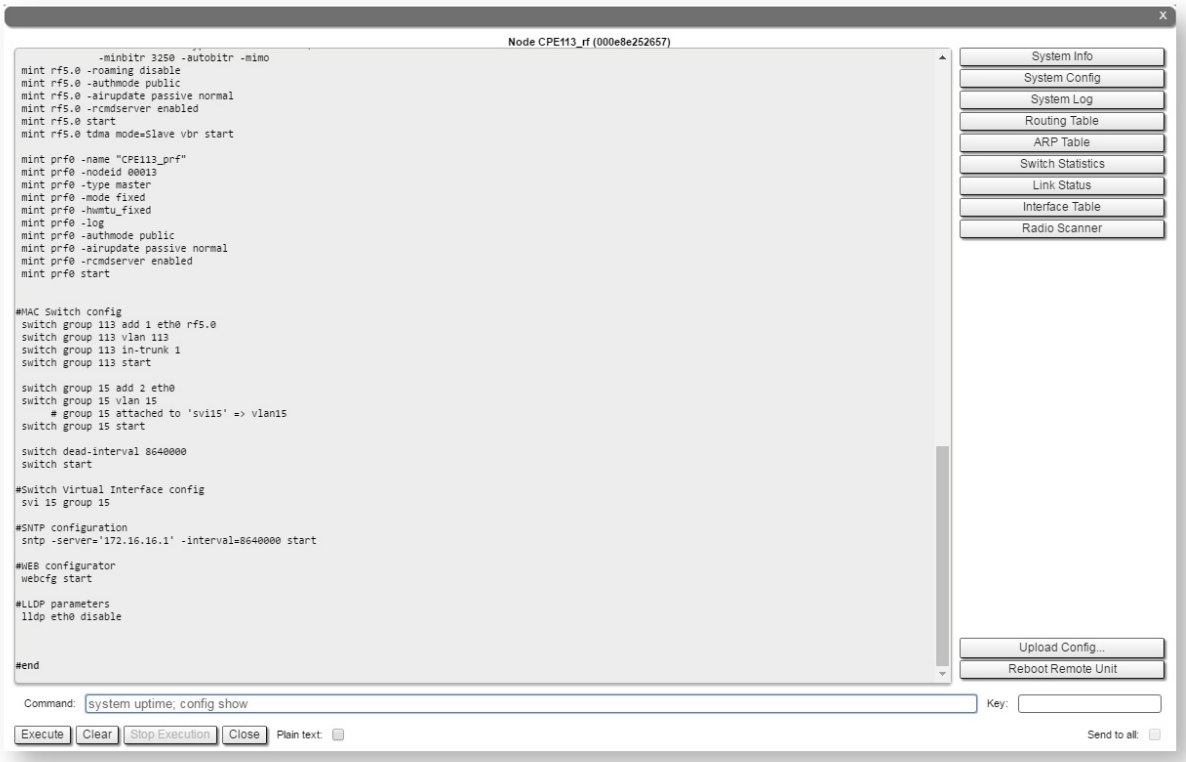


Figure - Remote commands

Detailed information about options in this tool is described in the "Remote Commands" section.

In TDMA based software in the "Wireless Links Statistics for Interface rf5.0" section some additional information is available:

- about wireless link parameters;
- deflection angle from the main antenna direction towards the subscriber terminal, in the column "Distance" (only for **R5000-Qmxb** sector base station with beamforming technology).

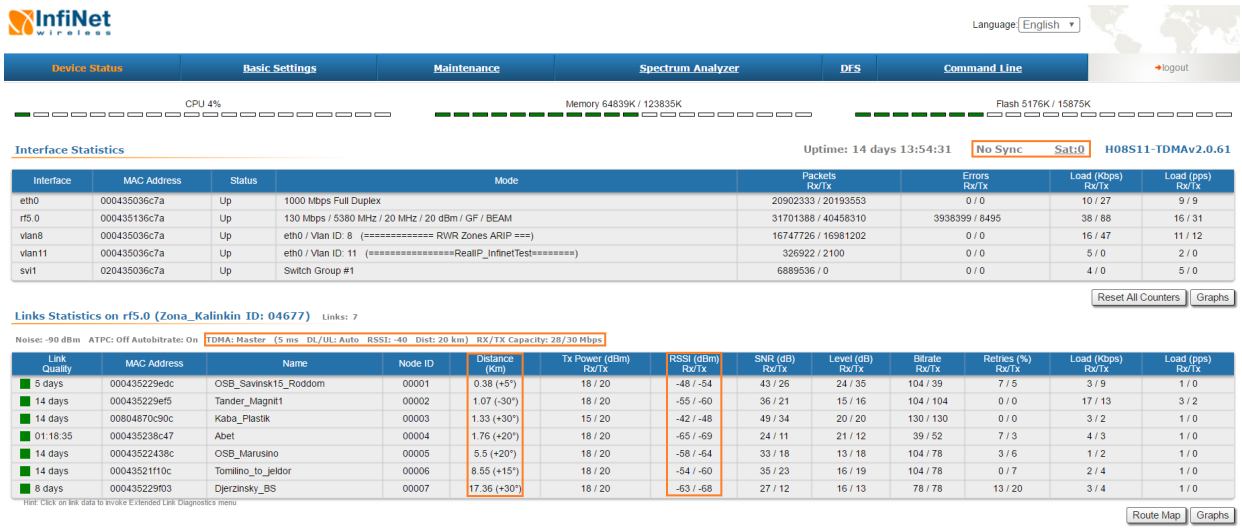


Figure - Wireless Links Statistics for the Radio interface in the TDMA based software

Parameter	Description
Current TDMA parameters	■ Displays the current TDMA parameters: ○ Operational mode of the unit (Master/Slave) ○ Time slot duration (in microseconds) ○ Downlink percentage of the time slot ○ Maximum RSSI level (in dBm) ○ Maximum operational distance (in kilometers) ○ RX/TX Capacity
RSSI (dBm) Rx/Tx	■ Displays the power present in a received radio signal ○ "*Rx*" – the power of received radio signal, measured at the local unit ○ "*Tx*" - the power of received radio signal, measured at the remote unit

Parameter	Description
Sync Status	▪ Displays the current status of device synchronization with external timing reference from GPS/GLONASS ○ "*Sync*": the device is in sync. The value in brackets is current value of the offset (in microseconds) between the internal clock of the device and the external timing reference from GPS/GLONASS ○ "*Wait Sync*": the device is waiting the external timing reference from GPS/GLONASS. Synchronization is enabled on the device, but it doesn't receive external timing reference from GPS /GLONASS ○ "*No Sync*": the device is not in sync. The current value of offset between the internal clock and the external timing reference from GPS/GLONASS is beyond the allowed value range (±10 microseconds)
Sat:	▪ The number of visible GPS/GLONASS satellites

Table - Wireless Links Statistics - Radio particular parameters in the TDMA based software

4.2.3 Switch Statistics

This section displays the number of unicast, broadcast and flood packets switched within each Switch group and also within kernel system (internal traffic), in real-time (since the last reboot):

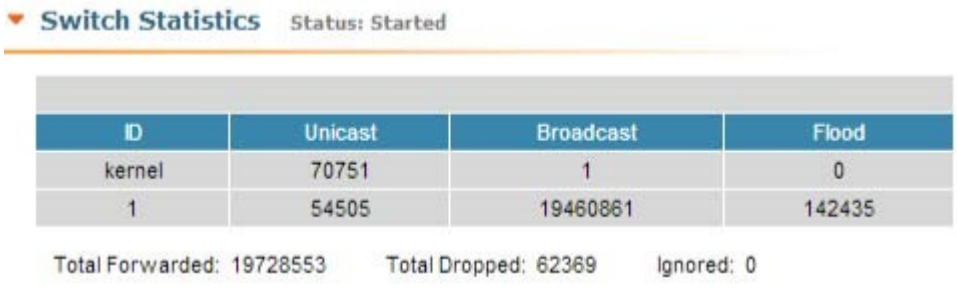
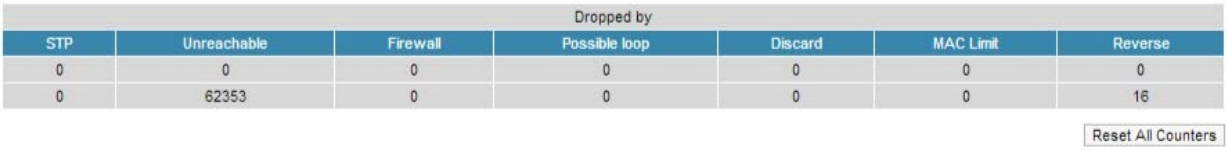


Figure - Switch Statistics

It also displays the number of dropped packets for: STP, unreachable destination, firewall, possible loop, discard, MAC limits and reverse, within each Switch group and kernel, in real-time (since the last reboot):



Dropped by						
STP	Unreachable	Firewall	Possible loop	Discard	MAC Limit	Reverse
0	0	0	0	0	0	0
0	62353	0	0	0	0	16

Reset All Counters

Figure - Switch Statistics

Total forwarded, dropped and ignored packets are displayed in real-time, too.

All these counters can be reset by clicking the «**Reset All Counters**» button.

Switch Statistics parameters:

Parameter	Description
Unicast	▪ Sending a packet to a single host (network destination) identified by a unique address
Broadcast	▪ Sending a packet to all hosts (network destinations) simultaneously (broadcasting is done by specifying a special broadcast address on packets)
Flood	▪ Sending a packet along the same link multiple times (without specifying a destination address for the packets) ▪ Several copies of the same packet would ultimately reach all nodes in the network in flooding
STP	▪ Spanning Tree Protocol - standardized as IEEE 802.1D ▪ Creates a spanning tree within a network of connected layer-2 bridges (typically Ethernet switches) and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes ▪ The value displayed in the Switch Statistics table represents the number of the packets blocked by the Spanning Tree Protocol

Parameter	Description
Unreachable	▪ The sender could not reach the specified network destination ▪ The value displayed in the Switch Statistics table represents the number of the packets dropped because they flood to unreachable destination
Firewall	▪ A software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rules set ▪ The value displayed in the Switch Statistics table represents the number of the packets dropped by the firewall system in the network
Possible loop	▪ A switching or bridging loop occurs in a network when there is more than one Layer 2 path between two endpoints ▪ Because a physical topology that contains switching or bridging loops is needed for the redundancy reasons, the solution is to allow physical loops, but create a loop-free logical topology using the spanning tree protocol (STP) on the network switches ▪ The value displayed in the Switch Statistics table represents the number of the packets dropped because they belong to a possible loop (more than one port declares same packet source)
Discard	▪ The value displayed in the Switch Statistics table represents the number of the packets dropped by the configuration (for example: "switch group N start [discard]")
MAC Limit	▪ MAC address-table limit reached (switch maxsources (MAXSOURCES|0) # default 5000) ▪ The value displayed in the Switch Statistics table represents the number of the packets dropped because the limit of MAC address-table was reached

Parameter	Description
Reverse	▪ The value displayed in the Switch Statistics table represents the number of the packets dropped because they have the same source and destination port (the frame came to the unit through one port and according to the switching table it must leave through the same port)

Table - Switch statistics parameters

By clicking the «**Show System Log**» button, you can view the "System Log" section:

Figure - System log

The "System Log" section allows browsing the unit's system log. It is possible to minimize /enlarge the system log window by clicking the buttons: 

You can delete all the information saved in the system log by clicking the «**Clear System Log**» button. You can hide the System Log section by clicking the «**Hide System Log**» button.

4.2.4 Extended Interface Statistics

The "Extended Interface Statistics" tools gather complete information and enhanced statistics for each interface of the unit. Each interface type has its own set of available tools applicable to it.

In order to access the "Extended Interface Statistics" tools, click on the row of each interface within the "Interface Statistics" section:

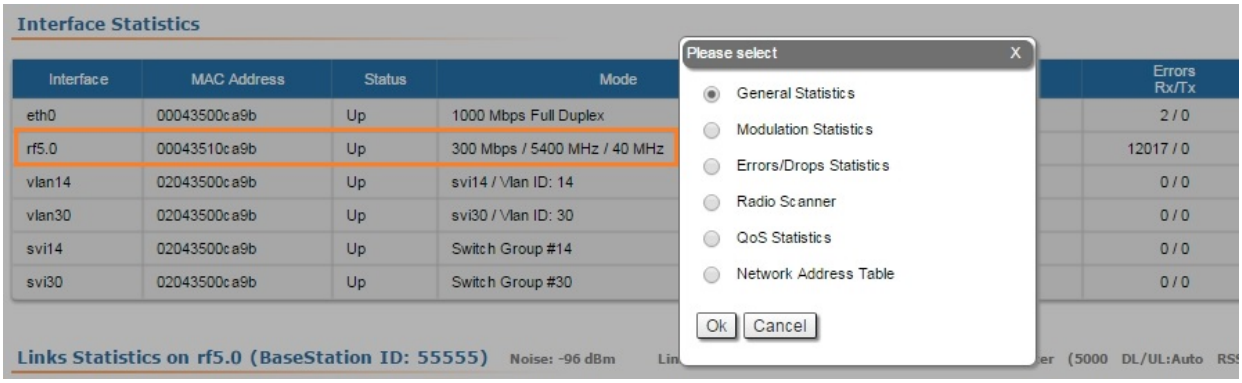


Figure - Extended Interface Statistics

General Statistics

The "General Statistics" tool displays the information about the interface such as the *interface mode, current status, Rx and Tx statistics,* etc. The actual statistics details depend on the interface type.

By clicking the «**Close**» button, you return to the "Device Status" page.

By clicking the «**Reset**» button, you clear all counters displayed in the page.

The "*Auto Refresh*" option is active by default and refreshes the statistics automatically. You can disable the auto refresh.

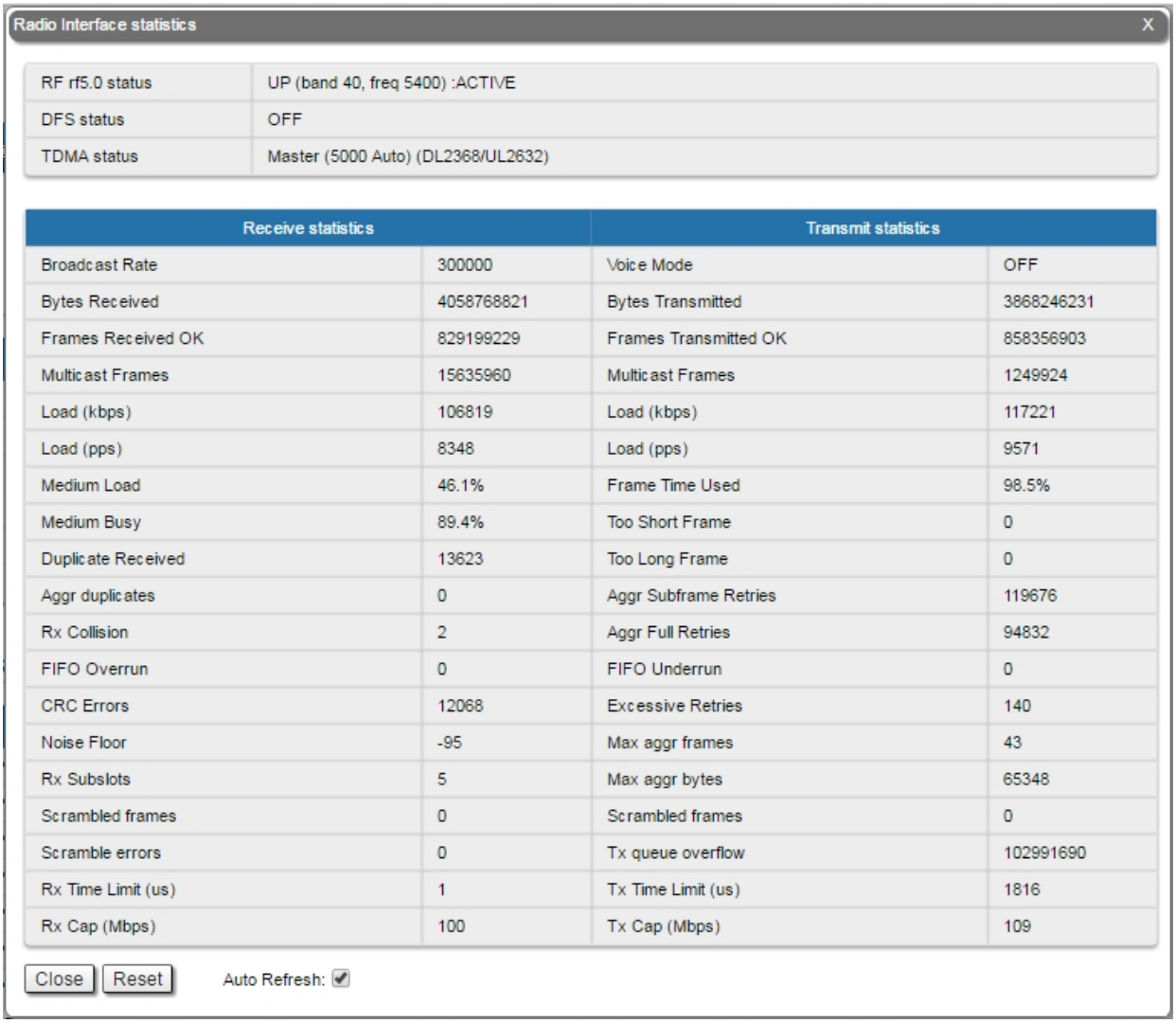


Figure - General Statistics

Modulation Statistics

The "Modulation Statistics" tool displays the information about modulation types, such as receive and transmit statistics for different coding scheme.

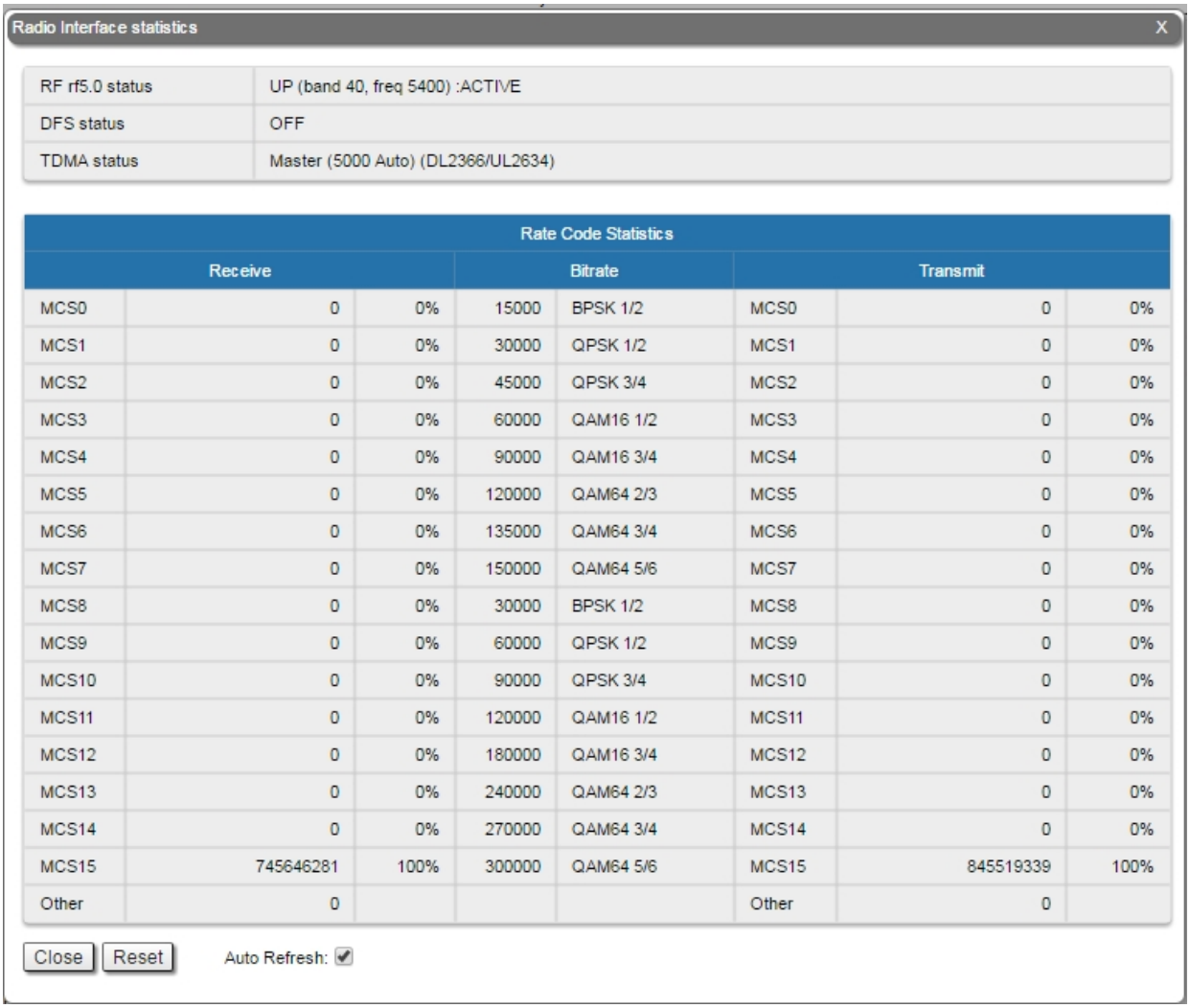


Figure - Modulation Statistics

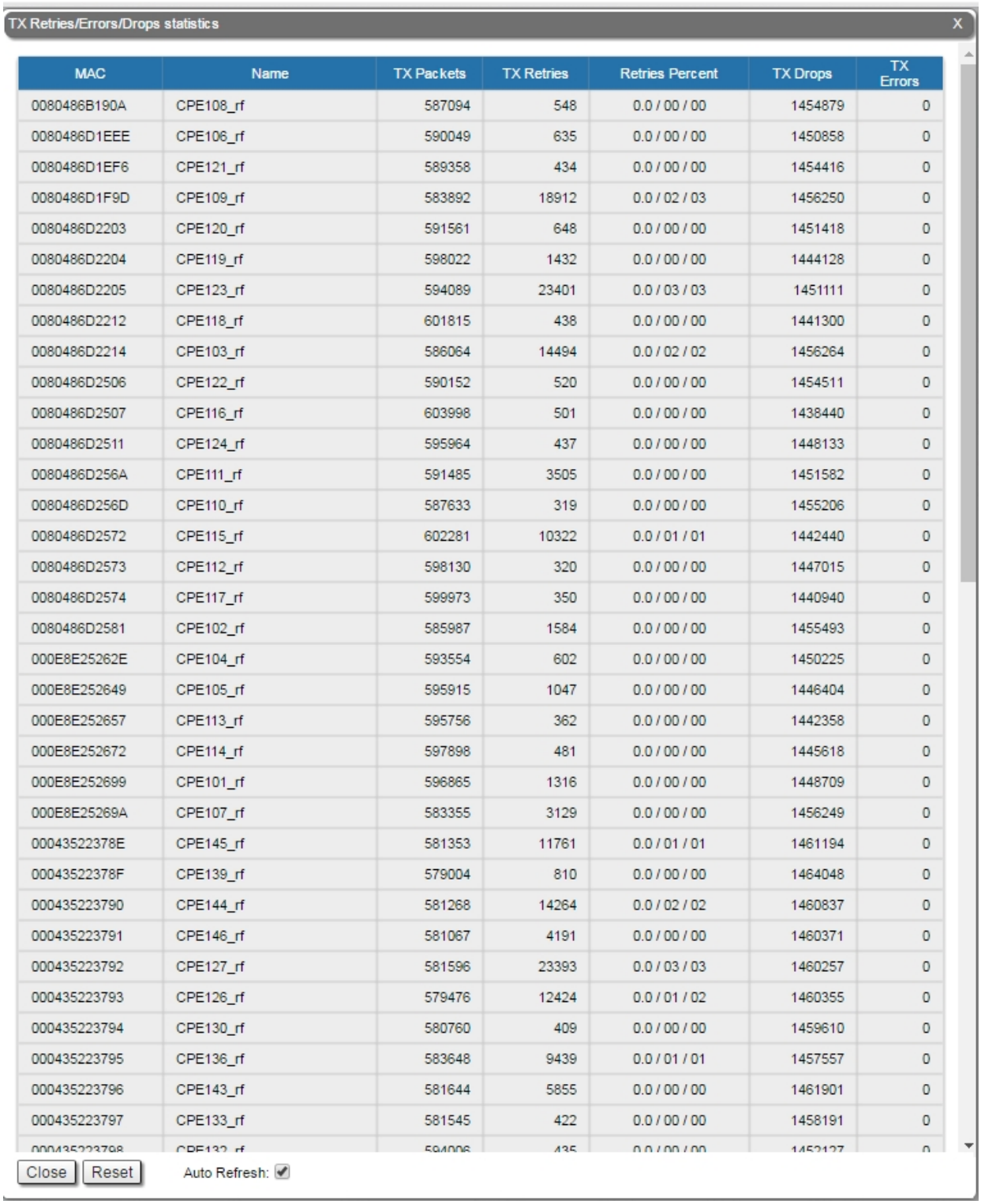
By clicking the «**Close**» button, you return to the "Device Status" page.

By clicking the «**Reset**» button, you clear all counters displayed in the page.

The "*Auto Refresh*" option is active by default and refreshes the statistics automatically. You can disable the auto refresh.

Errors/Drops Statistics

The "Errors/Drops Statistics" tool displays the number of errors and link drops during transmission for each link.



MAC	Name	TX Packets	TX Retries	Retries Percent	TX Drops	TX Errors
0080486B190A	CPE108_rf	587094	548	0.0 / 00 / 00	1454879	0
0080486D1EEE	CPE106_rf	590049	635	0.0 / 00 / 00	1450858	0
0080486D1EF6	CPE121_rf	589358	434	0.0 / 00 / 00	1454416	0
0080486D1F9D	CPE109_rf	583892	18912	0.0 / 02 / 03	1456250	0
0080486D2203	CPE120_rf	591561	648	0.0 / 00 / 00	1451418	0
0080486D2204	CPE119_rf	598022	1432	0.0 / 00 / 00	1444128	0
0080486D2205	CPE123_rf	594089	23401	0.0 / 03 / 03	1451111	0
0080486D2212	CPE118_rf	601815	438	0.0 / 00 / 00	1441300	0
0080486D2214	CPE103_rf	586064	14494	0.0 / 02 / 02	1456264	0
0080486D2506	CPE122_rf	590152	520	0.0 / 00 / 00	1454511	0
0080486D2507	CPE116_rf	603998	501	0.0 / 00 / 00	1438440	0
0080486D2511	CPE124_rf	595964	437	0.0 / 00 / 00	1448133	0
0080486D256A	CPE111_rf	591485	3505	0.0 / 00 / 00	1451582	0
0080486D256D	CPE110_rf	587633	319	0.0 / 00 / 00	1455206	0
0080486D2572	CPE115_rf	602281	10322	0.0 / 01 / 01	1442440	0
0080486D2573	CPE112_rf	598130	320	0.0 / 00 / 00	1447015	0
0080486D2574	CPE117_rf	599973	350	0.0 / 00 / 00	1440940	0
0080486D2581	CPE102_rf	585987	1584	0.0 / 00 / 00	1455493	0
000E8E25262E	CPE104_rf	593554	602	0.0 / 00 / 00	1450225	0
000E8E252649	CPE105_rf	595915	1047	0.0 / 00 / 00	1446404	0
000E8E252657	CPE113_rf	595756	362	0.0 / 00 / 00	1442358	0
000E8E252672	CPE114_rf	597898	481	0.0 / 00 / 00	1445618	0
000E8E252699	CPE101_rf	596865	1316	0.0 / 00 / 00	1448709	0
000E8E25269A	CPE107_rf	583355	3129	0.0 / 00 / 00	1456249	0
00043522378E	CPE145_rf	581353	11761	0.0 / 01 / 01	1461194	0
00043522378F	CPE139_rf	579004	810	0.0 / 00 / 00	1464048	0
000435223790	CPE144_rf	581268	14264	0.0 / 02 / 02	1460837	0
000435223791	CPE146_rf	581067	4191	0.0 / 00 / 00	1460371	0
000435223792	CPE127_rf	581596	23393	0.0 / 03 / 03	1460257	0
000435223793	CPE126_rf	579476	12424	0.0 / 01 / 02	1460355	0
000435223794	CPE130_rf	580760	409	0.0 / 00 / 00	1459610	0
000435223795	CPE136_rf	583648	9439	0.0 / 01 / 01	1457557	0
000435223796	CPE143_rf	581644	5855	0.0 / 00 / 00	1461901	0
000435223797	CPE133_rf	581545	422	0.0 / 00 / 00	1458191	0

Figure - Errors/Drops Statistics

By clicking the «**Close**» button, you return to the "Device Status" page.

By clicking the «**Reset**» button, you clear all counters displayed in the page.

The "*Auto Refresh*" option is active by default and refreshes the statistics automatically. You can disable the auto refresh.

Radio Scanner

The "Radio Scanner" tool allows to estimate the efficiency of the radio links utilization, analyzing the radio-frequency environment for the current frequency, under the current channel bandwidth, without the radio link interruption and displays the following statistics:

- Radio parameters of every source in the radio link
- Number of sources, number of packets, including the skipped ones
- Number of pulses, their average level and average number of pulses per second

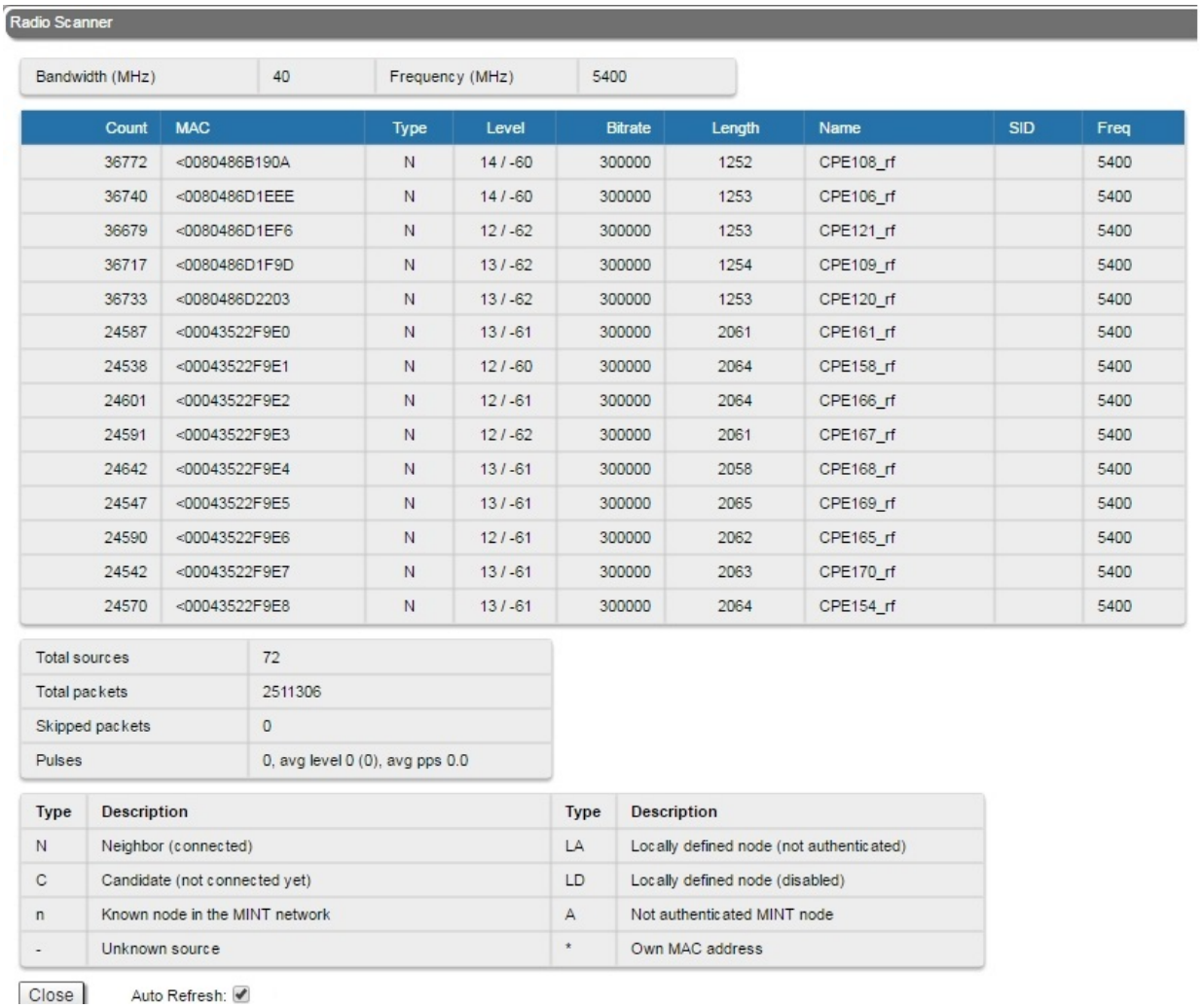


Figure - Radio Scanner

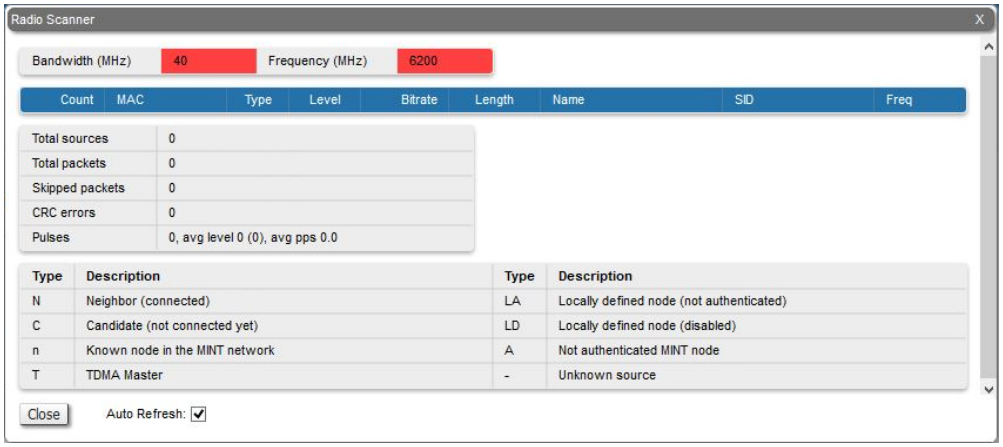
The abbreviations for each node type are also displayed in the interface:

Type	Description
N	▪ Neighbor (connected)
C	▪ Candidate (not connected yet)
n	▪ Known node in the MINT network
-	▪ Unknown source
LA	▪ Locally defined node (not authenticated)
LD	▪ Locally defined node (disabled)
A	▪ Not authenticated MINT node
*	▪ Own MAC address

Table - Node types

NOTE

"Frequency" and "Bandwidth" are highlighted in red when the frequency and bandwidth values are already not the same as they were when Radio Scanner was started.



This may occur when several profiles at the subscriber terminal link settings are configured. While searching the base station sector the subscriber terminal loops through all available profiles with different settings, highlighting them in red.

By clicking the «**Close**» button, you return to the "Device Status" page.

The "*Auto Refresh*" option is active by default and refreshes the statistics automatically. You can disable the auto refresh.

QoS Statistics

QoS (Quality of Service) characterizes the entire network performance which is defined by the parameters such as: throughput, latency, jitter, error rate, available bandwidth, etc. In order to provide the guaranteed Quality of Service for certain applications, users or data flows, different prioritization methods are used.

The "QoS Statistics" tool displays the statistics of the MINT priority queues for the interface.

Priority is one of the parameters which define in what sequence, different types of data traversing every InfiNet device in MINT network are treated. Each channel may be assigned a priority (for example: P01, P02 … P16).

Once assigned, a priority is automatically recognized by every node inside the MINT network. Each priority value corresponds to a device queue. Once in a queue, every packet is scheduled according to the queuing algorithm set on the device. QM manager supports "*Strict Priority Queuing*" and "*Weighted Fair Queuing*" scheduling algorithms. "*Strict Priority Queuing*" means that the packets from queue with lower priority are not processed until the queue with higher priority is not empty. "*Weighted Fair Queuing*" uses weights for every queue of an interface and allows different queues to have different service shares, depending on that weight.

Every channel is also characterized by the latency parameter. This parameter determines the maximum time for the packets to stay in the channel. If a packet is waiting in a queue of the channel more than the time specified in the latency parameter, then it is discarded. Latency can be set for each channel in the "Traffic Shaping" section.

Queue name	Priority/Queue number
QM_PRIO_NETCRIT	0
QM_PRIO_VOICE	1
QM_PRIO_RT1	2
QM_PRIO_VIDEO	3
QM_PRIO_RT2	4
QM_PRIO_QOS1	5
QM_PRIO_QOS2	6
QM_PRIO_QOS3	7
QM_PRIO_QOS4	8
QM_PRIO_BUSINESS1	9
QM_PRIO_BUSINESS2	10
QM_PRIO_BUSINESS3	11
QM_PRIO_BUSINESS4	12
QM_PRIO_BUSINESS5	13
QM_PRIO_BUSINESS6	14
QM_PRIO_BUSINESS7	15
QM_PRIO_BUSINESS8	16

Table - MINT priorities and WANFLeX queues

Transparent packet prioritization is a **WANFLeX** feature which allows QM manager to transparently map 802.1p/TOS/DSCP priority to MINT priority for the ease of deployment.

You have to make sure that “*Dot1p Tags*” and/or “*IP ToS*” options are enabled in the "QoS" section.

MINT priority	802.1p/TOS priority/DSCP
QM_PRIO_BUSINESS8	00/00/00 (CS0, 000000)
No priority	01/01/08 (CS1, 001xxx)
No priority	02/02/16 (CS2, 010xxx)
QM_PRIO_BUSINESS1	03/03/24 (CS3, 011xxx)
QM_PRIO_QOS3	04/04/32 (CS4, 100xxx)
QM_PRIO_VIDEO	05/05/40 (CS5, 101xxx)
QM_PRIO_VOICE	06/06/48 (CS6, 110xxx)
QM_PRIO_NETCRIT	07/07/56 (CS7, 111xxx)

Table - MINT priority to 802.1p/TOS priority/DSCP map

This section displays the number of inbound packets to each priority queue and the number of dropped packets:

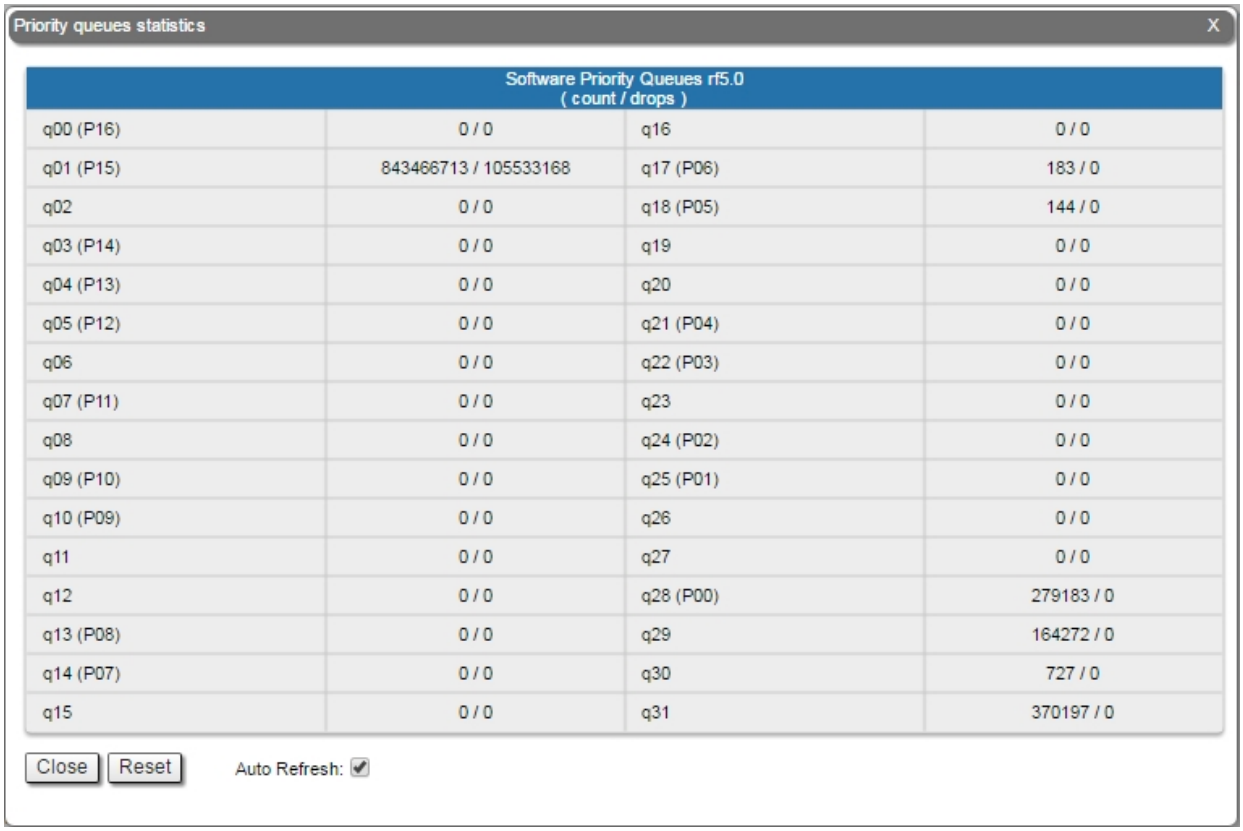


Figure - QoS Statistics

By clicking the «**Close**» button, you return to the "Device Status" page.

By clicking the «**Reset**» button, you clear all counters displayed in the page.

The "*Auto Refresh*" option is active by default and refreshes the statistics automatically. You can disable the auto refresh.

Network Address Table

The "Network Address Table" tool shows the network address table for the interface.

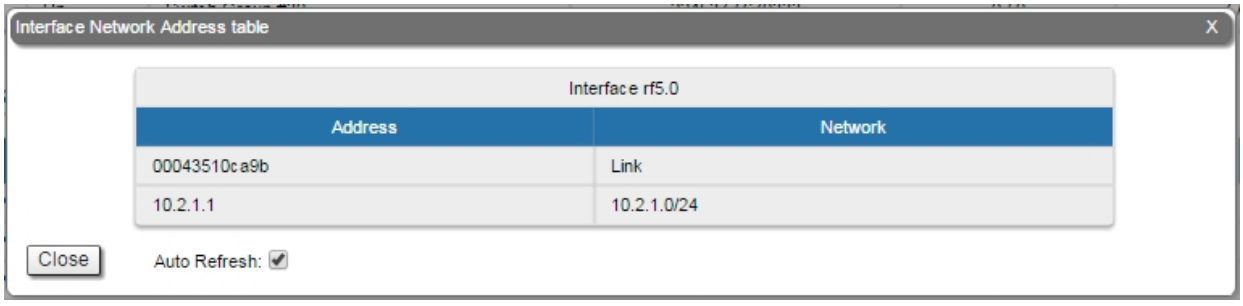


Figure - The Network Address Table for the local unit

By clicking the «**Close**» button, you return to the "Device Status" page.

The "*Auto Refresh*" option is active by default and refreshes the statistics automatically. You can disable the auto refresh.

LLDP Information

The "LLDP Information" tool allows to get information on the link layer discovery protocol.

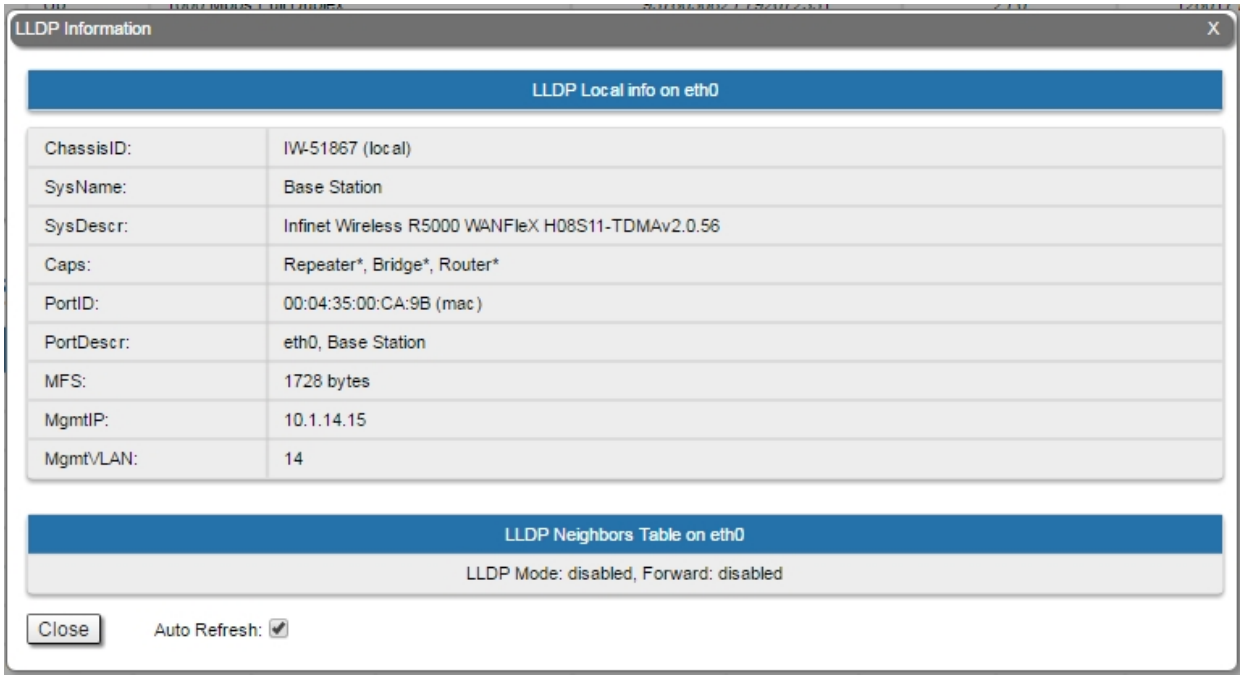


Figure - LLDP Information

By clicking the «**Close**» button, you return to the "Device Status" page.

The "*Auto Refresh*" option is active by default and refreshes the statistics automatically. You can disable the auto refresh.

4.2.5 Extended Link Diagnostics

Once a wireless connection between the unit and the remote neighbor is established, it is possible to make extended diagnostics and optimization for the wireless link.

In order to access the "Extended Link Diagnostics" tools, click on the row of each wireless link within the "Links Statistics on rf5.0" section:

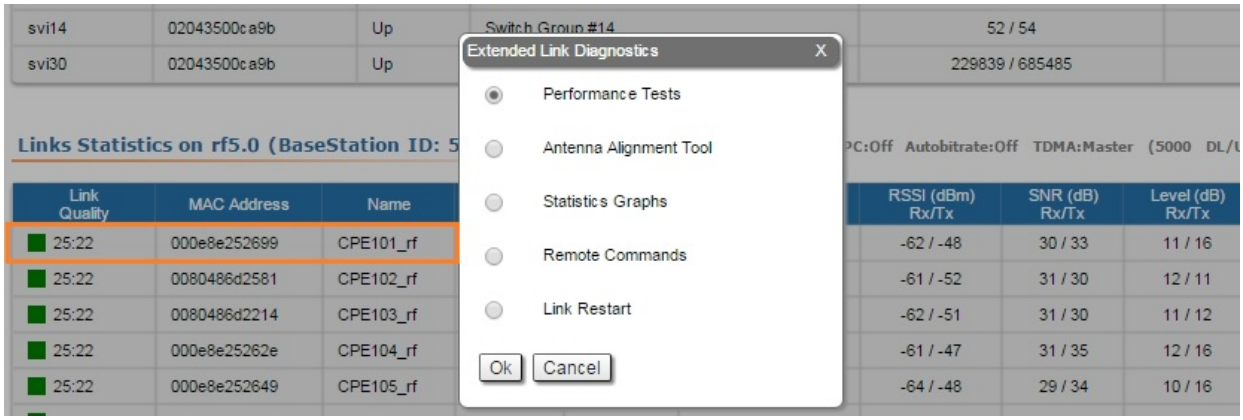


Figure - Extended Link Diagnostics

Five options are available: "Performance Tests", "Antenna Alignment Tool", "Statistics Graphs", "Remote Commands" and "Link Restart".

Performance tests

The "Performance tests" tool performs link throughput tests for the configured channel bandwidth and on the current frequency, without radio link interruption.

The "Performance tests" tool generates traffic between the devices and displays the channel throughput for the traffic with chosen priority. For the full throughput tests of the channel, you must set the highest priority “0” for the test traffic. In this case, the transmission of any other traffic is stopped for the testing time and the traffic generated by the tool will occupy all the channel.

The "Performance tests" tool displays the values of the full channel throughput which is available under the current settings, for each bitrate.

NOTE

All results are given in kilobits per second and retries levels are shown as a red chart.

Performance tests for "*MINT*" and "*TDMA*" firmware are not the same. There are two tests in "*MINT*": one with graduation on bitrate, other in "*Use MINT*" mode. In "*Use MINT*" mode 8 tests are performed on established bitrate. In case of "*TDMA*" firmware teat of graduation on bitrate is not performed. Both firmware support bidirectional test.

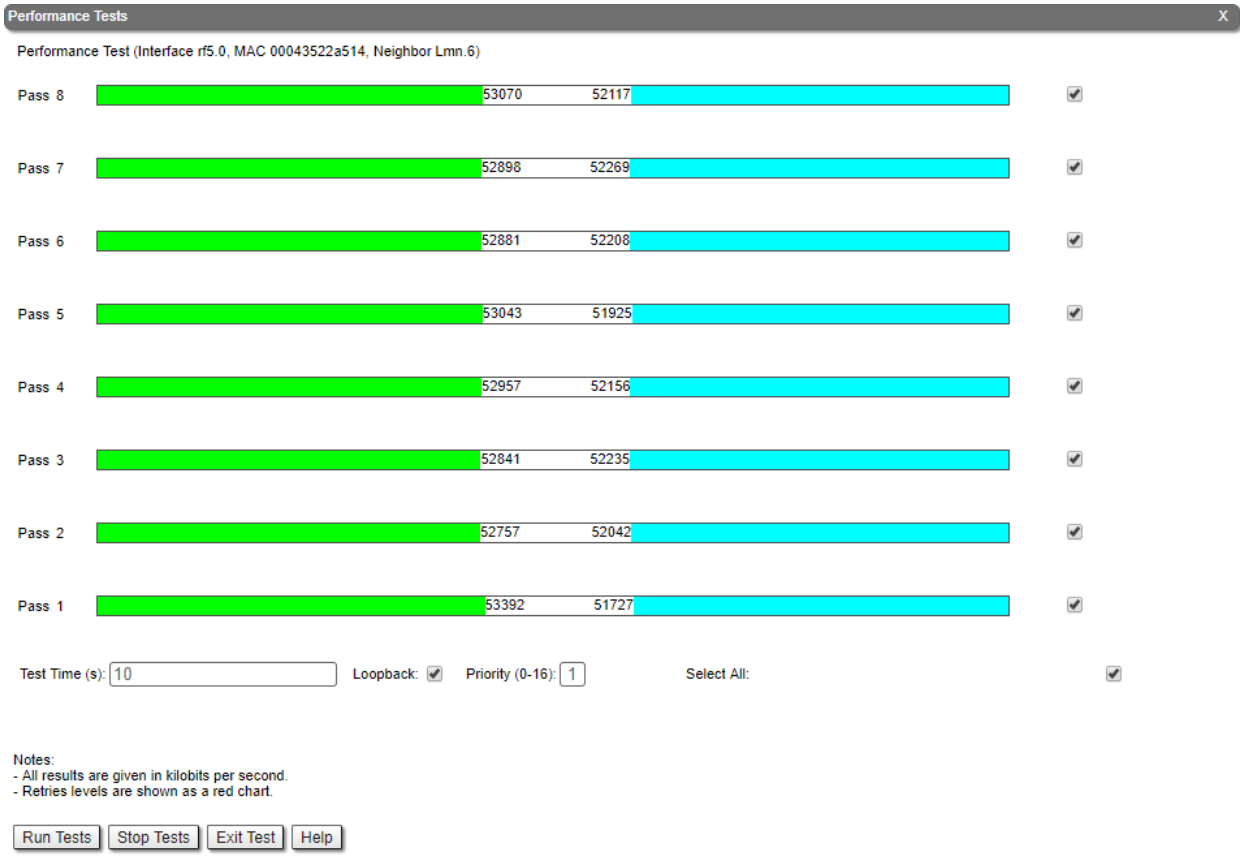


Figure - Performance test in case of "TDMA"

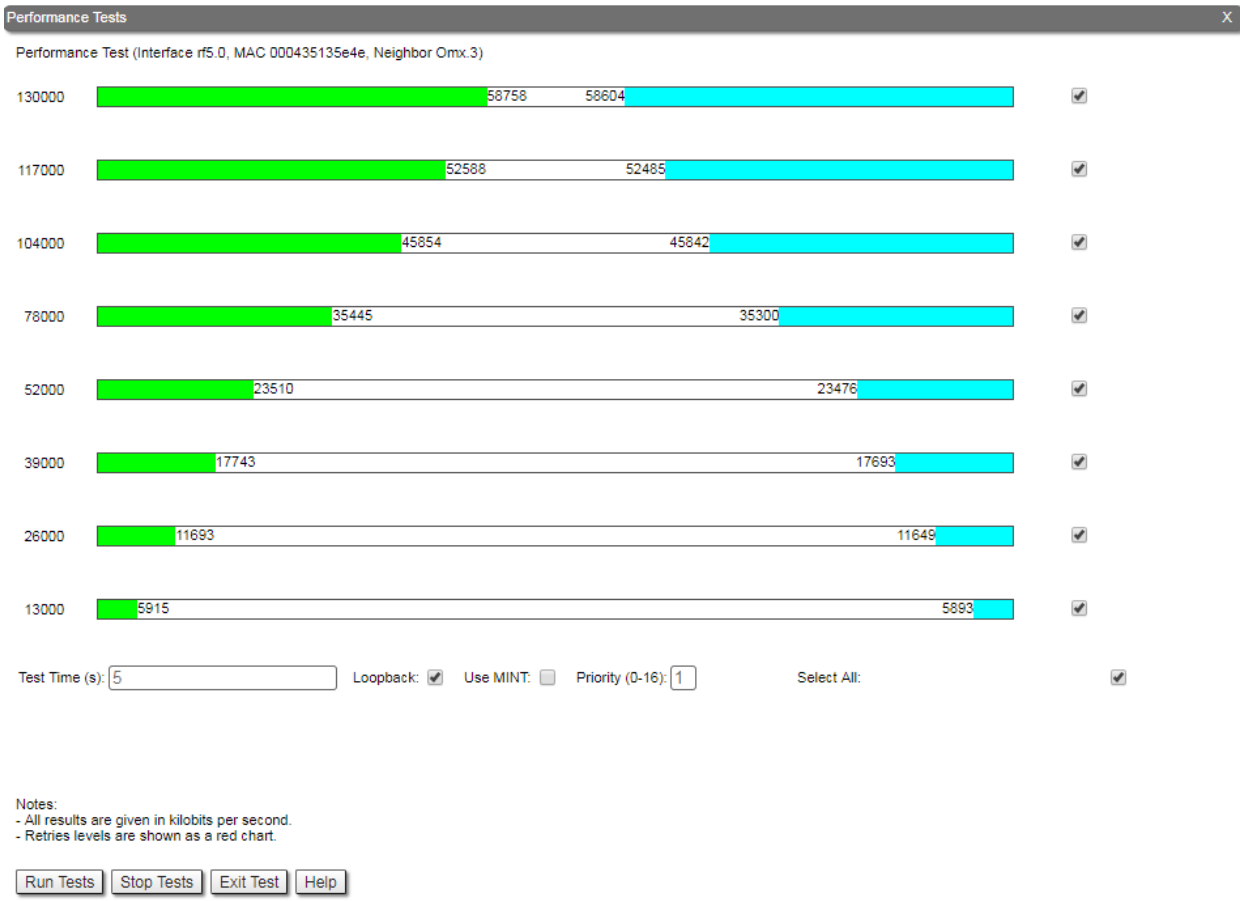


Figure - Performance test in case of "MINT"

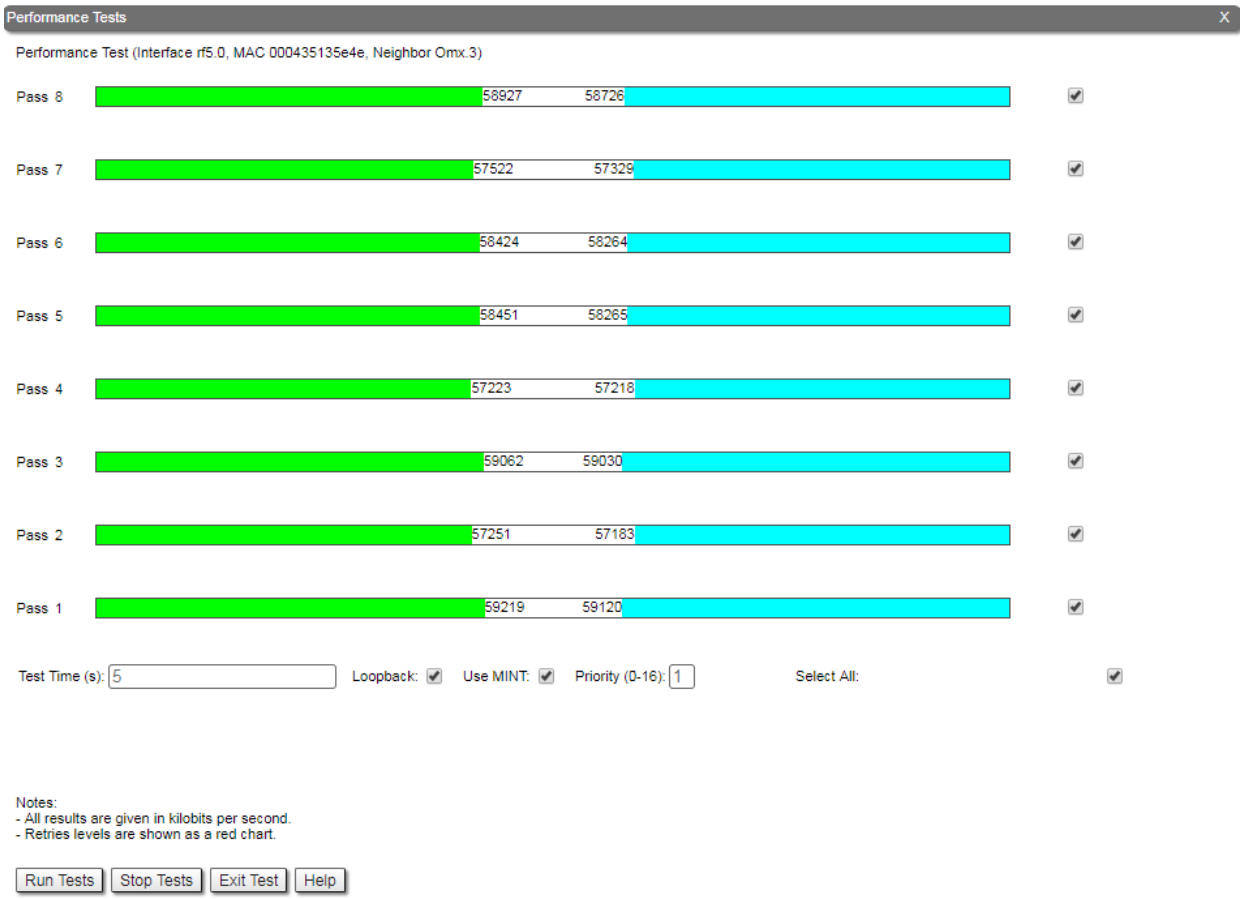


Figure - Performance test in case of "MINT" in "Use MINT" mode

By clicking the «**Run Tests**»/«**Stop Tests**» buttons at the bottom of the page, you can start/stop the performance tests.

By clicking the «**Exit Test**» button, you return to the "Device Status" page.

Each row corresponds to a certain bitrate value and can be selected or deselected for participating in the performance test by marking/unmarking the corresponding check-box on the right side. By marking "*Select all*" check-box, all the bitrates could be selected or deselected at once.

Three more parameters are available for management:

- "*Test time*" parameter - allows setting the duration (in seconds) of the test for each bitrate (5s by default).
- "*Bidirectional*" check-box - allows choosing between bi-directional (when checked) and unidirectional (when unchecked) performance test.
- "*Use MINT*" check-box - performs 8 tests on established bitrate.
- "*Priority (0-16)"* - By default, it is 16, which is lower than the data traffic that has priority 15. You can increase the test priority by setting a lower value.

The bitrates list on the "Performance test" tool consists of the bitrates that correspond to the channel bandwidth set on the unit (5/10/20/40MHz). To perform the tests for the bitrates related to the other channel bandwidth, you need to reconfigure the channel bandwidth (the "*Channel Width*" parameter in the "Radio Setting" section of the "Basic Settings" page) on both units within the tested link.

Examples given:

Bi-directional performance test output description for 180 Mbps bitrate (40 MHz channel bandwidth):

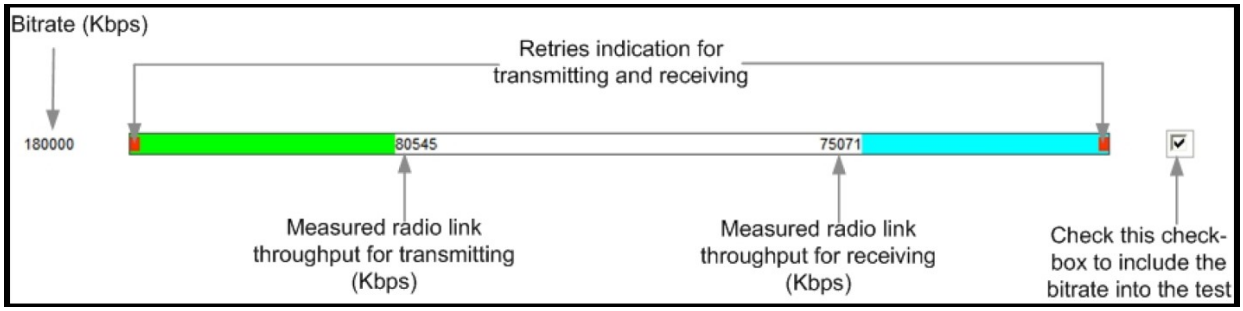


Figure - Bidirectional performance test output

In order to see detailed information about throughput, errors and retries, you can move the mouse cursor over the indication strip of the required bitrate.

Antenna Alignment Tool

The "Antenna Alignment Tool" allows to visualize the signal characteristics on both sides of the link in order to make the antenna alignment process more accurate and easier.

The accuracy of the antenna alignment at the neighbor device is very important for the link quality.

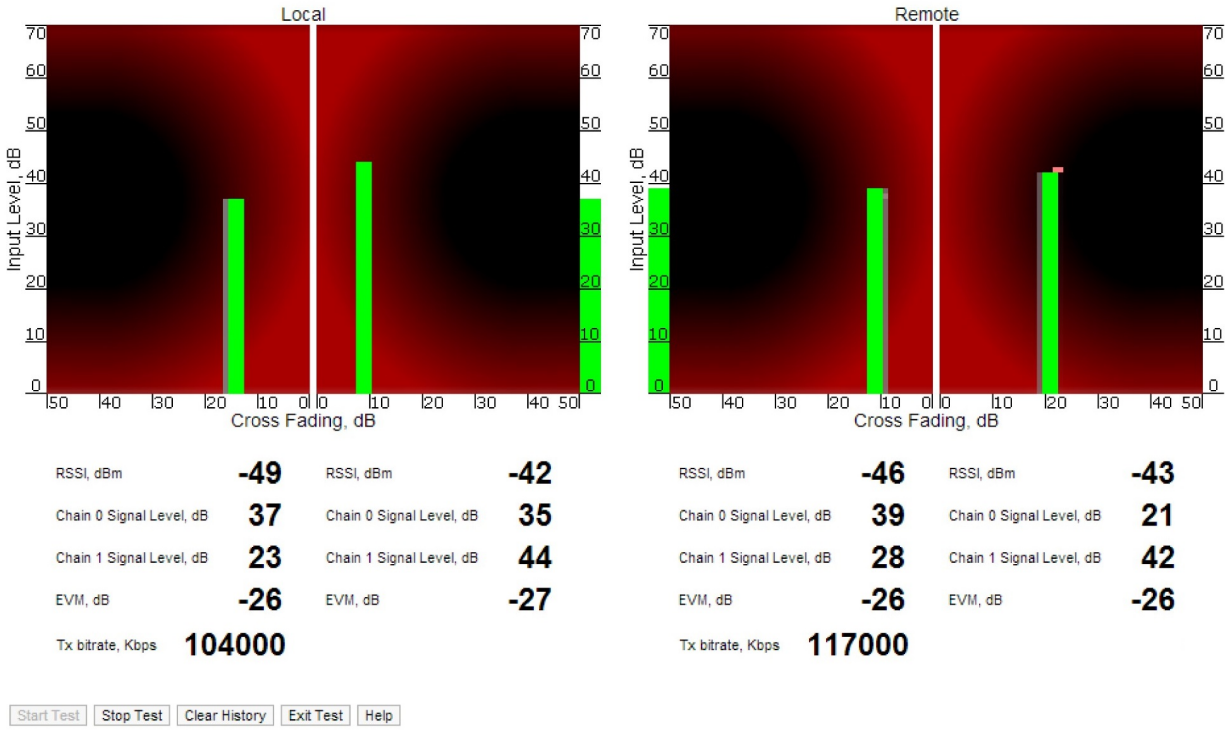


Figure - Alignment test

By clicking the «**Start Test**»/«**Stop Test**» buttons at the bottom of the page, you can start/stop the alignment test.

By clicking the «**Clear History**» button, you delete all data stored from the moment you clicked the «**Start Test**» button.

By clicking the «**Exit Test**» button, you return to the "Device Status" page.

Once the test is started, the antenna alignment can be monitored using the graphic and text indicators. The indicators for both local and remote devices are displayed together in the same page which allows viewing the alignment process for both sides of the link.

Each side of the link (local and remote) has two similar test indicator sets, corresponding to each antenna polarization (one for Vertical polarization and another for Horizontal). This allows controlling the alignment process for each antenna polarization for the local and for the remote device simultaneously.

The text indicators are:

- "*RSSI*" - indicates the power level of the received radio signal (measured in dBm)
- "*Chain 0 Signal Level*" - input signal level (measured in dB) indicator of antenna number 0 (vertical polarization)
- "*Chain 1 Signal Level*" - input signal level (measured in dB) indicator of antenna number 1 (horizontal polarization)
- "*Error Vector Magnitude (EVM)*" - indicator of the measured input signal quality (it should be as high as possible in absolute value; the recommended level is not less than 21 dB; some old firmware had EVM value positive, but most the firmware has negative value, so for the troubleshooting, evaluate the absolute EVM value)
- "*Retries*" - percentage of transmit packet retries
- "*Tx bitrate*" - displays the current bitrate for the remote and local unit (measured in Kbps)

Graphical indicator:

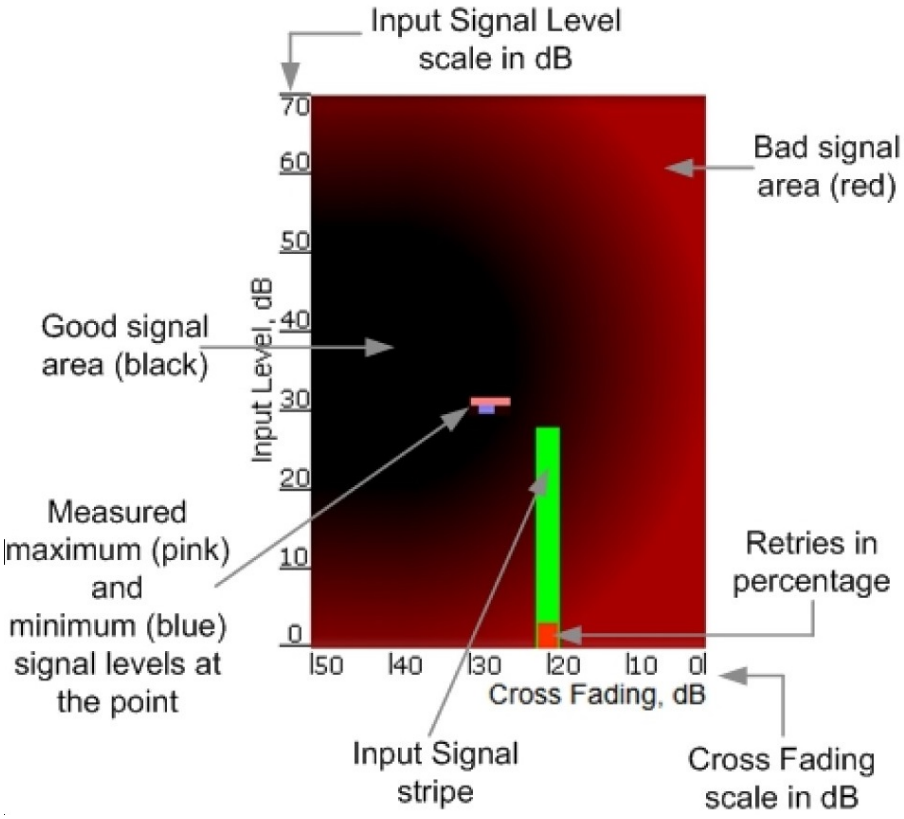


Figure - Alignment test - graphical indicator

The main indicator is the Input Signal stripe.

The height of the Input Signal stripe is measured in dB by the Input Signal Level scale. The higher the stripe is, the stronger the signal is.

The stripe may change its position along the Cross Fading scale, showing how much influence the corresponding device antenna has (for example: how much vertically and horizontally polarized signals influence each other). Higher the value of the stripe according to the Cross Fading scale (the farther stripe is from the 0 dB value), less the influence antennas have on each other.

The top of the Input Signal stripe can be located in black (Good signal) or red (Bad signal) background areas or somewhere in between them. This means the signal is good, bad or average correspondingly. When aligning the antenna, it is recommended to try achieving the stripe top to be located in the black area.

At the bottom of the Input Signal stripe may appear a special red sub-stripe. This sub-stripe indicates the presence of the packet retries and the percentage of the total number of transmitted packets.

During the alignment test, the Input Signal stripe may change its position along the Cross Fading scale and increase or decrease in height, indicating the changes in the received signal. When the top of the stripe changes its location, moving from one point on the background area to another, it leaves pink and blue marks behind, indicating the maximum and minimum measured levels of the signal at a particular point. Thus, it makes possible to observe the “history” of the signal changes.

You can clear the marks by clicking the «**Clear History**» button at the bottom of the page.

Main recommendations when using the “Antenna Alignment" tool:

- It is recommended to start antenna alignment with searching the maximum signal level on a minimal possible bitrate. Afterwards, automatic MINT mechanisms will set the most appropriate bitrate when “*Autobitrate*” mode is enabled
- Input signal level should be between 12dB and 50dB. It is recommended that ATPC to be disabled
- If signal level is more than 50dB, it is recommended to lower the amplifier power
- If maximal signal level is less than 12, it is recommended to lower the channel width (for example: from 20MHz to 10MHz)
- In some cases, a signal level that is less than 12 may be enough for the radio link operation. In this case, you should be guided by parameters such as the number of retries and Error Vector Magnitude. If the number of retries is low (close to “0”) and EVM is more than 21 (Input Signal stripe is green) then the radio link is most likely, operating properly
- Retries value should be zero or as low as possible (less than 5%)
- The top of an Input Signal stripe should be located in the black area
- The signal quality should be good: EVM value should be more than 21
- Input signals of the two antennas of the device should have similar Cross fading values (Input Signal stripes should be symmetrically to the value of 0dB).

ALL described recommendations are applicable to both ("Local" and "Remote") sections.

Link samples:

- Good link sample

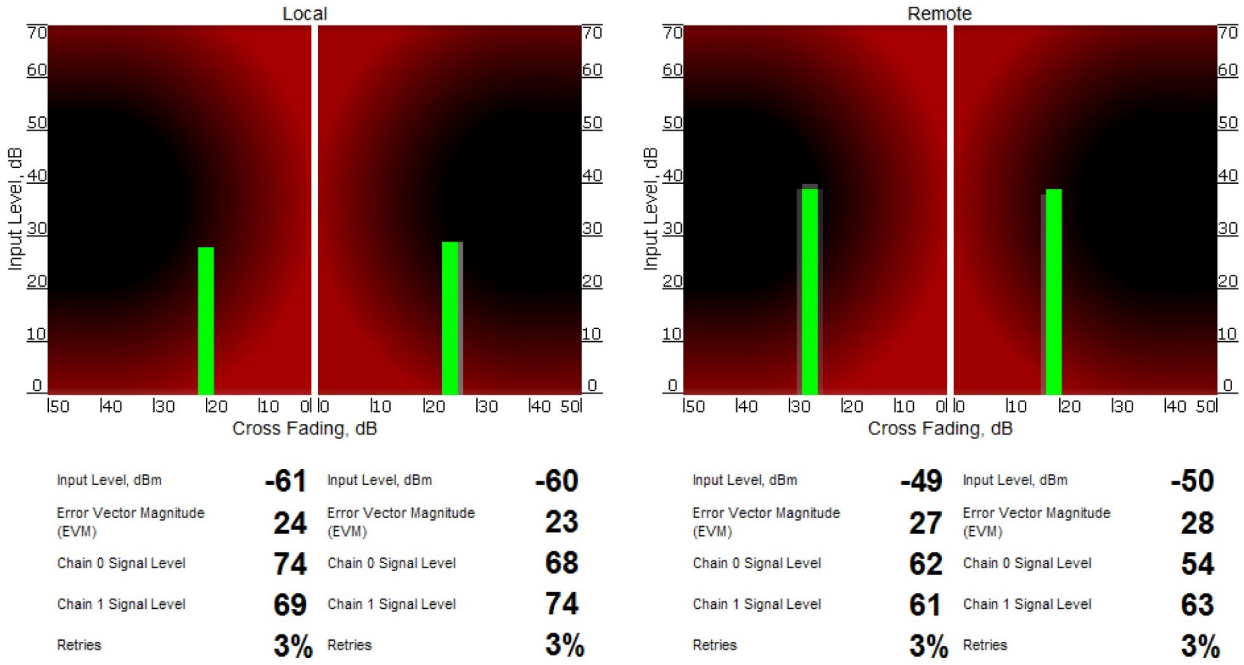


Figure - Alignment test - graphical indicator - positive example

- Bad link sample

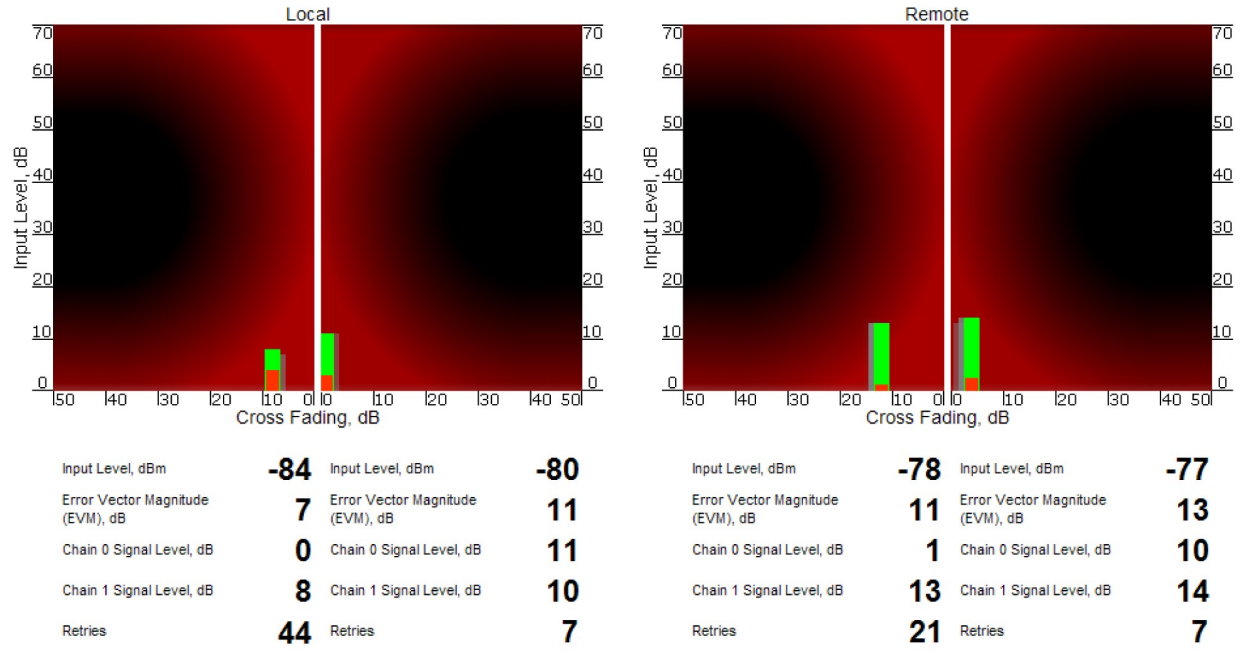


Figure - Alignment test - graphical indicator - negative example

Statistics Graphs

The "Statistics Graphs" tool has been developed based on “*digraphs*”, which is a fast, flexible open source JavaScript charting library.

The "Statistics Graphs" tool allows you to monitor the device parameters represented in the graphical charts. The following modes are available: real-time monitoring, daily and monthly data logs display (use the dropdown menu from the top of the page to change the mode).

The system displays, by default, the daily data logs. All charts support simultaneous zoom to improve usability: the “zoom in” action in a certain region on any of the charts reflects on all other charts that are re-scaled automatically to display the data collected during the same period of time.

Critical events like link outages or frequency swaps are marked by small red balloons on the bottom of each graph. Move the mouse over each balloon for details:

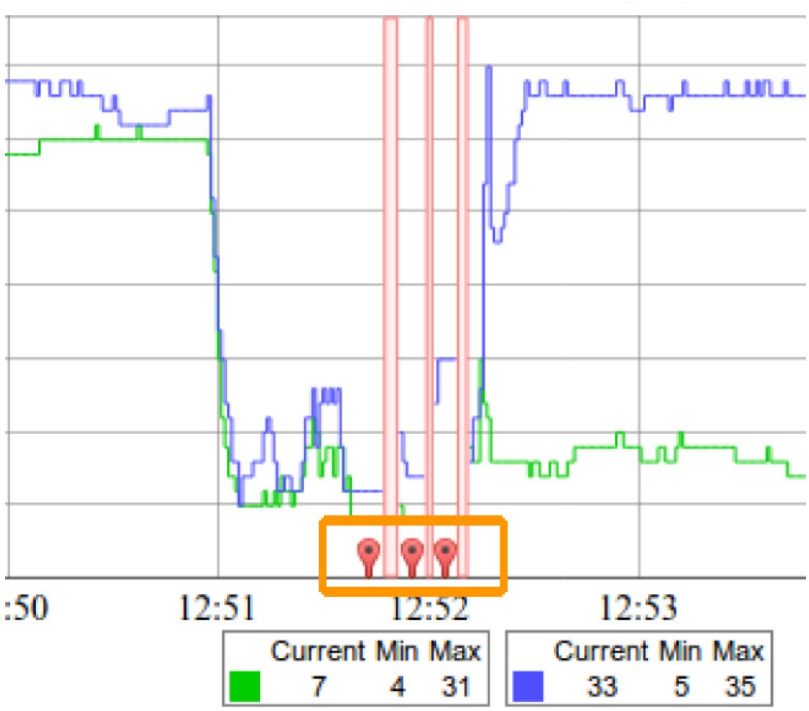


Figure - Statistics graphs - balloon indicators

Working with the charts:

- Select a chart region to zoom in
- Hold the «**Shift**» button and drag the graphs to the pan
- Double-click on any chart to reset the zoom.

The parameters that can be monitored are:

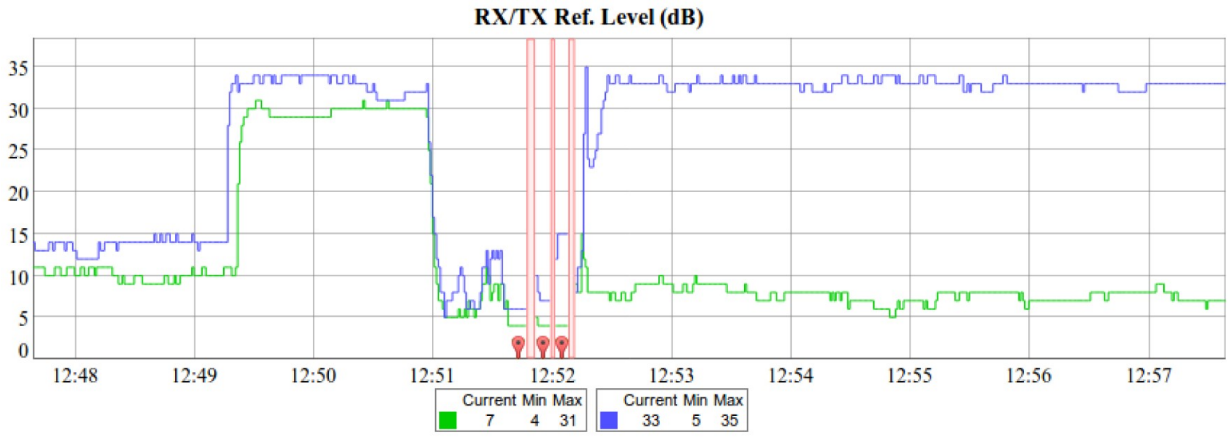


Figure - Statistics Graphs - RX/TX Ref. Level

This chart displays the measured RX (green) and TX (blue) signal levels. Red regions represent link outages. The default graph uses the CINR measurement method; however, the RSSI method can be selected from the drop-down menu.

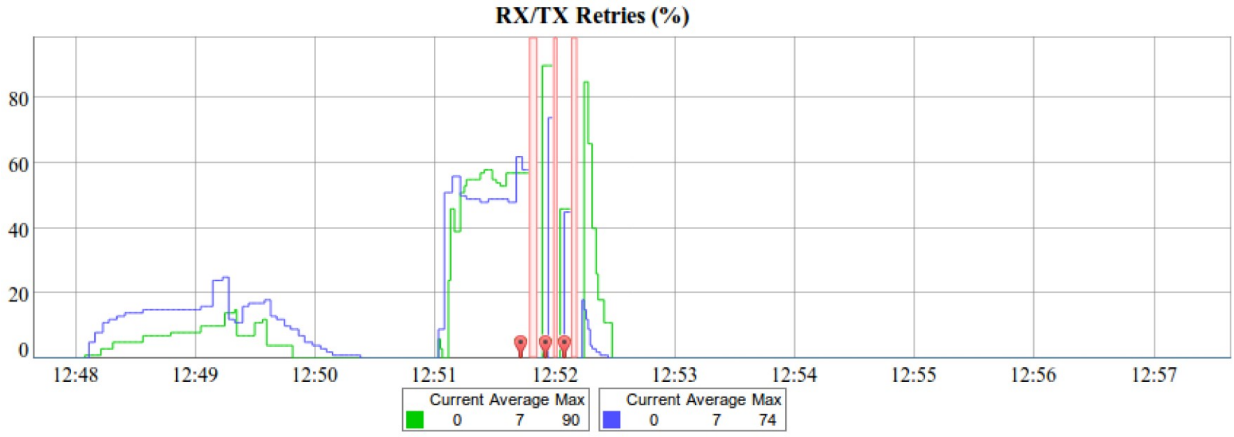


Figure - Statistics Graphs - RX/TX Retries

This chart displays the retry percentage (it provides a quick estimation of the link quality). Similar to the previous graph, RX retries are represented by the green lines, TX retries by the blue lines and link outages by the red lines.

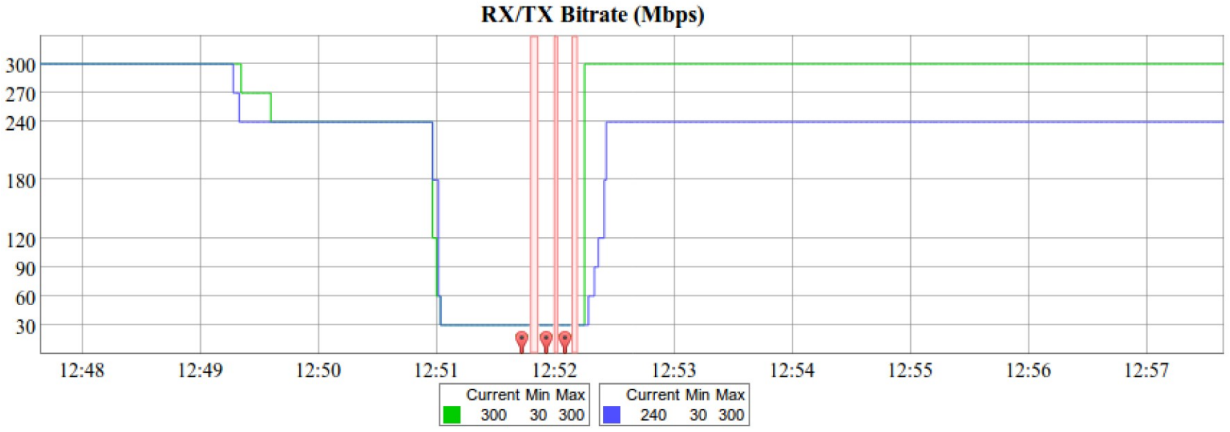


Figure - Statistics Graphs - RX/TX Bitrate

The Bitrate chart displays the bitrate for each of the two units in the link. These parameters indicate the link quality, too.

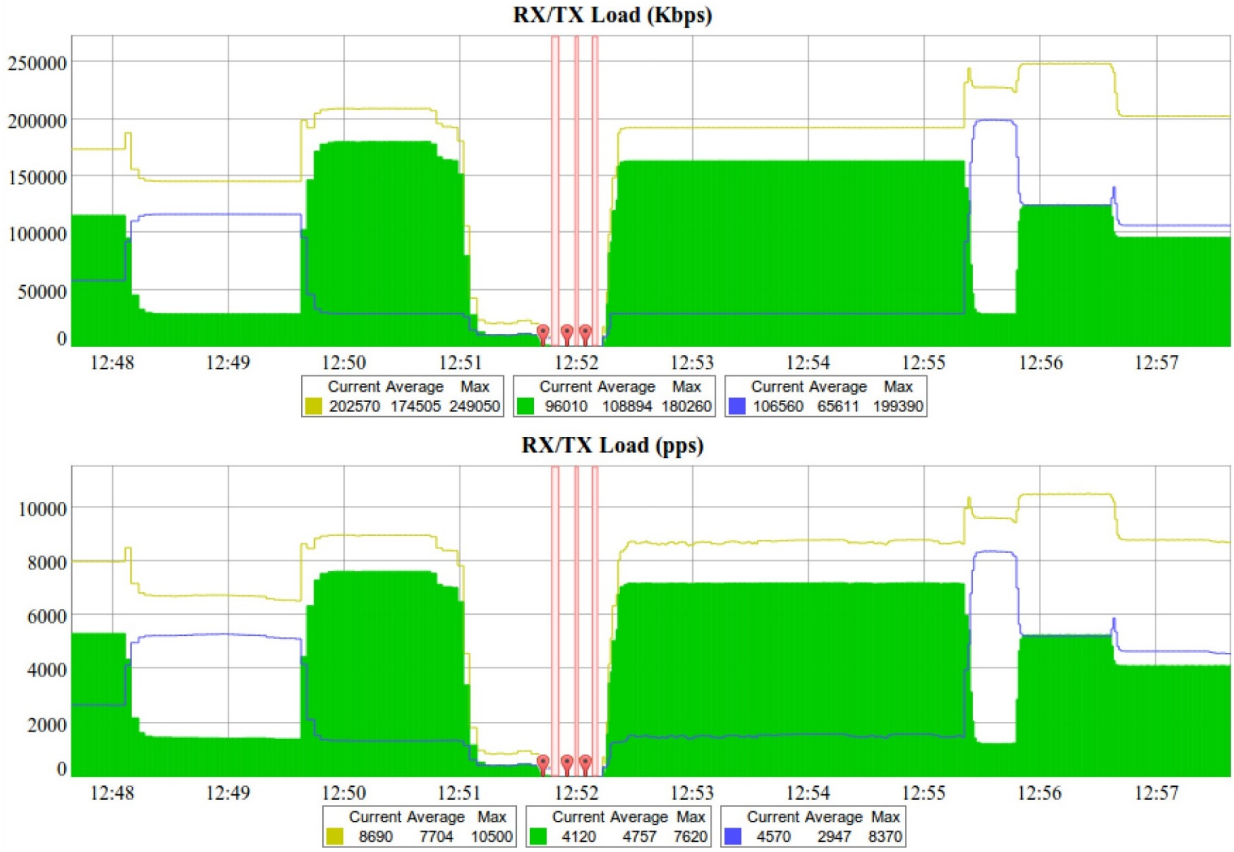


Figure - Statistics Graphs - RX/TX Load

The load charts display the actual link load information, either in real time or for a set period of time. The yellow lines represent the total link load, the green lines represent the RX load and the blue lines represent the TX load.

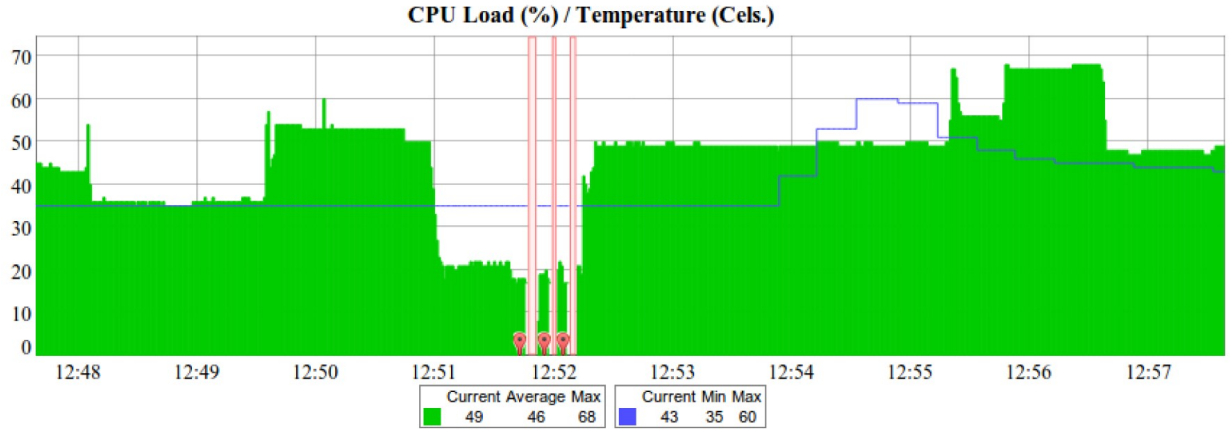


Figure - Statistics Graphs - CPU Load & unit temperature

The last chart displays the current CPU load and unit temperature (only for the units equipped with temperature sensors).

You can view the six graphs presented above into one or two columns per page by clicking the «**Change Layout**» button.

Remote Commands

The "Remote Commands" tool allows one MINT node to perform commands on another or all MINT nodes in the network at L2 level using **WANFleX OS** CLI commands.

Run the string you typed into the "*Command*" field by clicking the «**Execute**» button. For the full list and description of **WANFleX OS** CLI commands, please refer to the WANFleX OS User Manual.

You can set the key grant access to the remote node using the "*Key*" textbox and clicking the « **Execute**» button. Please note that this key must be prior set at the remote node via CLI (commands "*guestKey"*, "*fullKey"* - see details in the WanFlex OS User Manual).

Erase the string you typed into the "*Command*" field and all output from the display section by clicking the «**Clear**» button.

Stop a command execution during the execution phase by clicking the «**Stop Execution**» button.

By clicking the «**Close**» button, you return to the "Device Status" page.

You can choose between plain and rich text format by marking/unmarking the corresponding checkbox.

You can execute the same command from the BS to all CPEs in the network (to the nodes that are linked to the BS) by marking "*Send to all*" checkbox before clicking the «**Execute**» button.

You can upload the configuration file to the remote node by clicking the «**Upload Config…**» button and you can reboot the remote node by clicking the «**Reboot Remote Unit**» button (a warning message pops up before the reboot).

For the ease of usage of the "Remote Commands" tool, the corresponding buttons for the most used **WANFleX OS** CLI commands are available in the right side of the screen:

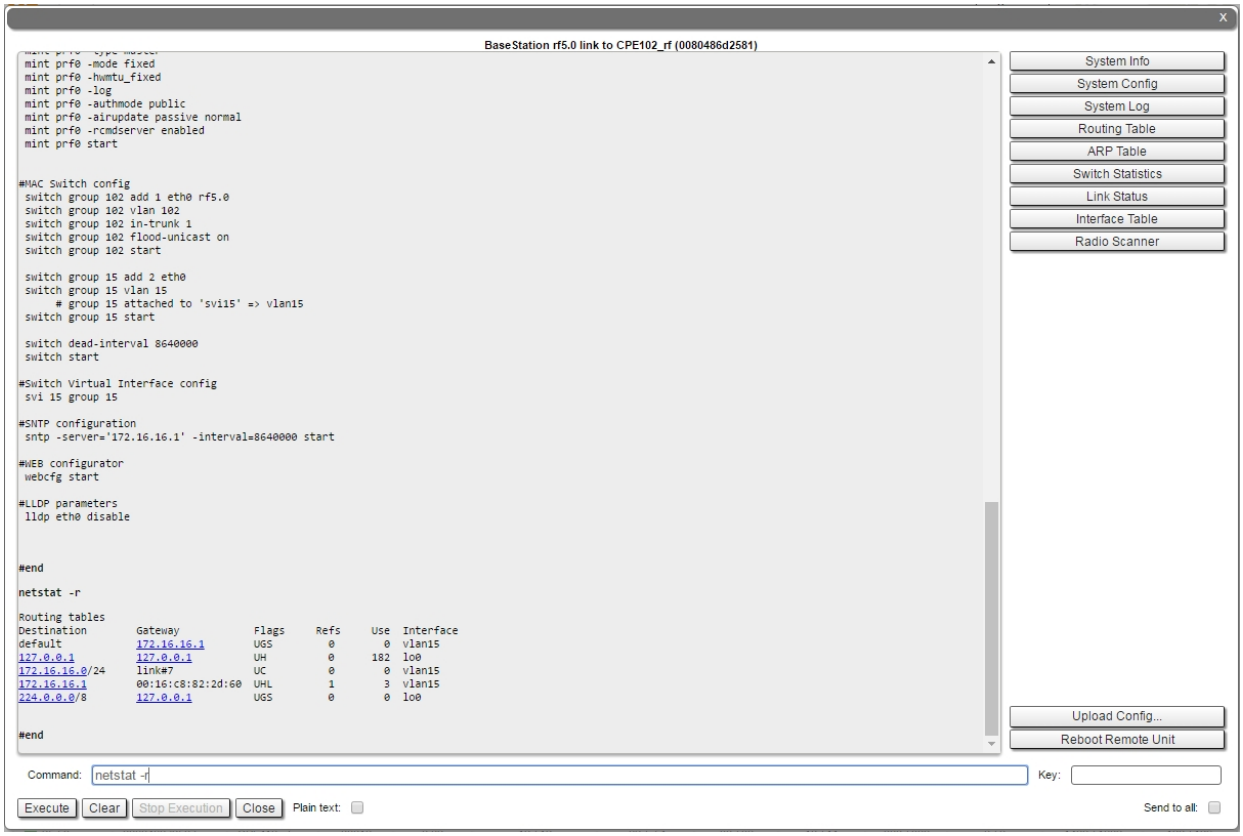


Figure - Remote commands

By clicking the «**System Info**» button, you fill in the command field with "*system version*, *system uptime* and *system cpu"* commands.

By clicking the «**System Config**» button, you fill in the command field with "*system uptime* and *config show"* commands.

By clicking the «**System Log**» button, you fill in the command field with "*system log show"* command.

By clicking the «**Routing Table**» button, you fill in the command field with "*netstat -r"* command.

By clicking the «**ARP Table**» button, you fill in the command field with "*arp view"* command.

By clicking the «**Switch Statistics**» button, you fill in the command field with "*switch statistics"* command.

By clicking the «**Link Status**» button, you fill in the command field with "*mint map detail"* command.

By clicking the «**Interface Table**» button, you fill in the command field with "*netstat-i"* command.

By clicking the «**Radio Scanner**» button, you fill in the command field with "*muffer rf5.0 -t5 -p mac3"* command.

All commands are executed automatically after clicking one of the buttons mentioned above.

NOTE

All **WANFleX OS** CLI commands can be executed from the "Remote Commands" tool.

Link Restart

You can restart the wireless link (re-association, re-authentication and re-connection) by selecting the “**Link Restart**” radio button and then by clicking the «**OK**» button in the link options.

A warning message pops up before the link restart. If the operation is executed, the link disappears from "Device Status" page until it is reestablished again.

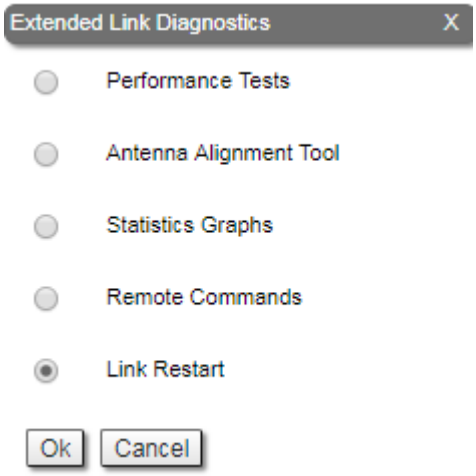


Figure - Link restart

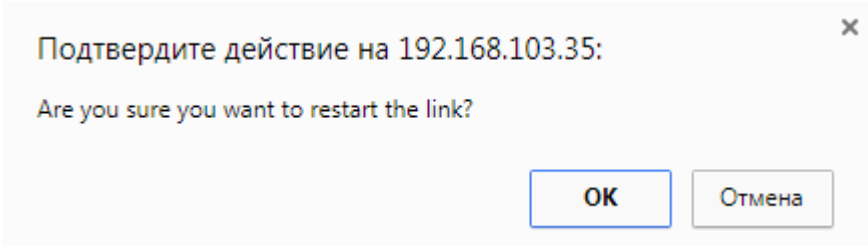


Figure - Link restart - warning message

4.2.6 Extended Switch Statistics

The "Extended Switch Statistics" tools allow gathering complete information and enhanced statistics for each group of the unit.

In order to access the "Extended Switch Statistics" tools, click on the row of each switch group or kernel within the "Switch Statistics" section:

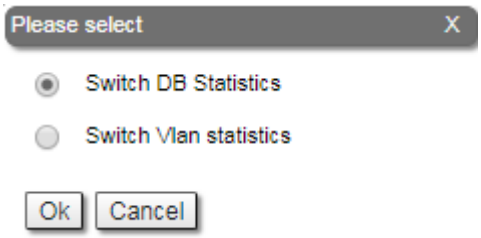


Figure - Extended Switch Statistics

Two options are available: "Switch DB statistics" and "Switch VLAN statistics".

Switch DB Statistics

The "Switch DB Statistics" tool gathers complete information and enhanced statistics for each switch group, including kernel:

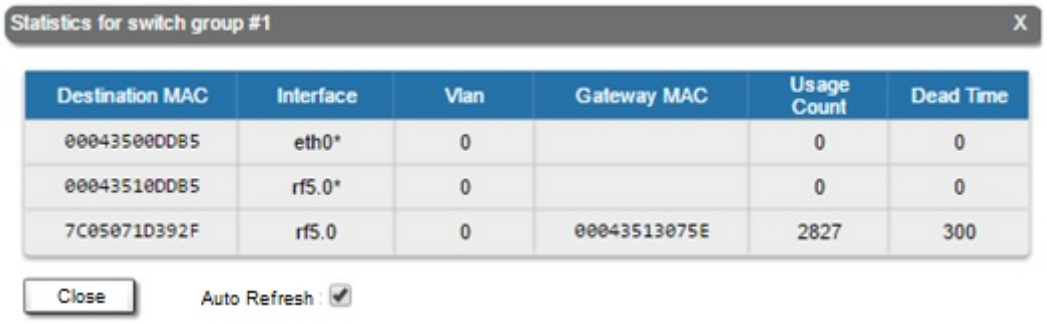


Figure - Switch DB Statistics

By clicking the «**Close**» button, you return to the "Device Status" page.

The "*Auto Refresh*" option is disabled by default. You can enable the auto refresh in order to have the statistics automatically refreshed.

Switch VLAN Statistics

The "Switch VLAN Statistics" tool gathers complete information and enhanced statistics for each VLAN created:

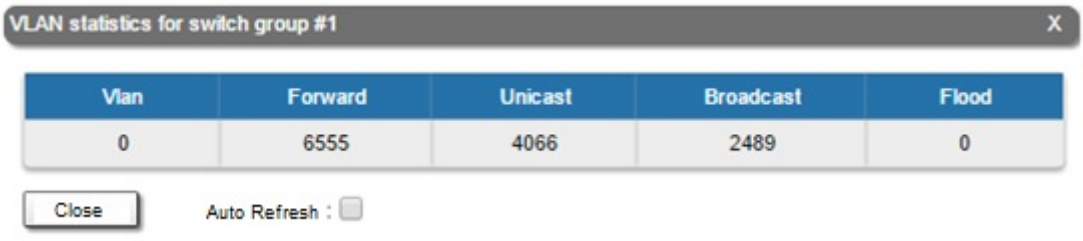


Figure - Switch VLAN Statistics

By clicking the «**Close**» button you return to the "Device Status" page.

The "*Auto Refresh*" option is disabled by default. You can enable the auto refresh in order to have the statistics automatically refreshed.

4.3 Basic Settings menu

InfiNet Wireless R5000 series units can be configured via Web interface, or via Command-line interface.

The parameters for the majority of the Command-line interface commands are displayed in the Web interface. Saving the configuration for these parameters in any of the two interfaces (Command-line and Web) is reflected in both interfaces.

However, for some other commands, the most important parameters can be set via Web interface, but the enhanced parameters of these commands can be set via Command-line interface only. The commands that do not have the enhanced parameters displayed in Web interface are: s*ys, ifconfig, prf, qm, tun, route, mint, switch, svi, lag, sntp, dhcpc* (please consult the information about the Extra Commands section within the current chapter, below).

The settings of these enhanced parameters will be lost after saving the configuration via Web interface.

The warning message below is displayed in the "Basic Settings" page from the Web interface if the configuration has been previously created via CLI, in order to avoid losing data for those only few commands that don't reflect their parameters in the Web interface:

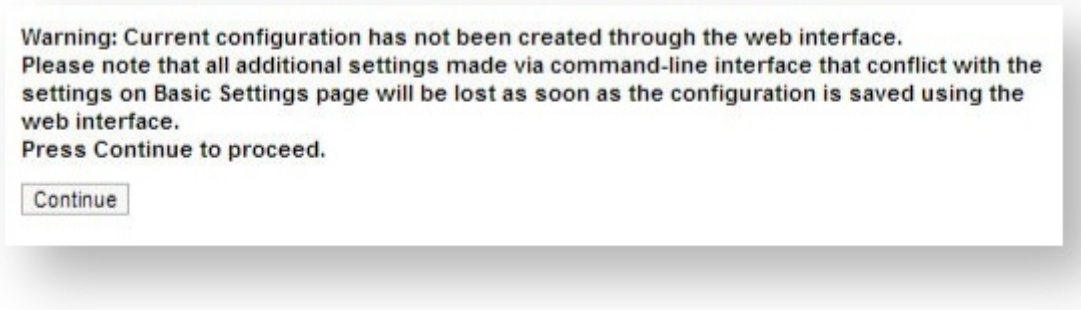


Figure - Basic settings warning message

NOTE

This message is not displayed in the default configuration, but only after the first configuration via CLI.

The "Basic Settings" page has the following sections:

4.3.1 System Settings

In this section, you can view and edit the basic system settings that are already created.

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

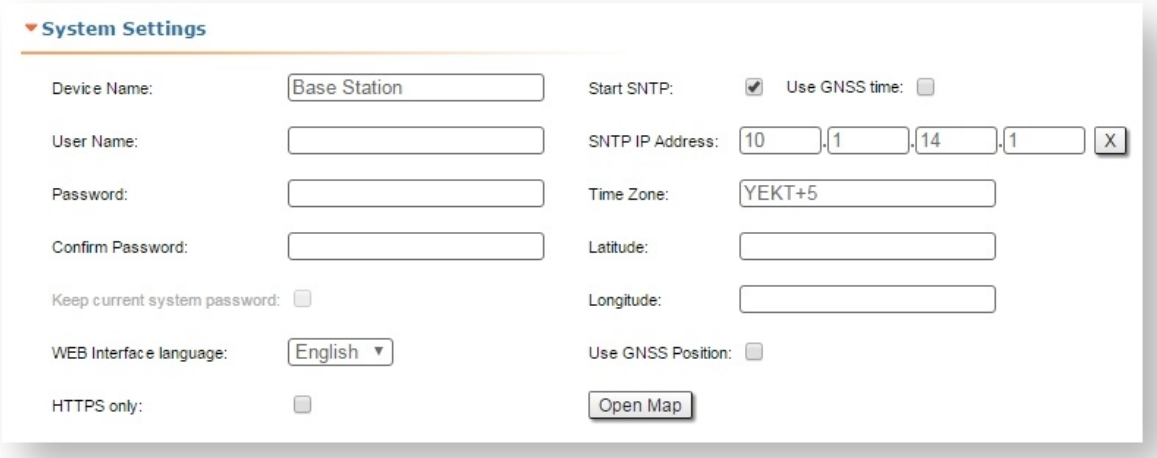


Figure - System Settings default configuration

General System Parameter	Description
Device Name	▪ You can set the device name ▪ This parameter is displayed in the web-page header
User Name	▪ Displays the username (Login) used to access the unit management interfaces ▪ You can change the current username

General System Parameter	Description
Password and Confirm Password	▪ You can change the password set in the previous configuration only after unmarking the option “*keep current system password*" in the corresponding checkbox ▪ You can return to the default settings for "*Password"* and "*User Name"* (any values with non-zero length) by unmarking the checkbox “Keep current system password” and leaving the corresponding fields empty and save the configuration at the bottom of the page
WEB Interface language	▪ You can change the default system language (English) into Russian, French, Italian or Chinese language
HTTPS only	▪ You can set that all HTTP connections to the unit to perform via HTTPS (HTTP with SSL only) by marking the option “HTTPS only” in the corresponding checkbox ▪ By default, this option is disabled
Start SNTP	▪ You can start SNTP service by marking the option “*Start SNTP*” in the corresponding checkbox ▪ By default, this option is disabled ▪ SNTP is necessary for correct time display, for example, in system logs
Use GNSS time	▪ Enable/disable GNSS time ▪ Disabled by default
SNTP IP Address	▪ You can set the IP address of a valid SNTP server ▪ The unit must have an active connection with the SNTP server in order to receive time services

General System Parameter	Description
Time Zone	▪ You can set the time zone in POSIX format. For example: GMT+4
Latitude	▪ You can set the latitude of the geographical place where the unit is installed ▪ GPS latitude format is [N/S]YY.YYYYYY ▪ Use the Google Map feature to automatically fill in this field (follow the indications below)
Longitude	▪ You can set the longitude of the geographical place where the unit is installed ▪ GPS longitude format is [E/W]XX.XXXXXX ▪ Use the Google Map feature to automatically fill in this field (follow the indications below)
Use GNSS Position	▪ Enable/disable GNSS position ▪ Disabled by default

Table - System Settings

Click the «**Open Map**» button to open the Google map:

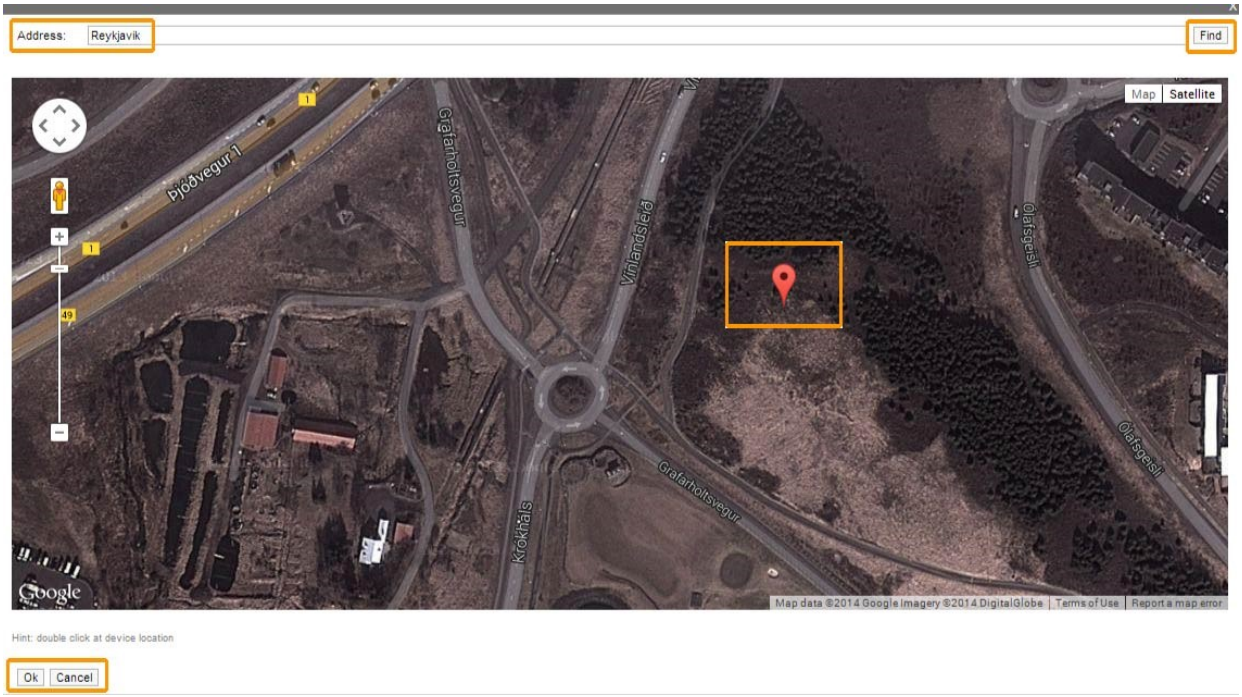


Figure - Google Map

Type the location name in the "Address bar", click the «**Find**» button to search for it and then move to the exact location where the unit is installed. Double click in that position on the map and the Google pointer (see picture above) will be placed there. After clicking the «**OK**» button, "*Latitude*" and "*Longitude*" fields are automatically filled in with the GPS coordinates.

4.3.2 Network Settings

In the "Network Settings" section, there are displayed all physical and logical network interfaces that are already configured. The physical interfaces (eth0 and rf5.0) are set by default and they cannot be removed. For these two interfaces, you are allowed to change the parameters only.

For the following layer 2 and 3 logical interfaces, you are allowed to add (by clicking the corresponding buttons and specifying the interface number), remove and change the parameters of the interface:

- "*Pseudo Radio Interface - prfX*" can be attached to the Ethernet interface in order to allow it to work as a radio interface using the MINT protocol, so that the node can find its neighbors and establish the links with them through this interface. The interface encapsulates MINT-frames into the Ethernet-frames and allows connecting the units of the MINT network using wired interfaces. Also, this interface can be joined with other interfaces;
- "*VLAN - vlanX*" can be assigned to a physical interface or to a virtual interface sviX. It is used for the creation of the logical network topology regardless of the physical topology of this network. VLAN allows creating groups of interfaces which have a common set of requirements. It contributes to reducing the multicast traffic in the network, as every VLAN is a separate multicast domain. VLAN usage increases the network security and manageability;
- "*LAG - lagX*" can be assign to two physical interfaces in order to use them as one logical interface for total throughput increasing and system reliability improving. The total throughput of the logical channel represents the sum of the capabilities of associated physical interfaces. In case of failure of any physical channel included in the logical channel, the system will continue to operate, using the rest operable physical channels. Interface allows creating high speed links (between the unit and the network switch, for example) by means of aggregation of the two available Ethernet-interfaces of the unit (it is intended for **Smn/Lmn** units with 2 Ethernet ports);
- "*Switch Virtual Interface - sviX*" is an L3 interface that can be assigned to a switching group for getting access to the unit management via this switching group. This interface becomes part of this switching group and can participate in the exchange of information with other group members so that any packets received by the group (according to its rules), or addressed to the sviX directly, or copies of multicast/broadcast packets, will be received by the unit through the "*sviX"*. This interface allows getting the remote access to the unit management. It is also used for the Management VLAN configuration;
- "*Tunnel - tunX*" is implemented like a PtP link between two routers that encapsulates the flow into the IP packets and send it to the end point of the link using the existing transport environment. It allows to unite two remote networks (which are not directly connected) in an integrated logical structure (VPNs) which use its own network address allocation and account policies, independent from the ones supplied by the service providers for each of the separate network segments;
- "*TAP - tapX*" interface simulates a link layer (L2) device and operates with Ethernet frames. TAP interface is used for creating a network bridge.

NOTE

Before making the configurations in the "Network Settings" section, please read the information presented in the "MAC Switch" section.

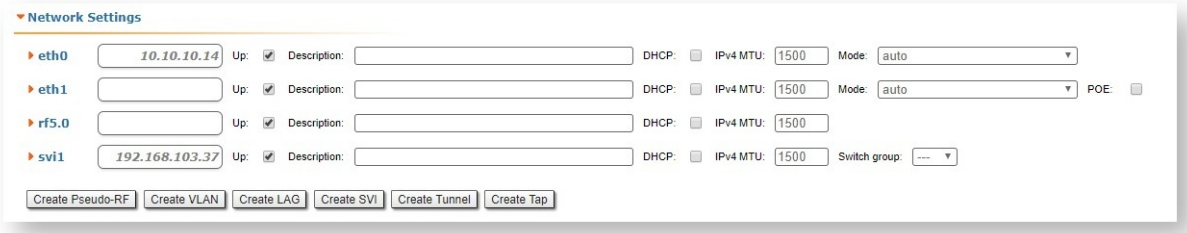


Figure - Network Settings default interfaces

Interface type	Operations
ethX	■ Configure the IP address(es) and the mask of the interface ■ The IP address(es) of the "*ethX"* interface is accessible via Ethernet LAN segment only (it won't be accessible via the "*rfX"* interface from other neighbor unit) ■ The IP address(es) of the "*ethX"* interface is used in the routing process ■ Enable/disable the interface ■ Enable/disable DHCP - obtain an IP address automatically ■ DHCP option is disabled by default ■ Set the interface description (up to 72 characters) ■ Set the interface mode (for example: 1000BaseTX-fullduplex) - the default value is “*Auto*” (recommended) ■ Activate/deactivate PoE: this option is available only for eth1 interface of the units with two Fast Ethernet ports; it is used to ease the CCTV setup or to power up another InfiNet Wireless unit (except **Omx**, **Mmx**, **Um** and **Xm**) - by default, it is deactivated

Interface type	Operations
rfX	■ Configure the IP address(es) and the mask of the interface ■ Enable/disable the interface ■ Enable/disable DHCP - obtain an IP address automatically ■ DHCP option is disabled by default ■ Set the interface description (up to 72 characters)
sviX	■ SVI interface is a logical L3 interface of the switch (solely used for the management of the unit) ■ Configure the IP address(es) and the mask of the interface (as the management IP address(es) of the unit) ■ Enable/disable the interface ■ Enable/disable DHCP - obtain an IP address automatically (as the management IP address(es) of the unit) ○ DHCP option is disabled by default ■ Set the interface description (up to 72 characters) ■ Remove the interface ■ Set the Switch group number which this interface is assigned to (bind the SVI interface to a switch group)

Interface type	Operations
prfX	■ PRF interface makes the Ethernet interface that it is assigned to, to appear as a regular RF interface in terms of the MINT network (for more information please refer to the WANFleX OS User Manual) ■ Configure the IP address(es) and the mask of the interface ■ Enable/disable the interface ■ Enable/disable DHCP - obtain an IP address automatically ■ Set the interface description (up to 72 characters) ■ Remove the interface ■ Set the parent interface to be transmitted the encapsulated packets (assign the PRF interface to the physical Ethernet interface) ■ Set the channel number (from 0 to 3) on which the frames are sent and received by the parent interface ■ Both PRF interfaces (of the two units in the link) must have the same channel assigned in order to establish the wireless link
vlanX	■ Configure the IP address(es) and the mask of the interface in case you use this interface for the management of the unit, only ■ Enable/disable the interface ■ Enable/disable DHCP - obtain an IP address automatically ■ Set the interface description (up to 72 characters) ■ Remove the interface ■ Set the parent interface to be transmitted the encapsulated packets ■ Configure the VLAN tag (or VLAN ID) for the current interface (from 1 to 4094) ■ Enable/disable Q in Q

Interface type	Operations
lagX	▪ Link aggregation interface is a logical interface used to combine multiple physical channels into one logical channel in order to increase link capacity and redundancy (for the units with two physical Ethernet ports) ▪ Configure the IP address(es) and the mask of the interface ▪ Enable/disable the interface ▪ Enable/disable DHCP - obtain an IP address automatically ▪ Set the interface description (up to 72 characters) ▪ Remove the interface ▪ Set the parent interface to be aggregated the encapsulated packets ▪ Enable/disable Fast Mode
tunX	▪ Configure the IP address(es) and the mask of the interface ▪ Enable/disable the interface ▪ Enable/disable DHCP - obtain an IP address automatically ▪ Set the interface description (up to 72 characters) ▪ Remove the interface ▪ Set the tunneling mode: IPIP or GRE
tapX	▪ Configure the IP address(es) and the mask of the interface ▪ Enable/disable the interface ▪ Enable/disable DHCP - obtain an IP address automatically ▪ Set the interface description (up to 72 characters) ▪ Remove the interface

Table - Network Settings

Click the «**Create Pseudo-**RF», «**Create** VLAN», «**Create** LAG» and «**Create** SVI» buttons in order to create the corresponding interfaces in the unit configuration.

In the "Network Settings" section, "Routing Parameters" zone, you can configure the static routes:

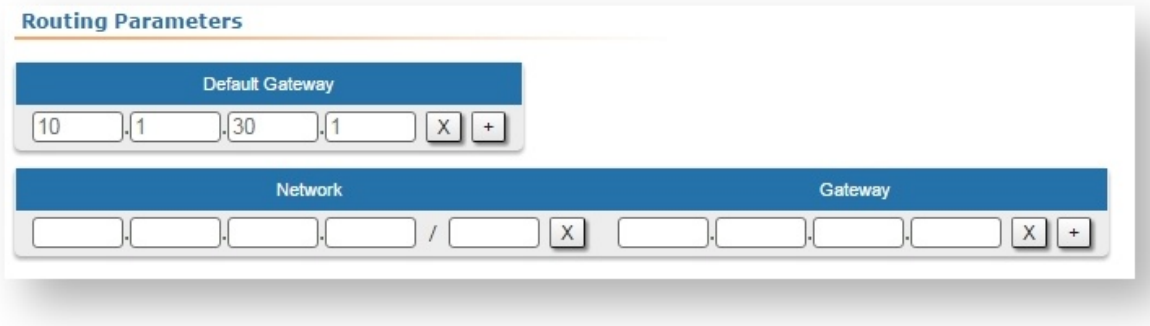


Figure - Static routing configuration

- In the "*Network*" field, you can configure the destination network IP-address
- In the "*Gateway*" field, you can configure the IP-address of the router through which the network address is reachable.

As all wireless MINT interfaces are in one virtual Ethernet segment, they can be enumerated by assigning IP addresses from one IP subnet (manually or automatically, via DHCP). Thus, getting to one node (via telnet, for example), you can access all the other nodes. The access from the "outside" network can be established by configuring the necessary routing, so that the "inner" MINT network can be accessible from the administrator's computer through the Ethernet port of the MINT node which is connected to the "outside" network. From the "inner" MINT network, the route to the administrator's computer should go through the radio-interface to the border router.

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

4.3.3 Link Settings

In the "Link Settings" section you can configure the parameters for the Radio interface, for the Pseudo Radio interface and for the Join function:

Figure - Link Settings section

The "Link Setting" section is consist from the following subsections:

"rf5.0" subsection

This subsection is used for:

- Radio link settings.
- Frequency limitation.
- Setting channel type mode.

Radio link settings

Radio link settings depends from the installed firmware version ("*MINT*" or "*TDMA*"). In the "*MINT*" version Polling technology is used (marker access), in the "*TDMA*" - TDMA technology (time division access).

NOTE

For more detailed information about **TDMA** and **Polling** technologies, their benefits and applications please refer to the document "Application features of TDMA and Polling" - White paper via http://infinetwireless.com/products/materials#white-papers (free registration is required).

Radio settings requirements depending on the technology are described on the following sections:

- Radio link settings in the marker access networks (Polling technology)
- Radio link settings in the time division access networks (TDMA technology)

Radio link settings in the marker access networks (Polling technology)

The marker access mode (Polling technology) can be enabled on the **Master** node.

"rf5.0" subsection is divided in two zones:

- The panel that describes global link settings, in the left side of the page
- The panel that describes the radio channel settings which are currently in use, in the right side of the page.

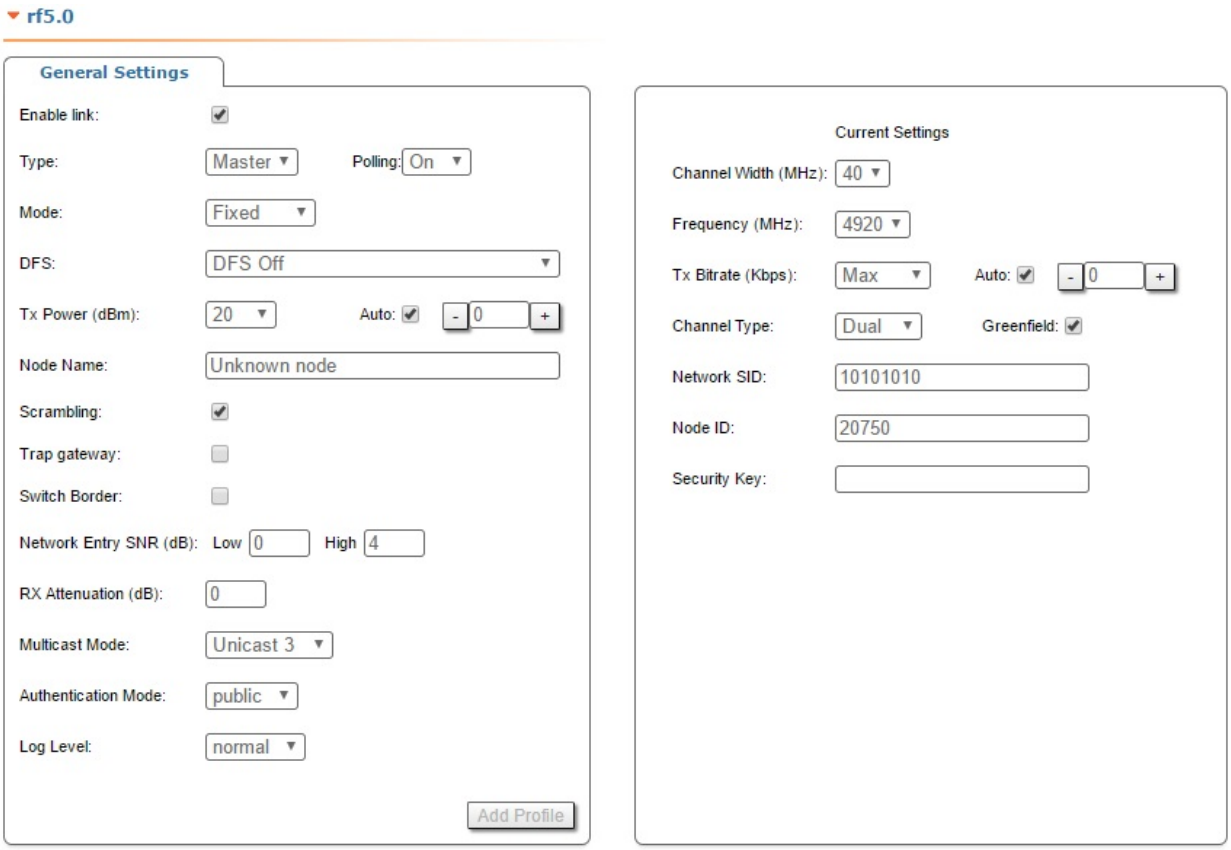


Figure - Master node configuration

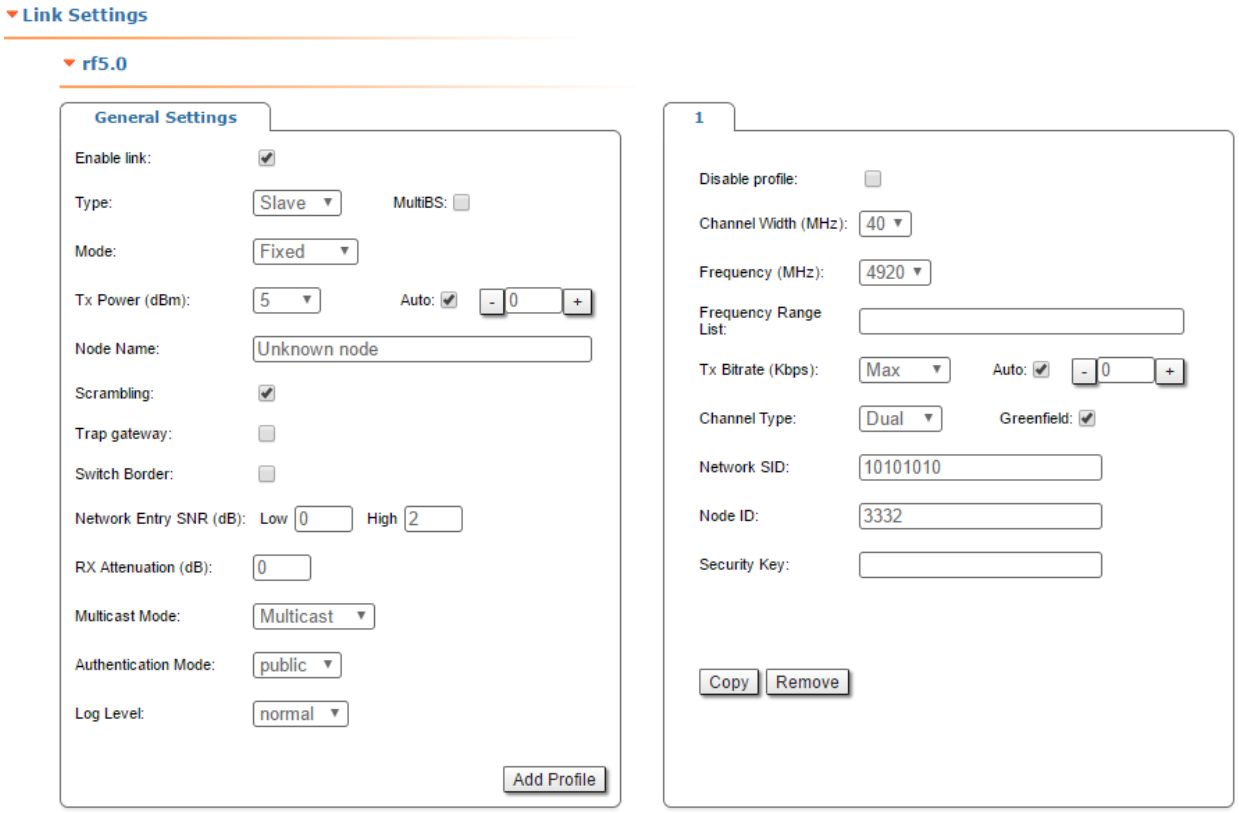


Figure - Slave node default configuration

The slave unit stores the radio parameters for the preferred base stations in radio profiles. Also, each profile consists of a fixed set of radio interface parameters. The heuristic search algorithm can quickly evaluate the general air media parameters and choose the profile which defines the most suitable network.

For example,

- It is suitable to configure radio profiles for the Slave units (with complete radio parameters of each BS) in a PtMP deployment when the CPEs can be linked to more than one BS either in fixed, nomadic or mobile situations, for the redundancy purpose (different profile for each BS). When the CPE tries to establish a wireless connection, it chooses the BS with the best link quality (determined by the RSSI, SNR, bitrate, number of errors, number of retries, etc.). If the connected BS is down, the CPE retries to connect to it and after a number of unsuccessful attempts, it searches to connect to a new BS if the SNR allows it and if one of its radio profiles matches with the radio parameters of the new BS (in case of "MultiBS" option disabled)

The frequency roaming feature (which is enabled in the default configuration) allows the CPE with auto frequency set (roaming enable) to:

- Automatically switch from the main BS (roaming leader) to the backup BS (if it is provisioned with the radio profiles of both BSs)
- Automatically switch between different BSs while the CPE is moving (if it is provisioned with the radio profiles of the BSs)
- Automatically switch to the new frequency of the BS in case the current frequency was changed by the BS.

Data traffic is not interrupted during frequency roaming.

Parameter	Description
General Settings	
Enable link	▪ Enable/disable wireless link (enabled by default)
Type	▪ Set the node type to Master or Slave ○ **Master**: can establish connections with all other types of nodes. It is able to form a network of any topology with other master nodes. A master node is usually used in the configuration of the both sides of the PtP links and in the configuration of the BS for the PtMP links. For master node only, the marker access (polling) can be enabled. Only one master node from a network segment can have this option enabled by means of which it is forming a star-topology segment (PtMP). With this, all other nodes break their connections with their respective neighbors (with exception of connections formed by Join). This node type is usually used for static networks with no (or very small) nomadic or mobile clients. ○ **Slave**: can only connect to master type nodes (the connection cannot be established between two slave nodes). A slave node is usually used in the configuration of the CPE.

Parameter	Description
MultiBS (Slave)	▪ Enabled: the CPE will immediately initiate the search for a new BS ▪ Disabled: the CPE will have more attempts to re-establish wireless connection to the lost BS ▪ It is available for Slave node only
Mode	This setting determines the operating mode of the device. The operating mode is determined by the application of this node in the network. ▪ **Fixed** - the node has a fixed position in the network, it is constantly on. It is a core node of the network. Recalculation of the MINT connections cost in this mode will occur every 3 seconds. ▪ **Nomadic** - the node can change its geographic location, but data exchange within the network, as a rule, occurs when the node does not move. The cost of MINT connections will be recalculated every 1.5 seconds. ▪ **Mobile** - the node often moves. Data exchange take place during the movement . Recalculation of the cost of MINT connections will occur every second.
Polling (Master)	▪ Set the polling mode: ○ *"Off"* - Polling disabled. ○ *"On"* - unit operates in "Polling Master" mode. ○ *"QoS"* - Polling operates taking into account the traffic priority for uplink. ▪ It is strongly recommended to keep Polling on at all times to maximize the link performance ▪ Polling is required for PtMP systems and long haul PtP links ▪ Can be enabled on master node only

Parameter	Description
DFS (Master)	▪ Enable/disable DFS ▪ If “*DFS only*” is set, the DFS system monitors interferences but does not perform radar detection ▪ If "*DFS with Radar Detection*" is set, the DFS system monitors interferences and performs radar detection ▪ For the two radios base stations, the “*Instant DFS*” option is available (one of the two radios is used for DFS scanning, Radar detection and Spectrum analyzing)  **CAUTION** Please note that, in some countries, switching “DFS off” and/or failing to detect public service radar signals are against the regulations and may result in legal action.
Radar Detection (Slave)	▪ Enable/disable "*Radar Detection"* features (a special license with the country code is necessary) ▪ The DFS system performs radar detection and if a radar signal is detected, that frequency is marked as occupied and it can be used again only after a hold-down interval (the link is switched automatically to another frequency)
Max Links (Master)	▪ Maximum allowed number of connected CPEs (in the case of radio connection) . When this value is reached, other attempts to connect to the base station will be rejected

Parameter	Description
Tx Power	▪ Set the output power of the radio interface ▪ Acts as a top limit for the output power control if the ATPC mechanism is turned on ▪ Two operating ranges of Tx power are available: ▪ “-10...10” (if chosen top limit is 10 dBm or less) ▪ “0...27” (if chosen top limit is from 10.5 dBm to 27 dBm) ▪ By default, it is turned on (it is strongly recommended to remains “on”) ▪ The offset parameter is used to adjust the thresholds
Node Name	▪ Set the name for this node in the network ▪ By default, it is the "*Unknown*" node ▪ This node name will appear on the neighbor lists
Scrambling	▪ Enable/disable the data scrambling to improve the connection stability (enabled by default)
Trap gateway	▪ Enable/disable gateway for SNMP-traps
Switch border	▪ Enable/disable the switch border mode. In this mode the unit operates as a "borderline" between the MINT domains, i.e. prevents the distribution of information about the switch groups and data transfer between these domains, while retaining all the capabilities of the MINT protocol (obtaining information about the whole MINT network, sending remote commands etc.)

Parameter	Description
Network Entry SNR (dB)	▪ "*low*" - this option sets the minimal signal level for the neighbor. Signal level is measured in dB above the noise threshold for the current bitrate. If the level gets lower than specified value the connection with a neighbor will be lost. ▪ "*high*" - this option sets the minimal SNR for a new neighbor. Signal level is measured in dB above the noise threshold for the current bitrate. If neighbor's signal level is equal or higher than a specified value the node will consider this neighbor to be a candidate
RX Attenuation	▪ The noise level measured by the radio module is calculated as the minimum received signal level (RSSI) in a certain period ▪ The "*RX Attenuation*" parameter allows manually raise noise threshold on several dB. In this case the radio module won't react to signals below the established threshold. In certain cases it gives the ability to be protected from the low signals interferences which disrupt the radio module as a result of capture effect. This effect is expressed in the fact that the radio module having captured the low signal from the foreign source, tries to strengthen it and to accept completely ignoring a strong signal from the client which has appeared later ▪ This parameter allows to protect the receiver from the powerful signal source overload

Parameter	Description
Multicast Mode (Master)	▪ Traffic transmission mode: ○ "*Multicast*" - conventional mode that uses modulation one step lower than the lowest modulation among the traffic receivers when transmitting the "*multicast/broadcast*" frames. In the case of "*multicast*" streams information from "*IGMP Snooping*" module is used to obtain a list of subscribers. Consequently, the list of all connected sector clients is used for the "*broadcast* " traffic. ○ Transformation of "*Multicast*" to "*Unicast*". In case two or more clients are assigned to the same "*multicast*" stream a copy of source stream will be sent to each of them in the "*Unicast*" mode. ○ "*Unicast 2", "Unicast 3", "Unicast 4", "Unicast 5"* - the number of subscribers limitation. Conventional "*Multicast* " mode will be used when the number is exceeded. ○ "*Unicast All*" - transformation is always executed. Transformation to "*Unicast*" requires memory data copying that increases CPU load. Besides, the use of "*Unicast*" streams increases the volume of transmitted traffic proportional to the number of subscribers and reduces the sector available throughput.  **NOTE** "*Unicast 3*" mode is set by default.  **NOTE** Transformation of "*Multicast*" to "*Unicast*" via CLI is described in the section "mint command".

Parameter	Description
Authentication Mode	▪ Set the mode: ○ *"static"* - the unit can establish connections only with units, which MAC-addresses are listed in the "Static Links" section ○ *"public"* - the unit can establish connections with any other units which have the same security key and the corresponding wireless connection settings ○ "*remote*" - centralized authentication method suitable for point-to-multipoint connections. It assumes the storage of the end node keys within the MINT network both at the base station and at other nodes directly connected to the base station.
Log Level	▪ Set the log level: ○ *off* ○ *normal* ○ *detailed*
Current Settings	
Channel Width	▪ Set the bandwidth of the radio interface in MHz ▪ It must be the same at both ends of the link
Frequency	▪ Set the radio interface frequency (in MHz) ▪ It must be the same at both ends of the link ▪ If it is set to “*Auto*”, the Slave node is scanning on all frequencies for the Master nodes

Parameter	Description
Frequency Range List	▪ Set the frequencies that are allowed to be chosen by the DFS mechanism (available only when the DFS system is enabled) ▪ It is available to support the legacy products ▪ Note that this option is different from the "*Customer Frequency Grid*" tool which allows narrowing down the frequency range available in the "*Frequency*" option from the Radio profile
Tx Bitrate	▪ Set the maximum operating bitrate of the radio interface (from 13000 to 130000 Kbps) ▪ Acts as a top limit for the bitrate if the Autobitrate mechanism is turned on ▪ By default, it is turned on (it is strongly recommended to remains “on”) ▪ Adjust the Autobitrate system thresholds when the remote SNR doesn’ t have the normal level
Channel Type	▪ The channel type can be set as: ○ Dual: enables MIMO operational mode with different Tx and Rx data streams (recommended) ○ Single: allows to operate as MIMO with duplicate Tx streams, MISO or SISO depending on the Tx/Rx chain configuration (description below) ▪ InfiNet MIMO 2x2 technology effectively doubles the spectrum efficiency and allows to achieve a real throughput up to 280 Mbps in 40 MHz band

Parameter	Description
Greenfield	▪ Enable/disable the "*Greenfield*" mode ▪ When activated, the "*Greenfield*" mode increases the link performance by 10-15%, by reducing the packet overhead (optimizes the frames transmitted via the RF link) ▪ "*Greenfield*" mode must be enabled at both ends of the link (the wireless link does not establish if "*Greenfield*" mode is enabled at one end of the link and disabled at the other end of the link)
Network SID	▪ Set the network system identifier (up to 8-digit HEX figure) ▪ It must be the same at both ends of the link
Node ID	▪ Set the device identification number ▪ The parameter is optional ▪ Node ID can be configured by the administrator for a better representation of a neighbors table (nodes within a wireless network)
Security Key	▪ Set the secret key word for encoding of the protocol messages ▪ It must be up to 64 characters long, without spaces ▪ It must be the same at both ends of the link

Table - Radio settings parameters in the marker access networks

On each radio profile, the following options are available (for the **Slave** unit only):

- "**Disable profile**" check box disable a radio profile
- Add a new radio profile by clicking the «**Add Profile**» button
- Copy the radio profile values to a new radio profile by clicking the «**Copy**» button
- Remove the radio profile by clicking the «**Remove**» button.

Radio link settings in the time division access networks (TDMA technology)

Time division mode must be set on **Master** node.

"rf5.0" subsection is divided in two zones:

- The panel that describes global link settings, in the left side of the page
- The panel that describes the radio channel settings which are currently in use, in the right side of the page.

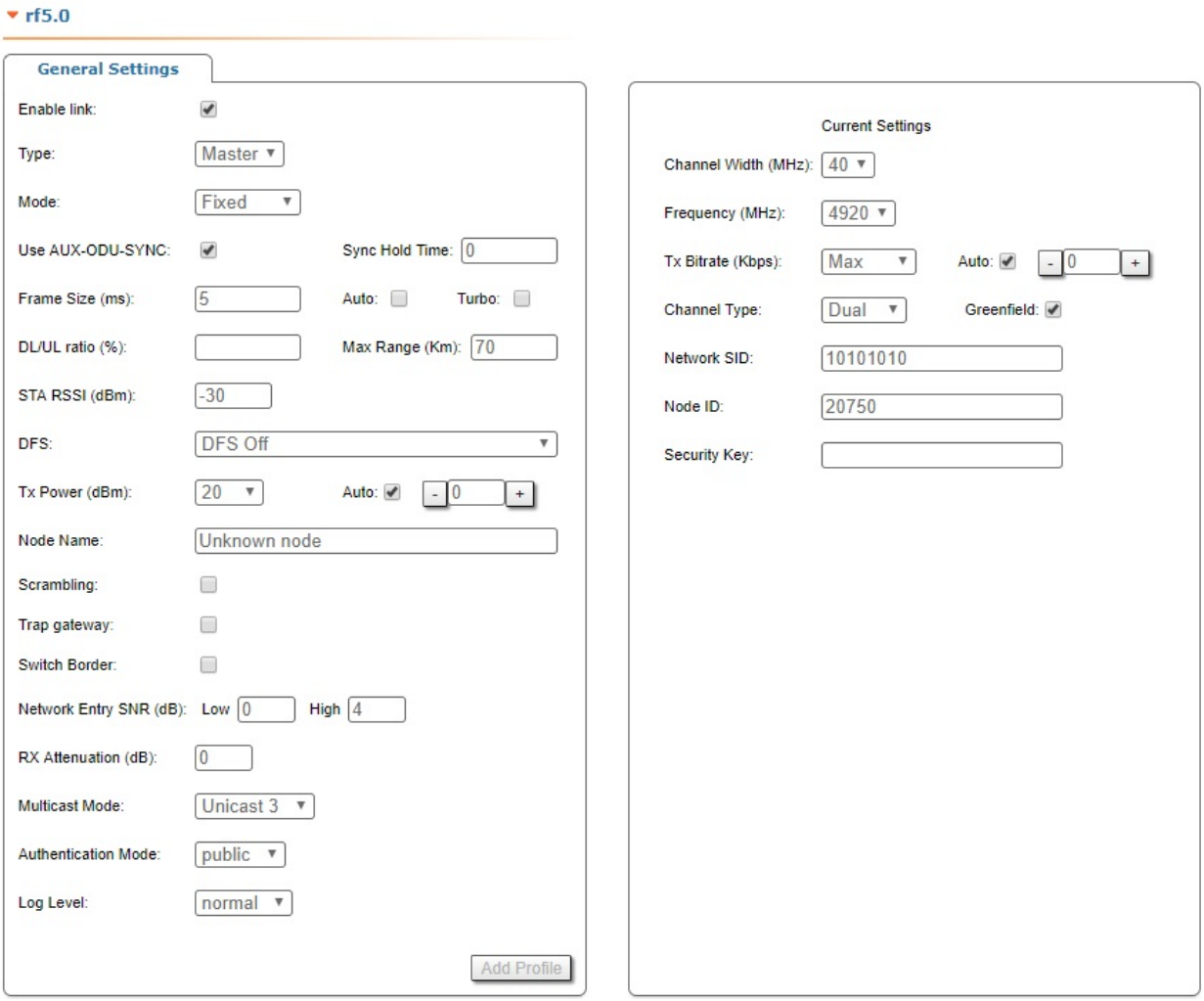


Figure - Master node configuration

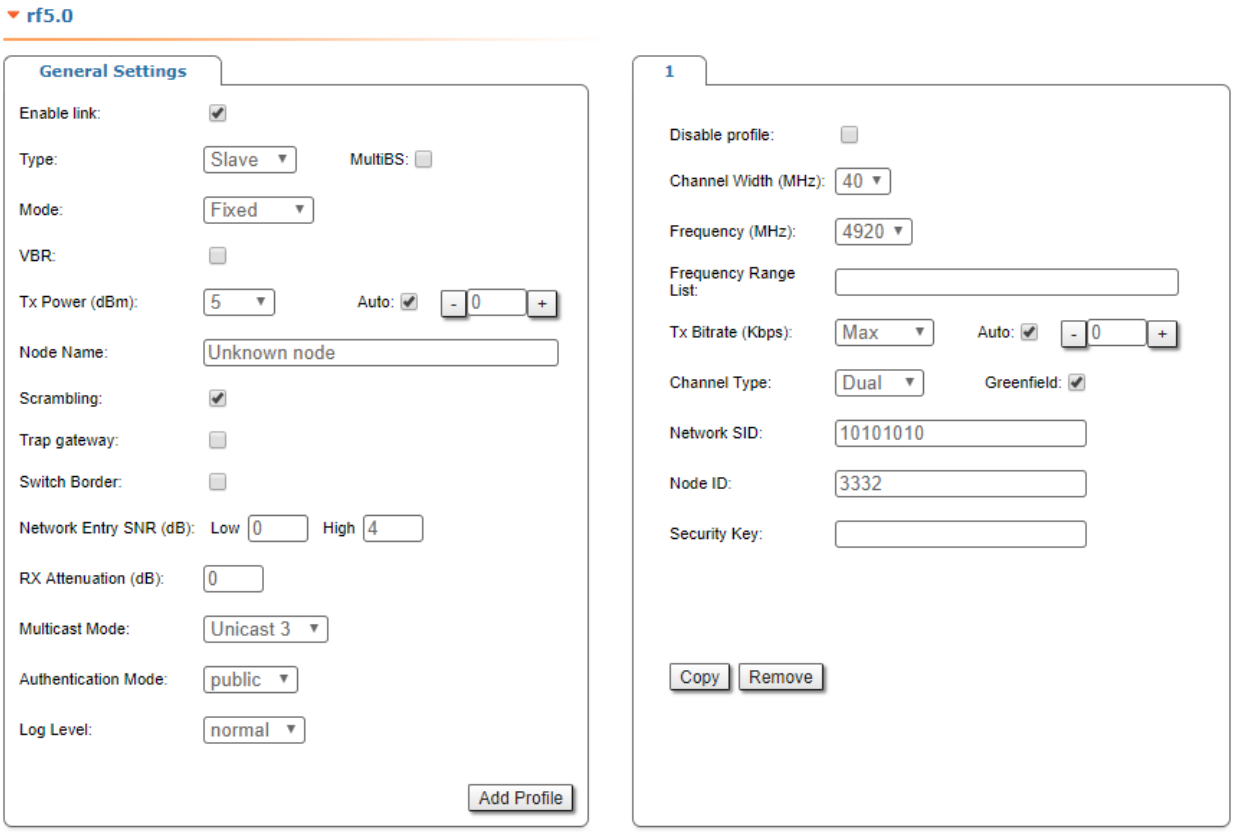


Figure - Slave node configuration

Parameter	Description
General Settings	
Enable link	▪ Enable/disable wireless link (enabled by default)
Type	▪ Set the node type to Master or Slave ○ **Master**: can establish connections with all other types of nodes. It is able to form a network of any topology with other master nodes. A master node is usually used in the configuration of the both sides of the PtP links and in the configuration of the BS for the PtMP links ○ **Slave**: can only connect to master type nodes (the connection cannot be established between two slave nodes). A slave node is usually used in the configuration of the CPE.

Parameter	Description
MultiBS (Slave)	▪ Enabled: the CPE will immediately initiate the search for a new BS ▪ Disabled: the CPE will have more attempts to re-establish wireless connection to the lost BS ▪ It is available for Slave node only
VBR (Slave)	▪ The mode at which the service information is carried out at above a minimum bitrate (if possible)
Radar Detection (Slave)	▪ Enable/disable "*Radar Detection"* features (a special license with the country code is necessary) ▪ The DFS system performs radar detection and if a radar signal is detected, that frequency is marked as occupied and it can be used again only after a hold-down interval (the link is switched automatically to another frequency)
Max Links (Master)	▪ Maximum allowed number of connected CPEs (in the case of radio connection) . When this value is reached, other attempts to connect to the base station will be rejected
Use AUX-ODU-SYNC (Master)	▪ Enable/disable external synchronization unit, in seconds  **NOTE** Information about AUX-ODU-SYNC connection is described in the section "Connection to the synchronization unit".

Parameter	Description
Sync Hold Time (Master)	▪ Standalone downtime in case of external synchronization unit disable. Value "0" (zero) disables this parameter control, command to work always is set ▪ In case of external synchronization unit disable, the devices can synchronously work for some time using own clock signal generator. However, eventually, because of generators frequencies mismatch, the time discrepancy can reach unacceptable values and devices will begin to interfere with each other. In this case, through fixed time the device will stop the transmitter and will stop operation of TDMA until synchronization unit enable
Frame Size (Master)	▪ Set the time slot duration (in milliseconds) ○ Consists of transfer time, reception time and guard intervals ○ The range is from 2 to 10 ms in increments of 0.1 ms ○ The recommended values for links PtP at the balanced channel depending on channel width: 2-2,5 ms for 40 MHz, 2-4 ms for 20 MHz, 3-5 ms for 10 MHz, >5 ms for 5 MHz ○ The recommended values for links PtMP depending on channel width: 5 ms for 20 and 40 MHz
Auto (Master)	▪ This option works only for links "PtP" and allows to reduce the window size and a delay at absence or a small amount of traffic. Automatically selects the frame size
Turbo (Master)	▪ Increases the average throughput in an noisy environment by increasing the proportion of service information to compensate the data loss.

Parameter	Description
DL/UL ratio (%) (Master)	■ Set the DL percentage of the time slot ○ The range is from 20 to 80% in increments of 1% ○ The empty field enables the mode of flexible DL/UL ratio adjustment depending on traffic load ■ Real accepted values depend on the used bandwidth, the frame size and the used modulations. To determine the established value acceptability it is necessary to control parameters (*Tx Time Limit/Rx Time Limit*) in radio interface statistics. Any of these parameters shall not be less than zero. In the PtMP system with a large number of clients, the ratio of real throughput in this or other way does not match the established DL/UL value. Uplink performance will always be less, because of big overheads of the uplink traffic servicing. In case of a large number of clients value more than 65% practically do not lead to throughput increase in Downlink. Rated speed in Uplink and Downlink (Rx Cap/Tx Cap) is reached only in case of sector full and balanced load by all clients
Max Distance (Km) (Master)	■ Set the maximum operational distance (in kilometers) ○ Has an impact on guard intervals duration ○ The range is from 1 to 100 km in increments of 1 km ■ It allows the system to calculate signal propagation time to the furthest subscriber and value of the guard interval between transmission and receiving phases. It is recommended to set 3-5 km more than really measured distance. In case of LOS condition violation or with a large number of reflections larger value as 10-20 km can be required

Parameter	Description
STA RSSI (dBm) (Master)	■ Set the target power of received radio signal from **Slave** node at the input of **Master** node ○ The range is from -90 to -20 dBm in increments of 1 ■ It allows to reduce the radiation influence from the subscriber units to the neighbor sector due to insufficient suppression of the antenna pattern back lobe ■ To achieve maximum TDMA network performance it is important to obtain the highest possible signal level and modulation (bitrates), so transmitter power reducing is a necessary measure. If possible, it is better to try to reduce the impact of clients on neighbor sector (and vice versa), organizational measures (shielding, antennas diversity, etc.)
DFS (Master)	■ Enable/disable DFS ■ If "*DFS only*" is set, the DFS system monitors interferences but does not perform radar detection ■ If "*DFS with Radar Detection*" is set, the DFS system monitors interferences and performs radar detection ■ For the two radios base stations, the "*Instant DFS*" option is available (one of the two radios is used for DFS scanning, Radar detection and Spectrum analyzing)  **CAUTION** Please note that, in some countries, switching "DFS off" and/or failing to detect public service radar signals are against the regulations and may result in legal action.

Parameter	Description
Tx Power	▪ Set the output power of the radio interface ▪ Acts as a top limit for the output power control if the ATPC mechanism is turned on ▪ Two operating ranges of Tx power are available: ▪ “-10...10” (if chosen top limit is 10 dBm or less) ▪ “0...27” (if chosen top limit is from 10.5 dBm to 27 dBm) ▪ By default, it is turned on (it is strongly recommended to remains “on”) ▪ The offset parameter is used to adjust the thresholds
Node Name	▪ Set the name for this node in the network ▪ By default, it is the "*Unknown*" node ▪ This node name will appear on the neighbor lists
Scrambling	▪ Enable/disable the data scrambling to improve the connection stability (enabled by default)
Trap gateway	▪ Enable/disable gateway for SNMP-traps
Switch border	▪ Enable/disable the switch border mode. In this mode the unit operates as a "borderline" between the MINT domains, i.e. prevents the distribution of information about the switch groups and data transfer between these domains, while retaining all the capabilities of the MINT protocol (obtaining information about the whole MINT network, sending remote commands etc.)

Parameter	Description
Network Entry SNR (dB)	▪ "*low*" - this option sets the minimal signal level for the neighbor. Signal level is measured in dB above the noise threshold for the current bitrate. If the level gets lower than specified value the connection with a neighbor will be lost. ▪ "*high*" - this option sets the minimal SNR for a new neighbor. Signal level is measured in dB above the noise threshold for the current bitrate. If neighbor's signal level is equal or higher than a specified value the node will consider this neighbor to be a candidate
RX Attenuation	▪ The noise level measured by the radio module is calculated as the minimum received signal level (RSSI) in a certain period ▪ The "*RX Attenuation*" parameter allows manually raise noise threshold on several dB. In this case the radio module won't react to signals below the established threshold. In certain cases it gives the ability to be protected from the low signals interferences which disrupt the radio module as a result of capture effect. This effect is expressed in the fact that the radio module having captured the low signal from the foreign source, tries to strengthen it and to accept completely ignoring a strong signal from the client which has appeared later ▪ This parameter allows to protect the receiver from the powerful signal source overload

Parameter	Description
Multicast Mode (Master)	■ Traffic transmission mode: ○ "*Multicast*" - conventional mode that uses modulation one step lower than the lowest modulation among the traffic receivers when transmitting the "*multicast/broadcast*" frames. In the case of "*multicast*" streams information from "*IGMP Snooping*" module is used to obtain a list of subscribers. Consequently, the list of all connected sector clients is used for the "*broadcast* " traffic. ○ Transformation of "*Multicast*" to "*Unicast*". In case two or more clients are assigned to the same "*multicast*" stream a copy of source stream will be sent to each of them in the "*Unicast*" mode. ○ ○ "*Unicast 2", "Unicast 3", "Unicast 4", "Unicast 5"* - the number of subscribers limitation. Conventional "*Multicast* " mode will be used when the number is exceeded. ○ "*Unicast All*" - transformation is always executed. Transformation to "*Unicast*" requires memory data copying that increases CPU load. Besides, the use of "*Unicast*" streams increases the volume of transmitted traffic proportional to the number of subscribers and reduces the sector available throughput. **NOTE** "*Unicast 3*" mode is set by default. **NOTE** Transformation of "*Multicast*" to "*Unicast*" via CLI is described in the section "mint command".

Parameter	Description
Authentication Mode	▪ Set the mode: ○ *"static"* - the unit can establish connections only with units, which MAC-addresses are listed in the "Static Links" section ○ *public* - the unit can establish connections with any other units which have the same security key and the corresponding wireless connection settings ○ "*remote*" - centralized authentication mode with remote server (e.g. RADIUS or relay). In this mode any node can request the information from a remote authentication server (remote authentication server parameters are set using "*AAA*" command). This means that the node must have an access to this server (e.g. using IP)
Log Level	▪ Set the log level: ○ *off* ○ *normal* ○ *detailed*
Current Settings	
Channel Width	▪ Set the bandwidth of the radio interface in MHz ▪ It must be the same at both ends of the link
Frequency	▪ Set the radio interface frequency (in MHz) ▪ It must be the same at both ends of the link ▪ If it is set to "*Auto*", the Slave node is scanning on all frequencies for the Master nodes

Parameter	Description
Frequency Range List	▪ Set the frequencies that are allowed to be chosen by the DFS mechanism (available only when the DFS system is enabled) ▪ It is available to support the legacy products ▪ Note that this option is different from the "*Customer Frequency Grid*" tool which allows narrowing down the frequency range available in the "*Frequency*" option from the Radio profile
Tx Bitrate	▪ Set the maximum operating bitrate of the radio interface (from 13000 to 130000 Kbps) ▪ Acts as a top limit for the bitrate if the Autobitrate mechanism is turned on ▪ By default, it is turned on (it is strongly recommended to remains “on”) ▪ Adjust the Autobitrate system thresholds when the remote SNR doesn’ t have the normal level
Channel Type	▪ The channel type can be set as: ○ Dual: enables MIMO operational mode with different Tx and Rx data streams (recommended) ○ Single: allows to operate as MIMO with duplicate Tx streams, MISO or SISO depending on the Tx/Rx chain configuration (description below) ▪ InfiNet MIMO 2x2 technology effectively doubles the spectrum efficiency and allows to achieve a real throughput up to 280 Mbps in 40 MHz band

Parameter	Description
Greenfield	▪ Enable/disable the "*Greenfield*" mode ▪ When activated, the "*Greenfield*" mode increases the link performance by 10-15%, by reducing the packet overhead (optimizes the frames transmitted via the RF link) ▪ "*Greenfield*" mode must be enabled at both ends of the link (the wireless link does not establish if "*Greenfield*" mode is enabled at one end of the link and disabled at the other end of the link)
Network SID	▪ Set the network system identifier (up to 8-digit HEX figure) ▪ It must be the same at both ends of the link
Node ID	▪ Set the device identification number ▪ The parameter is optional ▪ Node ID can be configured by the administrator for a better representation of a neighbors table (nodes within a wireless network)
Security Key	▪ Set the secret key word for encoding of the protocol messages ▪ It must be up to 64 characters long, without spaces ▪ It must be the same at both ends of the link

Table - Radio settings parameters in the time division networks

On each radio profile, the following options are available (for the **Slave** unit only):

- "**Disable profile**" check box disable a radio profile
- Add a new radio profile by clicking the «**Add Profile**» button
- Copy the radio profile values to a new radio profile by clicking the «**Copy**» button
- Remove the radio profile by clicking the «**Remove**» button.

NOTE

In case of first TDMA firmware installation (instead of polling), the system automatically will starts the **Master** TDMA mode, which works in the **Master** Polling mode (*mint pollstart*) with the parameters "*win = 5, dist = 70, dlp = 50, rssi = -20*". These settings are not optimal for most networks, but allow to recover quickly network functioning at the first start. All other devices will be launched in the **Slave** TDMA mode. It gives the opportunity to transfer already operating network to TDMA. At first it is necessary to update firmware on **Slave** devices and reboot them. Then to update the firmware on the base station.

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

Frequency limitation

The licensed frequencies range per each bandwidth is displayed in the "rf5.0" subsection, in "*Default Frequency Grid*" fields. Changes to these default values can be performed in the "*Customer Frequency Grid*" fields; you can:

- Limit the licensed frequencies range per each bandwidth (see the screenshot below)
- Change the center frequency step (for example: 4915-5945/5 means that the step between the center frequencies from 4915 GHz and 5945 GHz is 5MHz).

The changes performed in "*Customer Frequency Grid*" will be available in the "*Frequency*" drop down list from the radio profiles and in DFS page in "*Frequency grid*" field.

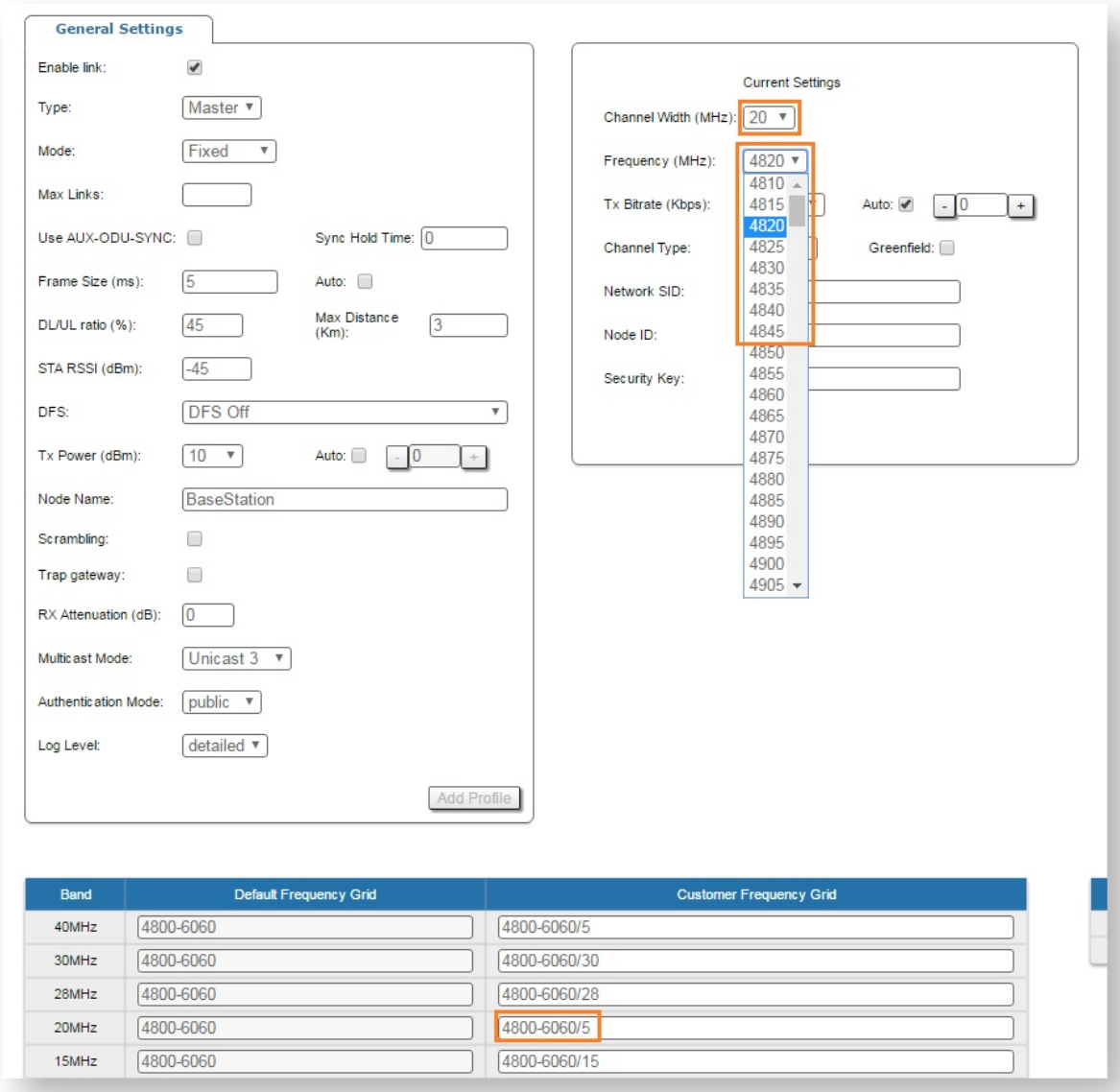


Figure - Customer frequency grid

Setting channel type mode

When Channel Type is set to “*Single*”, then *Tx* and/or *Rx of Chain #1* (for horizontal polarization antenna) can be deactivated:

Figure - Chain #

- "Chain #0" is connected to the port of the vertical polarized integrated antenna
- "Chain #1" is connected to the port of the horizontal polarized integrated antenna

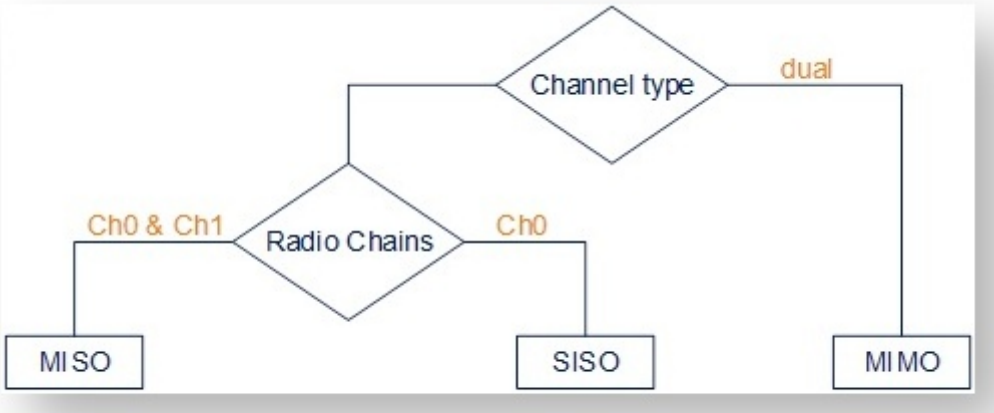


Figure - Configuration options

NOTE

MIMO, MISO and SISO are defined from the perspective of the data sent by the local unit (not considering the number of physical antennas used for tx and rx like in the classical definition). Therefore, these represent local configuration options. For example, one stream of data can be sent by one chain (1 antenna) corresponding to SISO or the same stream can be sent by both chains (2 antennas) corresponding to MISO.

Settings for "MIMO " mode

Different data streams are transmitted over "Chain #0" and "Chain #1". MIMO uses multiple antennas at both the transmitter and receiver side to improve communication performance and data is sent on both the horizontal and vertical polarizations (data is space-time coded - spatial multiplexing, to improve the reliability of data transmission):

Channel Type	Dual	
Radio Chain	#0	#1
Rx	Activated	Activated
Tx	Activated	Activated

Table - Settings for MIMO mode

Settings for "MISO" mode

The same data streams are transmitted over "Chain #0" and "Chain #1", lowering the performance of the link, but enhancing the ability to transmit data in case of interference or obstacles in transmission path (a special mode of operation of MIMO devices used in NLOS conditions or in a noisy RF environment):

Channel Type	Single	
Radio Chain	#0	#1
Rx	Activated	Activated
Tx	Activated	Activated

Table - Settings for MISO mode

Settings for "SISO " mode

The data streams are transmitted over Chain #0 (corresponding to vertical polarization) only, lowering the performance of the link, but increasing the link distance (transmitter operates with one antenna as does the receiver; there is no diversity and no additional processing for recomposing the Rx signal):

Channel Type	**Single**	
Radio Chain	**#0**	**#1**
Rx	**Activated**	**Deactivated**
Tx	**Activated**	**Deactivated**

Table - Settings for SISO mode

The picture below summarizes the link establishment between two units that are configured in different operational modes. As it can be noticed, only the combination MIMO – SISO is not functional.

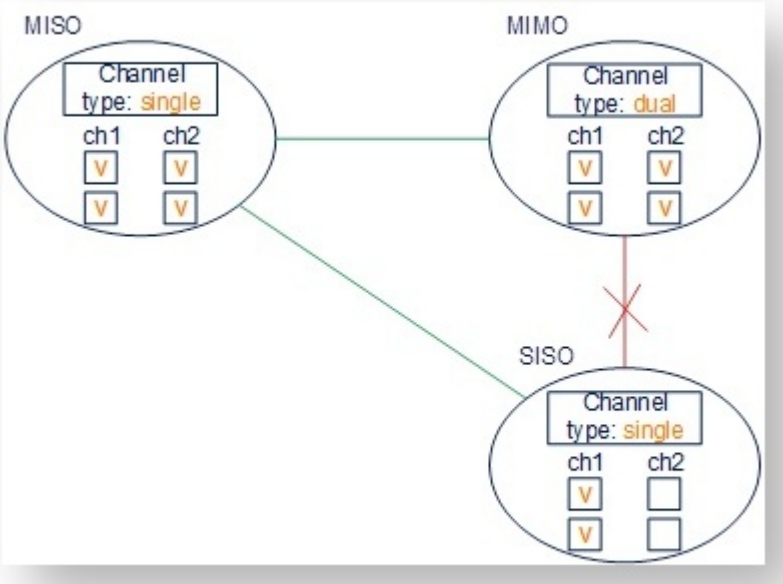


Figure - Radio link establishment

"prf" subsection

In the "prf" subsection, you can configure the pseudo-RF link as a MINT network node. The "prf" subsection is available for configurations only after at least one pseudo-RF interface has been created in "Network Settings" section. Pseudo-RF virtual interface is used to provide MINT -over-Ethernet. Every BS or CPE supports PRF interfaces. All parameters available in "prf" subsection are explained in "rf5.0" subsection above:

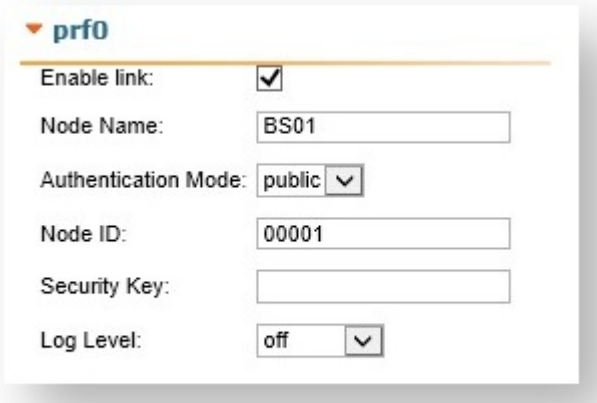


Figure - PRF settings

"Join" subsection

In the "Join" subsection, you can link two or more radio/pseudo-RF interfaces of one unit into one MINT domain. Each of these interfaces may act as an independent MINT network node. The "Join" subsection is available for configurations only after at least one pseudo-RF interface has been created in "Network Settings" section.

In order to join the interfaces, simply enable the check boxes of the corresponding interfaces, as shown in the screenshot below:

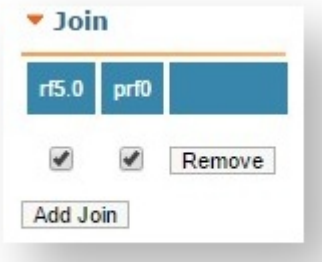


Figure - «Remove» and «Add Join» buttons

4.3.4 Static Links

In the "Static Links" section, you can set up fixed links to the unit. Although the radio parameters and security key match with other nodes, the node that has Static Links set up is only linked with the nodes which are configured in this section. The parameters are:

- "*MAC*" - MAC address of the neighbor unit
- "*Key*" - link security key (up to 64 characters long, without spaces).

Another two options are available:

- Disable the link by marking the option “*Disabled*" in the corresponding checkbox
- Add a link description in the “*Note*" field

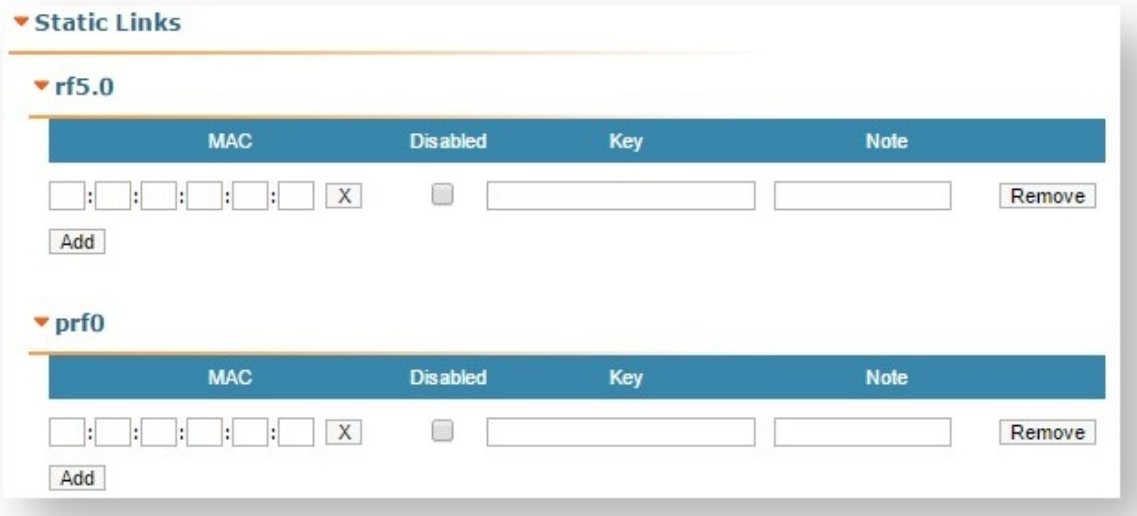


Figure - Static Links settings

By clicking the «**Add**» button, you create a new fixed link to the unit.

By clicking the «**Remove**» button, you can delete an already created fixed link.

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

4.3.5 MAC Switch

//<![CDATA[AJS.toInit(function(){ /* For anonymous users */ if (AJS.params.remoteUser == "){ /* Remove action menu on selected text */ AJS.$('#action-menu-link').hide(); /* Remove comments section */ AJS.$('#comments-section').hide(); /* Find elements with inline comments */ var commentedElements = Array.from(document. getElementsByClassName("inline-comment-marker")); /* If any found */ if (commentedElements.length > 0) { /* For each inline-commented element clear data-ref and class */ for (var i=0; i < commentedElements.length; i++) { commentedElements[i].dataset.ref= ""; commentedElements[i].className = ""; } } /* Else do nothing */ } }); //]]> Switch configuration

The Switch configuration is based on a set of rules for the switching groups:

- An unique numeric identifier (1-4095) for each group
- Two or more local network interfaces (*ethX, rfX, tunX, etc*) and a set of rules (filters) which allow placing different types of traffic into different switching groups
- Each node can have several switching groups. The same interfaces or group of interfaces can be used in several groups simultaneously
- Switching groups are activated on different nodes of the MINT network. The nodes that have the same switching group identifier in their configurations represent a "switching zone"
- "Switching zone" exists only within the MINT network segment.

Switching groups

The MINT network can be viewed as one virtual distributed layer-3 switch, where border nodes act as external ports of the virtual switch. The virtual switch task is to transport frames from one external port to another. It is important to understand that switching groups should be created only on the nodes where frames enter from or leave to the "outside" network ("outside" relative to MINT). On the repeater nodes (in mesh topology) there is no need to create switching groups.

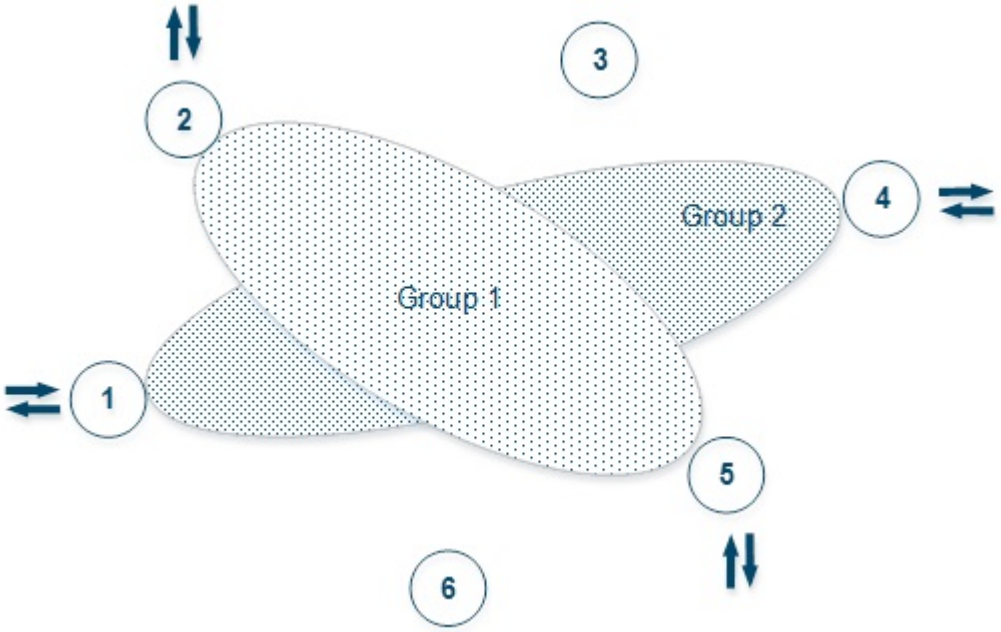


Figure - Switching Groups

In order to put an incoming frame into one of the switching groups, a set of flexible rules is used, which allow sorting frames according to various criteria, like:

- VLAN tag
- Protocol type
- Addresses (MAC/IP)
- Ports
- Any PCAP expressions.

Trunk groups

Trunk group is a switching group in the "*Trunk*" mode.

Input flow from wired segment for Trunk group is divided into separate sub-groups (switching groups within Trunk group) depending on VLAN-tag of the packet. The group number of the switching group within Trunk group will be equal to the VLAN-number of packets which are switched to it.

The trunk groups are used for the ease of configuration, when VLAN flows are transmitted to several subscribers.

If you enable the trunk group at the BS side to transmit several VLAN-flows to several directions, then at the CPE side, you should use the "*In-Trunk*" option to specify the group number of the trunk group that includes the required switching group.

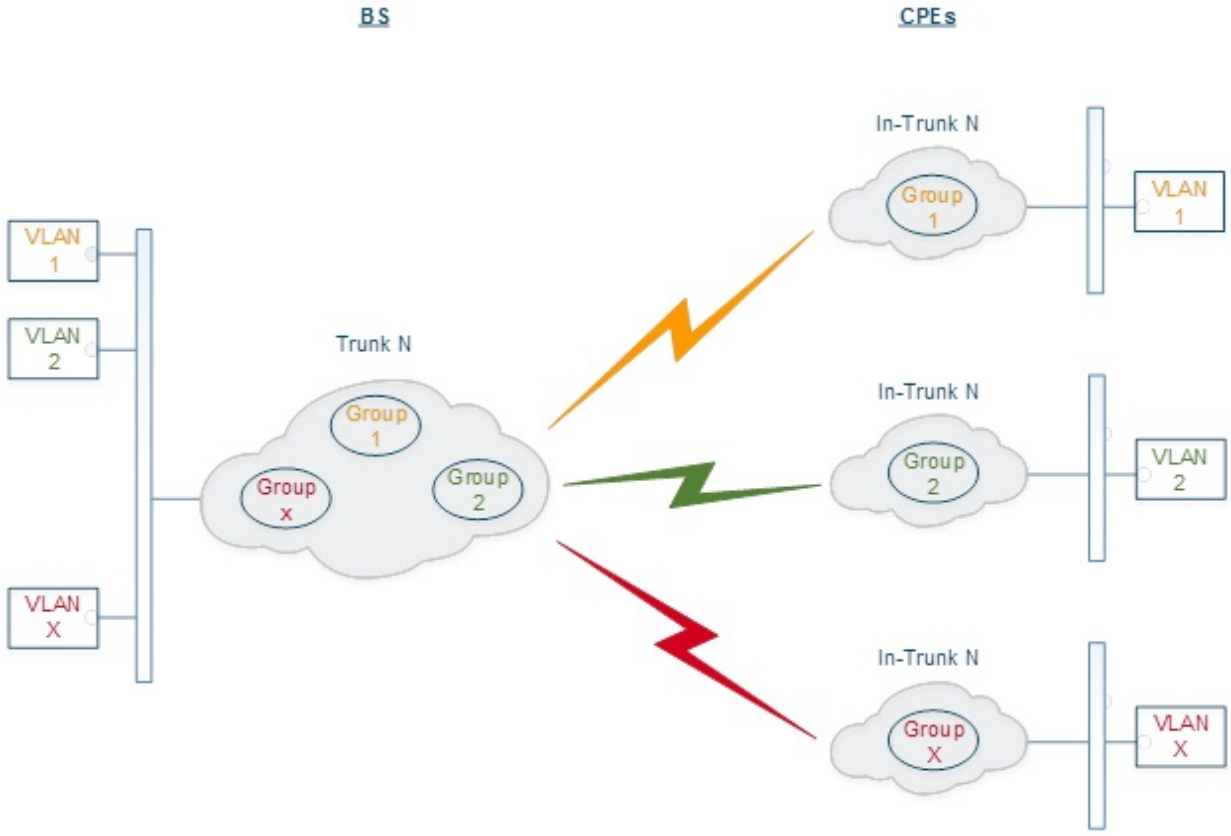


Figure - Trunk Groups

Trunk groups may also be used to solve the task of connecting several VLAN segments.

Special rules on interfaces allow flexible manipulations with VLAN ID tags: deleting, assigning and re-assigning (please consult the information provided in WANFleX OS User Manual).

Management connection to the unit

For the management purposes, you can create a dedicated Switch Group for all units in the MINT network, attached to the Switch Virtual Interface (SVI). Assign the IP addresses directly on the SVI interface for native management or create an additional VLAN interface attached to that SVI for Management VLAN. All packets sent via SVI interface will be distributed only within the assigned switch group.

The universal way to configure Management VLAN via common switch group is presented in the figure below (which illustrates the step by step sequence and not the way of packet passing).

You have to assign the IP addresses to "*vlanX*" and "*vlanY*" which have the parent interface svi1 (the management interface of Group 1), which includes "*eth0*" and "*rf5.0*" interfaces (see section "Remote management of the R5000 units"):

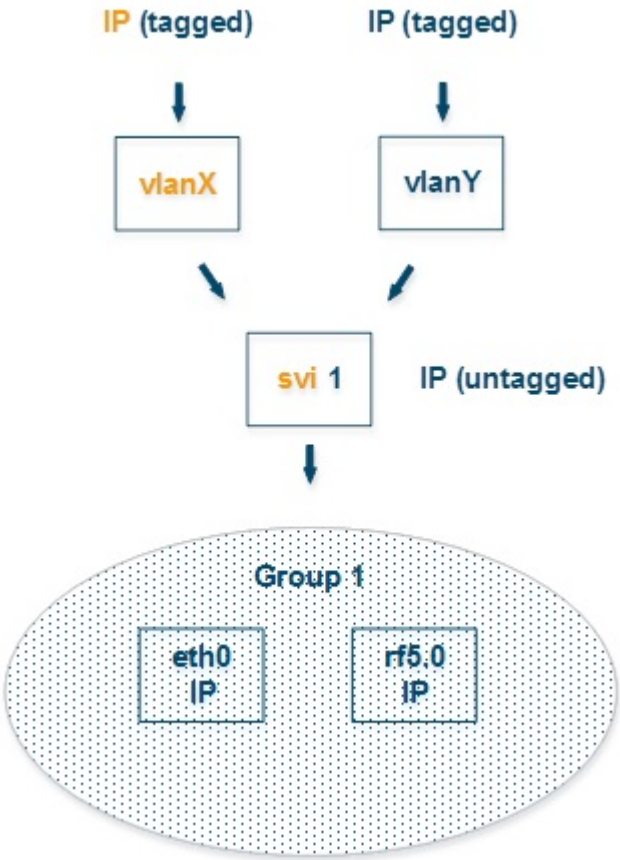


Figure - Management configuration 1

NOTE

Make sure that the group can and will accept traffic in "*vlanX*" and "*vlanY*".

An alternative way to configure Management VLAN via dedicated switch group is presented in the figure below (which illustrates the step by step sequence and not the way of packet passing).

You have to assign the Management IP addresses to "*sviM*" interface which is the management interface of Group M and includes "*vlanX*" (with parent interface "*eth0*") and "*rf5.0*" interface:

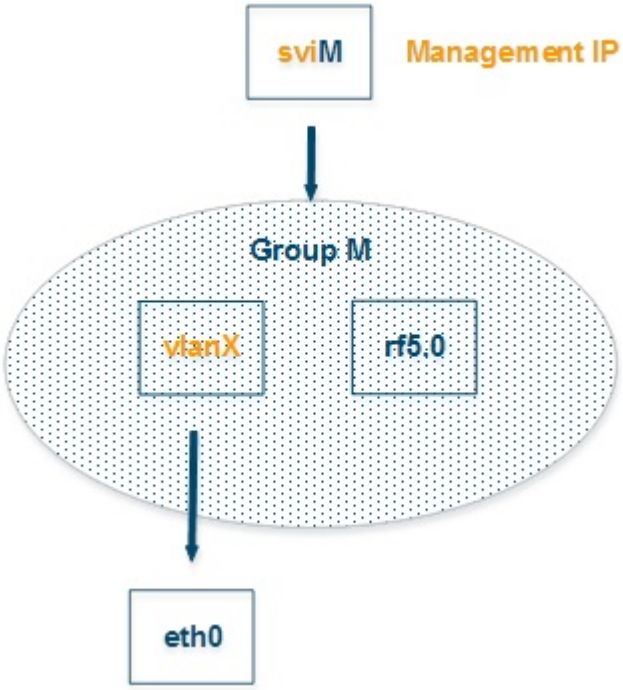


Figure - Management configuration 2

NOTE

Using a dedicated management group is the preferred configuration method as the VLAN interface is created only on one network device and the group does not require any additional rules.

Switch Group rules

Once assigned to one of the switching groups, a frame will never leave it until it reaches one of the external ports. Switching group rules are applied only when the frame enters to MINT network through one of its external ports. When leaving the network, no rules are required as the frame already belongs to one of the switching groups and it is automatically forwarded to an external port(s) that belongs to the corresponding switching group.

NOTE

Frames originated by MINT network nodes (for example: containing RIP/OSPF, ping packets, etc) do not belong to any of the switching groups. Therefore, they cannot leave MINT network via switching through any of the external ports.

Rules are used for the following purposes:

- Selecting an appropriate switching group when a packet is received through "*ethX*" interface. The packet is switched by the group the rules of which it fully satisfies.

CAUTION

A packet that cannot be associated with any switching group will not switched by the device. If there is no group with appropriate rules for the packet, it is discarded.

- When the packet is assigned to a switching group, the group decides whether the packet to be sent through one of the interfaces, or to discard it. The packet will only be sent if it satisfies the rules of this interface.

The rules consist of a "rules list" and a decision (deny/permit). While parsing the list, the switch checks whether a packet matches the rule. If it matches the rule, the decision set for this rule is applied to the packet. Otherwise, the list of rules is viewed further. Rules are taken one at a time. If a packet does not match to any rule, the default decision for this group or interface is taken.

The expression selects which packets will fit into the group. Only the packets for which the expression is “true” will be matched to the group. The expression consists of one or more primitives. Primitives usually consist of an id (name or number) preceded by one or more qualifiers.

Examples packet filter rules:

Single IP subnet:

```
net 192.168.1.0/24
```

Several IP subnets:

```
 net 192.168.1.0/24 or net 192.168.100.0/24
```

Several IP subnets with exceptions:

```
net 192.168.1.0/16 and not net (192.168.100.0/24 or 192.168.200.0/
24)
```

Several IP subnets inside VLAN:

```
vlan 50 and (net 192.168.1.0/24 or net 192.168.100.0/24)
```

PPPoE traffic:

```
pppoed or pppoes
```

which is synonym to:

```
ether proto 0x8863 or ether proto 0x8864
```

Disable IP multicast and broadcast:

```
not ip multicast
```

Detailed filter expression syntax description

The filter expression determines which packets are selected by the filter for further processing. If no expression is given, all the packets on the net are selected. Otherwise, only the packets for which expression is “true” are selected.

There are three different kinds of qualifier:

Qualifier	Description
type	▪ Qualifiers say to what the id name or number refers to ▪ Possible types are: host, net, port, portrange ▪ For example: “host foo”, “net 128.3”, “port 20”, “portrange 6000-6008” ▪ If there is no type qualifier, host is assumed
dir	▪ Qualifiers specify a particular transfer direction to and/or from id ▪ Possible directions are: src, dst, src or dst and src and dst ▪ For example, “src 1.1.1.1”, “dst net 128.3”, “src or dst port 21”. If there is no dir qualifier, src or dst is assumed
proto	▪ Qualifiers restrict the match to a particular protocol ▪ Possible protos are: ether, ip, ip6, arp, rarp, tcp and udp ▪ For example: “ether src 00:12:13:14:15:16”, “arp net 128.3”, “tcp port 21”, “udp portrange 7000-7009” ▪ If there is no proto qualifier, all protocols consistent with the type are assumed ▪ For example, “src 1.1.1.1” means “(ip or arp or rarp) src foo” (except the latter is not legal syntax), “net 1.2.3.0/24” means “(ip or arp or rarp) net 1.2.3.0/24” and “port 53” means “(tcp or udp) port 53”

Table - Qualifiers

More complex filter expressions are built up by using the words “and”, “or” and “not” to combine primitives. For example: “*host foo and not port ftp and not port ftp-data*”. To save typing time, identical qualifier lists can be omitted. For example: “*tcp dst port ftp or ftp-data or domain*” is exactly the same as “*tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain*”.

Allowable primitives are:

Primitives	Description

Primitives	Description
dst host *host*	▪ True if the IPv4 destination field of the packet is "*host*", which may be either an address or a name
src host *host*	▪ True if the IPv4 source field of the packet is "*host*"
host *host*	▪ True if either the IPv4 source or destination of the packet is host ▪ Any of the above host expressions can be prefixed with the keywords, *ip, ip6, arp, rarp* as in: "*ip host host*" ▪ This is equivalent to: "ether proto \ip and host host"
ether dst *ehost*	▪ True if the Ethernet destination address is "*ehost*" ▪ Ehost must have a numeric format: XX:XX:XX:XX:XX:XX
ether src *ehost*	▪ True if the Ethernet source address is "*ehost*"
ether host *ehost*	▪ True if either the Ethernet source or destination address is "*ehost*"
dst net *net*	▪ True if the IPv4 destination address of the packet has a network number of "*net*"
src net *net*	▪ True if the IPv4 source address of the packet has a network number of "*net*"
net *net*	▪ True if either the IPv4 source or destination address of the packet has a network number of "*net*"

Primitives	Description
net *net* **mask** *netmask*	▪ True if the IPv4 address matches net with the specific *netmask*. May be qualified with "*src*" or "*dst*"
net *net/len*	▪ True if the IPv4 address matches net with a netmask "*len*" bits wide ▪ May be qualified with "*src*" or "*dst*"
dst port *port*	▪ True if the packet is ip/tcp, ip/udp and has a destination port value of "*port*"
src port *port*	▪ True if the packet has a source port value of "*port*"
port *port*	▪ True if either the source or destination port of the packet is "*port*"
dst portrange *port1-port2*	▪ True if the packet is ip/tcp, ip/udp and has a destination port value between "*port1*" and "*port2*" ▪ "*port1*" and "*port2*" are interpreted in the same fashion as the port parameter for "*port*"
src portrange *port1-port2*	▪ True if the packet has a source port value between "*port1*" and "*port2*"
portrange *port1-port2*	▪ True if either the source or destination port of the packet is between "*port1*" and "*port2*" ▪ Any of the above port or port range expressions can be prefixed with the keywords, *tcp or udp*, as in: "*tcp src port port*" ▪ This matches only tcp packets whose source port is "*port*"

Primitives	Description
less *length*	▪ True if the packet has a length less than or equal to "*length"* ▪ This is equivalent to: “*len <= length*”
greater *length*	▪ True if the packet has a length greater than or equal to "*length"* ▪ This is equivalent to: “*len >= length*”
ip proto *protocol*	▪ True if the packet is an IPv4 packet of protocol type "*protocol"* ▪ *Protocol* can be a number or one of the names *icmp, icmp6, igmp, igrp, pim, ah, esp, vrrp, udp, or tcp* ▪ The identifiers tcp, udp, and icmp are also keywords and must be escaped via backslash (\), which is \\ in the C-shell ▪ This primitive does not chase the protocol header chain
ip protochain *protocol*	▪ True if the packet is IPv4 packet, and contains protocol header with type *protocol* in its protocol header chain ▪ For example, “ip protochain 6” matches any IPv4 packet with TCP protocol header in the protocol header chain ▪ The packet may contain, for example, authentication header, routing header, or hop-by-hop option header, between IPv4 header and TCP header ▪ The code emitted by this primitive is complex and cannot be optimized, so this can be somewhat slow
ether broadcast	▪ True if the packet is an Ethernet broadcast packet ▪ The *ether* keyword is optional

Primitives	Description
ether multicast	▪ True if the packet is an Ethernet multicast (or broadcast) packet ▪ The "*ether*" keyword is optional ▪ This is shorthand for "*ether[0] & 1 != 0*"
ip multicast	▪ True if the packet is an IPv4 multicast (or broadcast) packet
ether proto *protocol*	▪ True if the packet is of ether type *protocol* ▪ Protocol can be a number or one of the names ip, ip6 ,arp, rarp, atalk, aarp, sca, lat, mopdl, moprc, iso, stp, ipx, or netbeui ▪ These identifiers are also keywords and must be escaped via backslash (\) ▪ In the case of Ethernet, WANFleX checks the Ethernet type field for most of those protocols ▪ The exceptions are: ○ *iso, stp, and netbeui* **WANFleX** checks for an 802.3 frame and then checks the LLC header as it does for FDDI, Token Ring, and 802.11 ○ *atalk* **WANFleX** checks both for the AppleTalk etype in an Ethernet frame and for a SNAP-format packet as it does for FDDI, Token Ring, and 802.11 ○ *aarp* **WANFleX** checks for the AppleTalk ARP etype in either an Ethernet frame or an 802.2 SNAP frame with an OUI of 0x000000 ○ *ipx* **WANFleX** checks for the IPX etype in an Ethernet frame, the IPX DSAP in the LLC header, the 802.3-with-no-LLC-header encapsulation of IPX, and the IPX etype in a SNAP frame

Primitives	Description
ip, **arp**, **rarp**, **atalk**, **aarp**, **iso**, **stp**, **ipx**, *netbeui*	▪ Abbreviations for “ether proto p”, where “*p*” is one of the above protocols
svlan *[vlan_id]*	▪ True if the packet is an IEEE 802.1Q Service VLAN packet (ether proto 0x88a8)
vlan *[vlan_id]*	▪ True if the packet is an IEEE 802.1Q VLAN packet (ether proto 0x8100) ▪ If *[vlan_id]* is specified, only true if the packet has the specified vlan_id ▪ The first "*vlan"* or "*svlan"* keyword encountered in *expression* changes the decoding offsets for the remainder of *expression* on the assumption that the packet is a VLAN packet ▪ The "*vlan" "[vlan_id]"* expression may be used more than once, to filter on VLAN hierarchies ▪ Each use of that expression increments the filter offsets by 4 ▪ For example, “svlan 100 && vlan 200” filters on VLAN 200 encapsulated within Service VLAN 100, and “vlan 300 && ip” filters IPv4 protocols encapsulated in VLAN 300, and “svlan 100” filters all packets encapsulated within Service VLAN 100

Primitives	Description
mpls *[label_num]*	▪ True if the packet is an MPLS packet ▪ If *[label_num]* is specified, only true is the packet that has the specified *label_num* ▪ The first "*mpls"* keyword encountered in expression changes the decoding offsets for the remainder of *expression* on the assumption that the packet is a MPLS-encapsulated IP packet ▪ The "*mpls" "[label_num]expression* may be used more than once, to filter on MPLS hierarchies ▪ Each use of that expression increments the filter offsets by 4 ▪ For example, “mpls 100000 && mpls 1024 “ filters packets with an outer label of 100000 and an inner label of 1024, and “mpls && mpls 1024 && host 192.9.200.1” filters packets to or from 192.9.200.1 with an inner label of 1024 and any outer label
pppoed	▪ True if the packet is a PPP-over-Ethernet Discovery packet (Ethernet type 0x8863)
pppoes	▪ True if the packet is a PPP-over-Ethernet Session packet (Ethernet type 0x8864) ▪ The first "*pppoes"* keyword encountered in *expression* changes the decoding offsets for the remainder of *expression* on the assumption that the packet is a PPPoE session packet ▪ For example, “pppoes && ppp proto 0x21” filters IPv4 protocols encapsulated in PPPoE
tcp, **udp**, **icmp**	▪ Abbreviations for: “ip proto p”, where “*p*” is one of the above protocols
iso proto *protocol*	▪ True if the packet is an OSI packet of *protocol* type protocol ▪ *Protocol* can be a number or one of the names *clnp, esis, or isis*

Primitives	Description
clnp, **esis**, **isis**	▪ Abbreviations for: “iso proto p”, where “*p*” is one of the above protocols
expr relop expr	▪ True if the relation holds, where relop is one of >, <, >=, <=, =, !=, and *expr* is an arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [+, -, *, /, &, |, <<, >>], a length operator, and special packet data accessors ▪ Note that all comparisons are unsigned, so that, for example, 0x80000000 and 0xffffffff are > 0 ▪ To access data inside the packet, use the following syntax: “proto [expr : size]” ▪ *Proto* is one of *ether, fddi, tr, wlan, ppp, slip, link, ip, arp, rarp, tcp, udp, icmp*, and indicates the protocol layer for the index operation (*ether, fddi, wlan, tr, ppp, slip and link* all refer to the link layer) ▪ *tcp*, *udp* and other upper-layer protocol types only apply to IPv4 ▪ The byte offset, relative to the indicated protocol layer, is given by *expr* ▪ *Size* is optional and indicates the number of bytes in the field of interest; it can be one, two, or four, and defaults to one ▪ The length operator, indicated by the keyword len, gives the length of the packet ▪ For example, “ether[0] & 1 != 0” catches all multicast traffic ▪ The expression “ip[0] & 0xf != 5” catches all IPv4 packets with options ▪ The expression “ip[6:2] & 0x1fff = 0” catches only unfragmented IPv4 datagrams and frag zero of fragmented IPv4 datagrams ▪ This check is implicitly applied to the "*tcp*" and "*udp*" index operations ▪ For instance, "*tcp[0]*" always means the first byte of the TCP *header*, and never means the first byte of an intervening fragment ▪ Some offsets and field values may be expressed as names rather than as numeric values ▪ The following protocol header field offsets are available: icmptype (ICMP type field), icmpcode (ICMP code field), and tcpflags (TCP flags field)

Primitives	Description
	▪ The following ICMP type field values are available: icmp-echoreply, icmp-unreach, icmp-sourcequench, icmp-redirect, icmp-echo, icmp-routeradvert, icmp-routersolicit, icmp-timxceed, icmp-paramprob, icmp-tstamp, icmp-tstampreply, icmp-ireq, icmp-ireqreply, icmp-maskreq, icmp-maskreply ▪ The following TCP flags field values are available: tcp-fin, tcp-syn, tcp-rst, tcp-push, tcp-ack, tcp-urg

Table - Primitives

Primitives may be combined using:

- A parenthesized group of primitives and operators (parentheses are special to the Shell and must be escaped)
- Negation (`!' or `not')
- Concatenation (`&&' or `and')
- Alternation (`||' or `or').

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right. Note that explicit and tokens, not juxtaposition, are now required for concatenation. If an identifier is given without a keyword, the most recent keyword is assumed. For example, “*not host 1.1.1.1 and 2.2.2.2*” is short for “*not host 1.1.1.1 and host 2.2.2.2*” and should not be confused with “*not (host 1.1.1.1 or 2.2.2.2)*”.

MAC Switch Group parameters

In the "MAC Switch Group parameters" section, you can view the Switch Groups and Rules that are already created, including the management switch group; you can change the parameters for these Switch Groups, delete them by clicking the «**Remove Group**» button or create new ones by clicking the «**Create Switch Group**» button. The same operations are available for the switching rules: add a new rule within a switch group by clicking the «**Add Rule**» button (located within sub-menu "Rules" of this group) or delete an existing rule by clicking the «**Remove Rule**» button.

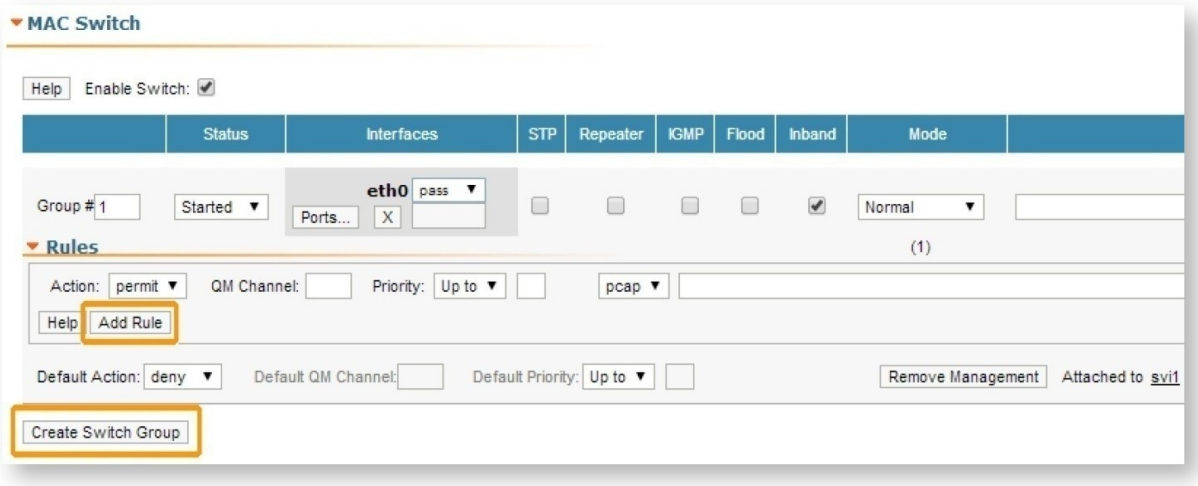


Figure - MAC Switch default configuration

General options in this section:

- «*Enable Switch*» - this checkbox enables/disables global switch operation

CAUTION

Disabling the switch in the absence of routing settings can lead to termination of packet transmitting through the device.

- «*Remove Management*» - by clicking this button you can delete the "*sviX*" interface, which is available in the default configuration, for the unit management
- «*Create Management*» - by clicking this button you can add a "*vlanX*" and an "*sviX*" interface for the unit management via Web interface (please consult the configuration examples presented in chapter "Configuration scenarios").

«Switch Group configuration» section:

Switch parameter	Description
Group #	- Displays the Switch Group number - Assign the switch group identifier (must be unique within the MINT network segment)

Switch parameter	Description
Status	▪ Select the Switch Group status: started, stopped or discard
Interfaces	▪ Add Ethernet or/and Radio as Switch Group interface(s) via the «**Ports**» button ▪ "*Select*": pass (selected by default), strip or tag for VLAN tag modification for each added interface ▪ The Interfaces section provides the means to control the VLAN tag processing mode, as each local interface supports three different scenarios: ▪ "*Pass*" - transparent mode, traffic remains unchanged. ▪ "*Strip*" - all tags are stripped. ▪ "*Tag*" - all packets are tagged with the specified VLAN tag ▪ Another option in this field is to remove one or both added interfaces
STP	▪ Add an STP VLAN number in case that spanning tree support is enabled
Repeater	▪ Enable/disable repeater support ▪ The unit acts as a simple switch, relaying packets to all ports, except the source port
IGMP	▪ Enable/disable IGMP snooping support ▪ Please refer to the information provided in the next section for details
Flood	▪ Allow/deny unlimited unicast flood without protection filter

Switch parameter	Description
Inband	▪ Allow/deny access to the device through in-band broadcast/multicast management traffic ▪ It is enabled by default
Mode	▪ Set the working mode of the switching group: normal, trunk, in-trunk (give it the trunk group number created on the BS), upstream, downstream ▪ Normal (standard mode) - the switch group operation is based on the configured Rules, packets are processed without modification (this is the default option) ▪ Trunk - the inbound traffic is untagged and placed into switch groups in accordance with its VLAN tag ▪ In-Trunk - allows filtering out the traffic that belongs to a certain switch group that is a member of a trunk Switch Group ▪ Upstream - used mainly in video surveillance systems for upstream multicast flows ▪ Downstream - used in video surveillance systems for downstream traffic
Description	▪ Type a description sentence for the current switch group
Default Action	▪ Set the default action: permit/deny ▪ In the absence of any Switching rule, or if a packet does not match to any Switching rule, the default action for this group or interface is taken

Switch parameter	Description
Default QM Channel	▪ Allocate a default logical channel ▪ The default logical channel must be prior created in the "Traffic Shaping" section ▪ In the absence of any Switching rule, or if a packet does not match to any Switching rule, the default logical channel is allocated ▪ For the indications on how to create a logical channel, please refer to the " Traffic Shaping" section below
Default Priority	▪ Allocate the default priority for all the packets going through the Switch group: ○ "*Up to*" - used to increase the packet priority to the specified value only if the processed packet has a lower priority ○ "*Set*" - used to assign a new priority regardless of the value already assigned to the packet ▪ In the absence of any Switching rule, or if a packet does not match to any Switching rule, the default priority is allocated

Table - MAC Switch

You can change the list order of the switch group using the "**up/down**" arrows.

A set of rules are applied to all packets within a switch group. You can create several switch rules within a switch group. The following parameters are available for switch rules:

Switch Rules parameter	Description
Action	▪ Set the action for the packets that match this rule: permit/deny
QM Channel	▪ Allocate a logical channel if there are logical channels prior created in the "Traffic Shaping" section ▪ If you allocate a number for a logical channel that was not prior created in the "Traffic Shaping" section, it has no effect in the rule configuration ▪ For the indications how to create a logical channel, please refer to the " Traffic Shaping" section below
Priority	▪ Allocate the priority for all the packets going through the new rule of the filter: ○ "*Up to*" is used to increase the packet priority to the specified value only if the processed packet has a lower priority ○ "*Set*" is used to assign a new priority regardless of the value already assigned to the packet
Packet capture filter	▪ Set the packet capture filter for Switching ▪ The syntax is called "PCAP expression" ▪ Please refer to filter expression syntax description above ▪ Validate rule by clicking the «**Validate**» button
VLAN **list**	▪ Set the VLAN ID ▪ It is available for the legacy configuration ▪ It can be set also in "PCAP expression" option (for example: VLAN 100 when "PCAP expression" is chosen) ▪ Validate rule by clicking the «**Validate**» button

Table - Switch Groups Rules

NOTE

In all three types of filters: Switching, IP Firewall and Traffic Shaping, there is the same syntax called “PCAP expression” for setting a rule. It is a universal tool for creating filters.

IGMP Snooping

In this section you can set the IGMP-parameters for the groups for which support of IGMP snooping is enabled (the IGMP check box is marked for these groups in the "MAC Switch" section).

IGMP Snooping is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups. By listening to and analyzing IGMP messages, the device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

In order for IGMP snooping to function, a multicast router must exist on the network and generate IGMP queries. The tables created for snooping (holding the member ports for each a multicast group) are associated with the multicast router. Without a multicast router, the tables are not created and snooping will not work. Furthermore, IGMP general queries must be unconditionally forwarded by all switches involved in IGMP snooping.

IGMP Snooping parameters can be set within "MAC Switch" section:

IGMP **Snooping parameter**	**Description**
Router Port Forwarding	▪ Enable/disable forwarding to router ports
Flood IGMP **Reports**	▪ Enable/disable flood IGMP reports to all bridging ports, not only to router ports
Permit Zero IP **Querier**	▪ Allow/deny query requests with source address 0.0.0.0
Replace Source IP	▪ Replace source IP in all IGMP reports/query packets

IGMP **Snooping parameter**	**Description**
Last Member Query Timeout (LMQT)	▪ Set the timeout (in seconds)
Group Membership Interval (GMI)	▪ Set the interval (in seconds)
Multicast Group Limit	▪ Set the limit number for the multicast group
Enable Querier	▪ Start/stop the IGMP querier
VLAN	▪ Set the IGMP querier VLAN ID in case of a VLAN broadcast domain
Disable Election	▪ Enable/disable the IGMP querier election process
Source IP	▪ Set the IP address of the IGMP querier ▪ By default, this is 0.0.0.0
Interval	▪ Set the IGMP querier send interval (in seconds)

Table - IGMP Snooping

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

4.3.6 IP Firewall menu

IP Firewall is a mechanism of filtering packets crossing an IP network node, according to different criteria. System administrator may define a set of incoming filters and a set of outgoing filters. The incoming filters determine which packets may be accepted by the node. The outgoing filters determine which packets may be forwarded by the node as a result of routing. Each filter describes a class of packets and defines how these packets should be processed (reject and log, accept, accept and log).

Packets can be filtered based on the following criteria:

- Protocol (IP, TCP, UDP, ICMP, ARP)
- Source address and/or destination address (and port numbers for TCP and UDP)
- The inbound network interface
- Whether the packet is a TCP/IP connection request (a packet attempting to initiate a TCP /IP session) or not
- Whether the packet is a head, tail or intermediate IP fragment
- Whether the packet has certain IP options defined or not
- The MAC address of the destination station or of the source station.

The figure below illustrates how packets are processed by the filtering mechanism of the router:

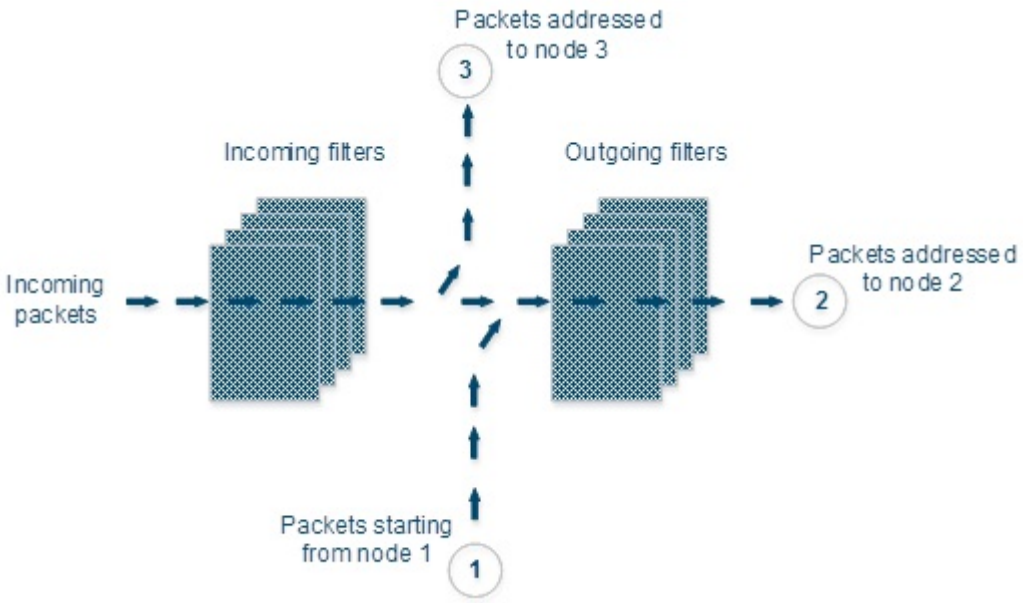


Figure - IP Firewall

There are two classes (sets) of filters - prohibiting (reject) and permitting (accept).

Furthermore, a filter may be applied to all inbound packets or only to packets arriving via a specific interface. Each received packet is checked against all filters in the order they are put in the set.

The first filter that matches the received packet determines how the packet are treated. If the filter is an accept filter, the packet is accepted, otherwise it is rejected. If the packet matches no filter in the set, or if the set is empty, the packet is accepted.

NOTE

The rejected packet are discarded without notification to the sender.

Packet filtering rules

Every packet entering a router passes through a set of input filters (blocking filters). The packets accepted by the input filter set are further processed by the IP layer of the router kernel. If the IP layer determines that the packet should go further and not landing here, it hands the packet to the set of outgoing filters (forwarding filters).

Information on packets rejected by any filter is displayed on the operator's terminal and the packets themselves are discarded without any notice to their sender.

A packet, "advancing through" a set of filters, is checked by every filter in the set, from the first one till the end of the set, or until the first matching filter. The algorithm is the following:

1. If the filter set is empty, the packet is accepted
2. Otherwise, the first matching filter decides what to do with the packet. If it is an accept filter, the packet is accepted. If it's a reject filter, the packet is rejected (discarded)
3. If no filter has been found that matches the packet, it is accepted.

IP Firewall parameters

In the "IP Firewall parameters" section, you can view the IP Firewall rules that are already created; you can create a new rule for the current switch group by clicking the «**Add Rule**» button, or you can permanently remove the rule from the configuration by clicking the «**Remove Rule**» button.

IP **firewall rule parameter**	**Description**

IP firewall rule parameter	Description
Action	■ Set the action for the rule: permit/deny/pass: ○ "*Permit*" - the packet is processed by the system (ignoring other firewall rules) ○ "*Deny*" - the packet is dropped ○ "*Pass*" - the packet is passed to the next rule in the list and logged in the system log (only if the log check box is marked)
Channel	■ Allocate a logical channel if there are logical channels prior created in " Traffic Shaping" section (it is active only if the action "permit" is selected) ■ If you allocate a number for a logical channel that was not prior created in "Traffic Shaping" section, it has no effect in the rule configuration ■ For the indications how to create a logical channel, please refer to " Traffic Shaping" section below
Priority	■ Set the priority for the packets going through the new rule of the filter: ○ "*Up to*" - used to increase the packet priority to the specified value only if the processed packet has a lower priority ○ "*Set*" - used to assign a new priority regardless of the value already assigned to the packet
Log	■ Enable/disable filter actions logging in the system log
Direction	■ Set the input/output direction for applying the new rule: ○ "*Input*" - the rule is used to process inbound traffic ○ "*Output*" - the rule is used to process outbound traffic and for post-routing packet filtering

IP **firewall rule parameter**	**Description**
Interface	■ Set the interface for applying the new rule ■ All the available interfaces are displayed in the dropdown list (physical and logical) ■ If “*any*” option is used, the rule is applied to all available interfaces
Group	■ Set the Switch Group number for the applying of the new rule ■ The Switch Group must be prior created
Rule	■ Set the packet capture filter for IP firewall ■ It is the same syntax called “PCAP expression”, as in the "Switching" section ■ Refer to the filter expression syntax description above ■ By clicking the «**Validate**» button, you can check the syntax in the expression in the “Rule” field

Table - IP Firewall

The «**Up/Down**» arrows allow you to organize rules list. The rules are processed one by one in a top-down order.

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

4.3.7 SNMP menu

The SNMP protocol support is an important feature of all communication devices because it allows the system administrator to manage the operation of a network as a whole, as well as of each component.

SNMP section contains a set of parameters to exchange data about network activity of the device.

The SNMP Protocol has two sides, the agent and the management stations:

- The agent sends data to the management station
- The management station collects data from all the agents on the network. You can set several destinations of traps with individual set of traps as well as several users with individual access rights.
- The agent sends alerts called traps (see Traps zone) and answers requests that were sent by the management station
- The management station captures and decodes the traps. The management station also requests specific information from the agent.
- The information is passed through requests and replies with the use of the MIB
- The management station is responsible for decoding the SNMP packets and providing an interface to the administrator. The interface can be a GUI or a command line.

Access

In the "Access" section, you can view and edit the current SNMP access settings; you can delete the current SNMP v.3 users by clicking the «**Remove User**» button or create new ones by clicking the «**Add SNMP v.3 User**» button:

SNMP access parameter	Description
Start SNMP	▪ Enable/disable SNMP daemon in the device
Version 1 enable	▪ Enable/disable SNMP v.1 and v.2c support ▪ The first version of the SNMP protocol lacks security in the operation of the protocol itself, which hinders its use for network management, so SNMP v.1 and v.2c works only in read-only mode ▪ By default, it is enabled

SNMP access parameter	Description
Community	▪ Set the community name for read-only mode (SNMP v.1 and v.2c only) ▪ The default SNMP v.1 and v.2c community name is "public" ▪ It is a security method for SNMP v.1 and v.2c, as Agents can be set to reply only to queries received by accepted community names ▪ In SNMP v.1 and v.2c the community name passes along with the data packet in clear text
Contact	▪ Set the contact information ▪ Used as a reference information about the device owner
Location	▪ Set the geographical location where the unit is installed ▪ Used as a reference information about physical device’s location
User Name	▪ Set the authorization user name of SNMP v.3
Password	▪ Set the authorization password of SNMP v.3
Security	▪ Set the security level: ○ the lowest level means no authentication or privacy (No Authorization No Privacy), you have to set the User Name only ○ the medium level means authorization and no privacy (Authorization No Privacy), you have to set User Name and Password ○ the highest level means authorization and privacy (Authorization and Privacy), you have to set the User Name, Password and Privacy Password

SNMP access parameter	Description
Read only	▪ Enable/disable the read-only permission ▪ Read/Write is the default value
Admin	▪ Enable/disable the full access to the variables ▪ For example: ability to reboot the device ▪ Limited access is the default value
Privacy Password	▪ Set the privacy password ▪ It is necessary when privacy is enabled for the required security level

Table - SNMP Access

Traps

SNMP protocol operation requires a network agent instance to send asynchronous messages (traps) whenever a specific event occurs on the controlled device (object). InfiNet Wireless units have a built-in "*SNMP Traps*" support module (which acts as an agent) that performs a centralized information delivery from unit internal subsystems to the SNMP server. This zone focuses on "*SNMP Traps*" agent configuration.

In this section, you can view and edit the current "SNMP traps" settings. You can clone, remove and clear target and traps by clicking the corresponding buttons:

SNMP traps parameter	Description
Enable SNMP **Traps**	▪ Enable/disable to send "*SNMP traps*"
Agent IP	▪ Set the IP address of the device which sends traps
Transport	▪ Set the transport method ▪ Two options are available: ○ “IP” - all SNMP traps are sent to the server specified in the “Destination” field below ○ “MINT Gateway” - this option should be used when the SNMP server is located beyond a gateway that acts as an SNMP agent for the whole MINT network
Gateway MAC	▪ Set the MAC address of the gateway in your MINT network (relay device) if you selected “*MINT Gateway*” option ▪ If there's no MAC address specified, all "*SNMP traps"* are sent to the MINT SNMP relay ▪ The relay can be specified by checking the "*Trap Gateway"* check-box in the "Link Settings" section
Destination	▪ Set the IP address of the server and the UDP port (162 port is commonly used)

Table - SNMP Traps

SNMP trap types

The check boxes below specify traps or trap groups that are sent to the server:

SNMP **trap types**	**Description**

SNMP trap types	Description
topoGroup	▪ Events about topology changes in MINT network
topoEvent	▪ Number of neighbors or their status has changed (full neighbor list)
newNeighborEvent	▪ The new Neighbor has appeared
lostNeighborEvent	▪ The Neighbor has been lost
radioGroup	▪ Events which are related to changes of radio link parameters
radioFreqChanged	▪ The Frequency has changed
radioBandChanged	▪ The Band has changed
mintGroup	▪ Events about link quality changes in MINT network
mintRetries	▪ Retries has changed by more than 10%
mintBitrate	▪ The Bitrate has changed
mintSignalLevel	▪ Signal Level has changed by more than 10%

SNMP trap types	Description
ospfGroup	▪ Events about OSPF table changes in MINT network
ospfNBRState	▪ The State of the relationship with this Neighbor has changed
ospfVirtNBRState	▪ The State of the relationship with this Virtual Neighbor has changed
ospfIFState	▪ The State of the OSPF Interface has changed
ospfVirtIFState	▪ The State of the Virtual OSPF Interface has changed
ospfConfigError	▪ Parameters conflict in the configuration of 2 routers
others	▪ Other changes in MINT network
linkEvent	▪ One of the communication links represented in the agent's configuration has come up or come down
trapdColdStartEvent	▪ Cold Start event has occurred
snmpdAuthenticationFailureEvent	▪ Not properly authenticated SNMP protocol message has been received

SNMP **trap types**	**Description**
syslog	▪ Events about messages recorded in a system log

Table - SNMP Trap Types

Click the «**Clone**» button if you need to setup multiple SNMP servers. Each server can have an individual set of traps directed toward it.

Click the «**Clear**» button in order to clear all check-boxes for the current server.

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

4.3.8 QoS Options

QoS manager is a convenient and flexible mechanism to manipulate the data streams going through the device. The user can create up to 200 logical QoS channels characterized by different properties (such as priority levels and data transfer rates) and then assign data streams to these logical channels according to special rules of assignment. Packets going through different channels are thus modifying their own properties as well as the properties of their respective data flows.

CAUTION

All the settings for the QoS classes performed via CLI will be lost after saving any changes in the WEB GUI.

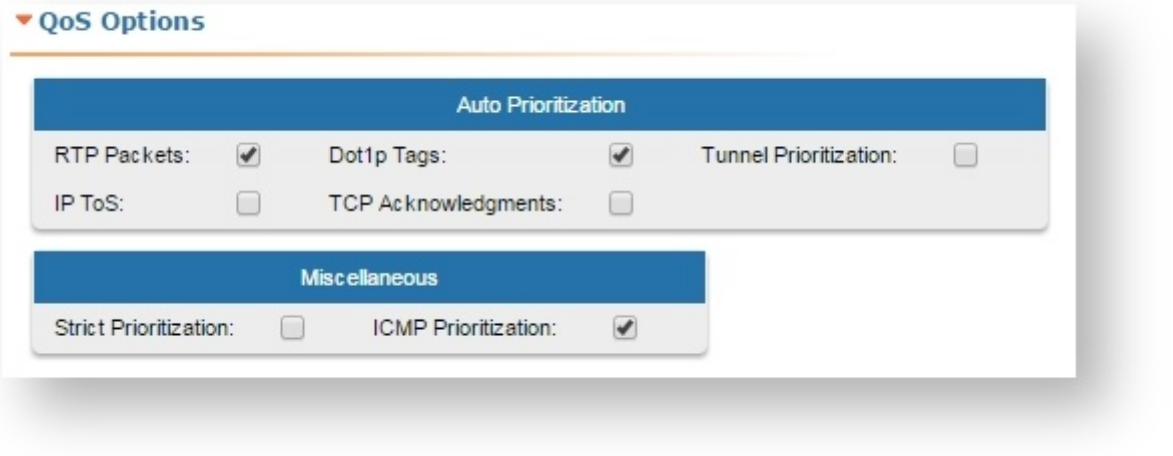


Figure - QoS Options default configuration

The following QoS parameters can be selected for traffic prioritization:

QoS **Parameter**	**Description**
RTP **Packets**	▪ Enable/disable automatic prioritization for all RTP traffic, regardless of the source or the destination IP ▪ Detect and prioritize the RTP packets (for example, if the packet is recognized as a voice packet, then it gets the priority 2, regardless of the previously assigned priority) ▪ Enabled by default
Dot1p Tags	▪ Enable/disable automatic prioritization for the packets tagged with IEEE 802.1p priority tags ▪ Detect and prioritize the packets using 802.1p tags ▪ Enabled by default
Tunnel Prioritization	▪ Enable/disable automatic prioritization for the tunnel traffic ▪ Allow prioritization within tunnels

QoS **Parameter**	**Description**
IP **ToS**	▪ Enable/disable automatic prioritization for the packets with a non-zero “ToS” field ▪ Detect and prioritize the packets using IP ToS tags
TCP **Acknowledgments**	▪ Enable/disable automatic prioritization for TCP ACK packets ▪ Automatically prioritize TCP acknowledgments
Strict Prioritization	▪ Enable Strict Prioritization traffic control policy ▪ By default, Weighted Fair Queue policy is used ▪ Refer to WANFleX OS User Manual for detailed policy descriptions ▪ Weighted fair queuing prioritization: unmark checkbox
ICMP **Prioritization**	▪ Enable/disable automatic prioritization for ICMP packets ▪ Allow ICMP traffic prioritization ▪ It does not increase the priority of "ping" packets (although they are ICMP packets)

Table - QoS

NOTE

Read the information in the section "Apply, Try and Preview buttons for the configuration" in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

4.3.9 Traffic Shaping

The "Traffic Shaping" section allows you to manipulate the data streams going through the device. You can create up to 200 logical channels characterized by different properties (such as priority levels and data transfer rates), and then to assign the data streams to these logical channels according to the special rules, previously created.

In the default configuration, there is no channel created. In order to prioritize the data flows and /or to set the data transfer rates, you have to create the logical channels by clicking the «**Add Channel**» button:

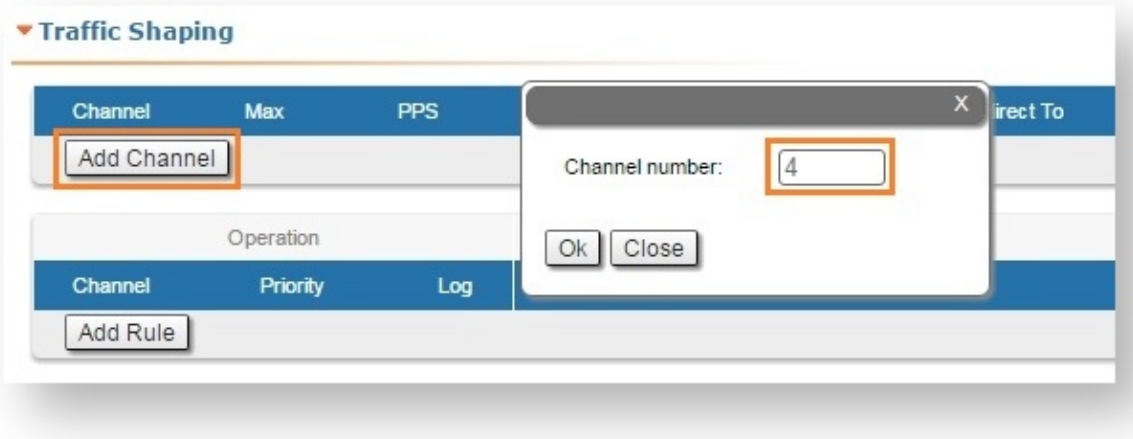


Figure - Add a logical channel

The following parameters can be configured in the "Traffic Shaping" section for the logical channels:

Logical channel parameter	Description
Channel	▪ Logical channel number (1-200 allowed)
Max	▪ Set the maximum transmit rate (in Kbps) ▪ You can limit the data traffic within a logical channel to a certain rate of kilobits per second

Logical channel parameter	Description
PPS	▪ Set the maximum packet per second rate (in pps) ▪ You can limit the data traffic within a logical channel to a certain rate of packets per second
Latency	Set latency value (between 5 ms and 200 ms) for each channel (queue length) ▪ Leave it empty for the default value ▪ Determines the maximum time the packets can to stay in the queue ▪ Packets are discarded if they are still in the queue after the value set for latency is reached
Priority	▪ Allocate the priority for all the packets going through a specific rule: ○ "*Up to*" - used to increase the packet priority to the specified value only if the processed packet has a lower priority ○ "*Set*" - used to assign a new priority regardless of the value already assigned to the packet
Redirect To	▪ Set the gateway IP address (only for the router mode) ▪ The whole stream is redirected to the specified IP-address regardless of the current routing configuration ▪ It may be useful when the router serves as a network access unit and two or more different clients want to access different providers through one unit
Information	▪ Set a description for the logical channel created

Table - Logical channel parameters

You can delete an existed logical channel by clicking the corresponding «**Remove Channel**» button.

You can create a traffic shaping rule by clicking the «**Add Rule**» button.

Traffic shaping rule parameter	Description
Channel	▪ Select the logical channel from the dropdown list ▪ All the parameters of this rule are applied to this channel
Priority	▪ Set the priority for the packets going through the new rule of the filter: ○ "*Up to*" - used to increase the packet priority to the specified value only if the processed packet has a lower priority ○ "*Set*" - used to assign a new priority regardless of the value already assigned to the packet
Log	▪ Enable/disable filter actions logging in the system log
Direction	▪ Set the input/output direction for applying the new rule: ○ "*Input*" - the rule is used to process inbound traffic ○ "*Output*" - the rule is used to process outbound traffic and for post-routing packet filtering
Interface	▪ Set the interface for applying the new rule ▪ All the available interfaces are displayed in the dropdown list (physical and logical) ▪ If "*any*" option is used, the rule is applied to all available interfaces
Group	▪ Set the Switch Group number for the applying of the new rule ▪ The Switch Group must be prior created

Traffic shaping rule parameter	Description
Rule	▪ Set the packet capture filter ▪ It is the same syntax called “PCAP expression”, as in the "Switching" section ▪ Refer to the filter expression syntax description above ▪ Validate the rule by clicking the «**Validate**» button

Table - Traffic shaping rules

You can delete an existed traffic shaping rule by clicking the corresponding «**Remove Rule**» button.

4.3.10 Extra commands

The "Extra Commands" section allows you to take advantage of the CLI configuration flexibility within the Web interface. While the Web interface is simple to use and understand, there are several parameters that can be configured via CLI **only**.

CAUTION

If any configuration changes are introduced via the Web interface later on, the configuration re-initializes and all CLI configured parameters are reset to default. Use this section to add CLI specific commands to the configuration in order to preserve the fine-tuning settings.

The commands that do not have the enhanced parameters displayed in Web interface are: *sys, ifconfig, prf, qm, tun, route, mint, switch, svi, lag, sntp, dhcpc*:

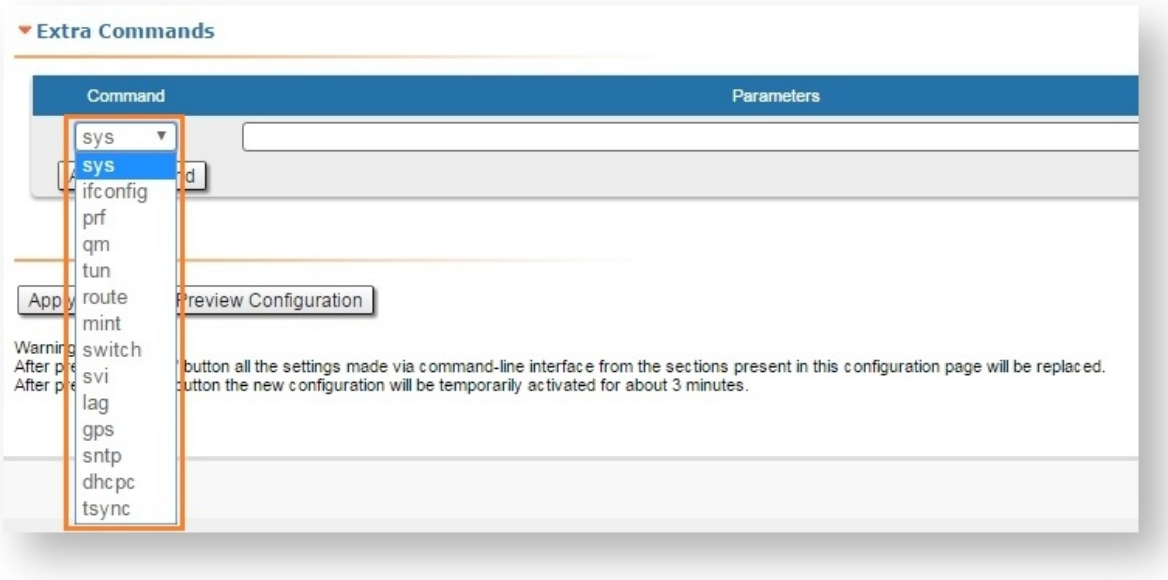


Figure - Extra commands

Parameter	Description
Command	▪ Select the command to add it to the device configuration
Parameters	▪ Insert the string to specify the command parameters and options ▪ Please refer to WANFleX OS User Manual for the full explanation of all command parameters and options
Disabled	▪ Check this option in order to disable the command temporarily

Table - Extra commands

- "**Up/Down**" arrows allow you to organize the command list
- Click the «**Remove Command**» button if you want to delete the command from the list permanently
- Click the «**Add command**» button if you want to add the command to the list

For example: choose "*sys*" command from the dropdown menu, type "no indicator" in the parameter field and then click the «**Apply**» button; this command is saved into the configuration (and not only executed) and is applied (switch off the LEDs of the unit) after reboot.

In the "Command Line" menu, the commands are only executed, but not saved into the configuration, while in "Extra commands" section from "Basic Settings" menu, the commands are executed and saved into the configuration.

4.3.11 Apply, Try and Preview buttons for the configuration

After performing the needed configuration in the "Basic Settings" menu, you must save all the new parameters by clicking the «**Apply**» button. If you are not sure about the effect of the new configuration performed, you can apply the new configuration temporarily by clicking the «**Test**» button. The previous configuration is automatically restored after a grace period of 180 seconds (3 minutes). You have the options to extend the grace period, or immediately accept/reject the changes.

By clicking the «**Preview Configuration**» button, you can view the configuration results in CLI-style format.

A warning message is displayed in this section to inform about the consequences of saving configuration via Web or CLI interfaces:

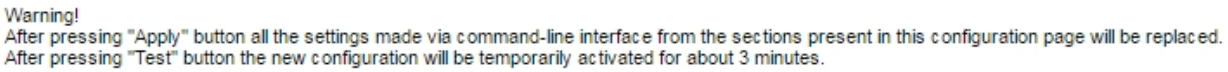


Figure - Apply, test and preview the configuration

After clicking the «**Apply**» button for saving the new configuration, the system will redirect you to the login page. After a 5 seconds timer you can log in back to the unit and check the new configuration.

4.4 Maintenance menu

The "Maintenance" menu allows you to perform service tasks for the device maintenance and to check the hardware and software version, reason for the last reboot, system uptime, current configuration, license, diagnostic card, etc.

"Maintenance" page has the following sections:

4.4.1 Firmware

Figure - Firmware

Parameter	Description
Firmware Version	▪ Displays the current firmware version ▪ The firmware string contains also the hardware platform type
Build Date	▪ Displays the firmware build date
Serial Number	▪ Displays the serial number of the unit
Part Number	▪ Displays the part number of the unit ▪ It contains information about the unit type
Platform	▪ Displays the processor model
Uptime	▪ Displays the system up time since the last reboot
Last Reboot Reason	▪ Displays the reason for the last reboot of the unit ▪ The options are: ○ Software fault ○ Unexpected restart ○ Manual restart ○ Manual delayed restart ○ Firmware upgrade ○ SNMP managed restart ○ Test firmware loaded

Table - Firmware parameters

By clicking the “Download Certificate for upgrade over SSL” link, you can download InfiNet Wireless self-signed certificate. This allows you to upgrade the unit software version when you are connected to the Web interface via HTTPS.

The system checks automatically for the firmware updates on the InfiNet Wireless repository and displays a warning message for 10s at each login to the Web interface if a new software version is available:

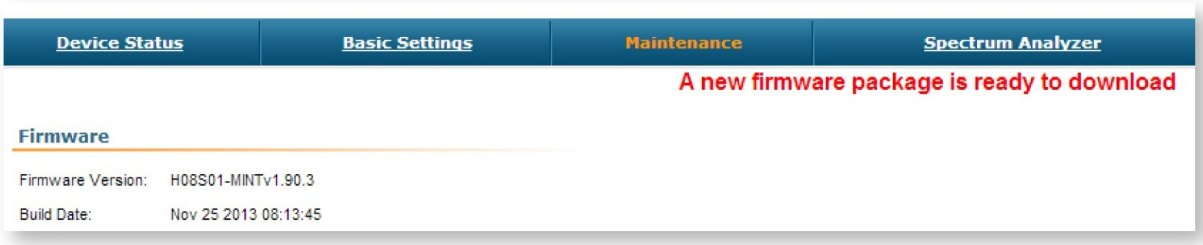


Figure - New firmware warning message

NOTE

It is not mandatory for the unit to have access to the Internet for this feature to work. However, the PC that is used to initialize the upgrade procedure must have access to InfiNet Wireless website (both http and ftp).

In case of new software version availability, after clicking the «**Check Latest Release**» button, the system provides the following options:

Figure - New firmware availability

By clicking the «**Upgrade Firmware**» button, the system starts the firmware upgrade process automatically:

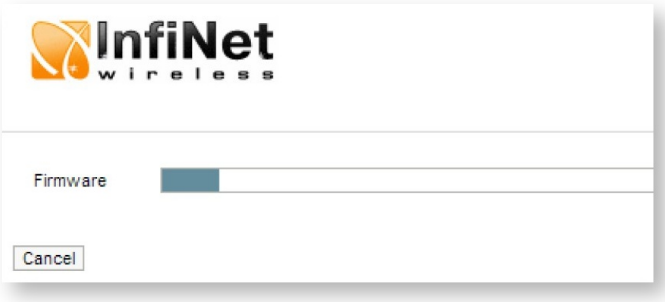


Figure - Firmware upgrade

After the firmware upgrade process ends, you have to reboot the unit before using the new software version:

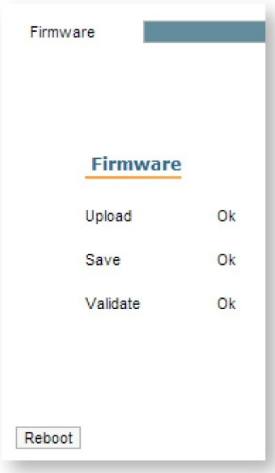


Figure - Firmware upgraded succesfully

By clicking the «**Save New Firmware**» button, you download the new firmware file locally on your PC.

If no new firmware version is available, the system provides a full change log for the latest firmware release after clicking the «**Check Latest Release**» button:

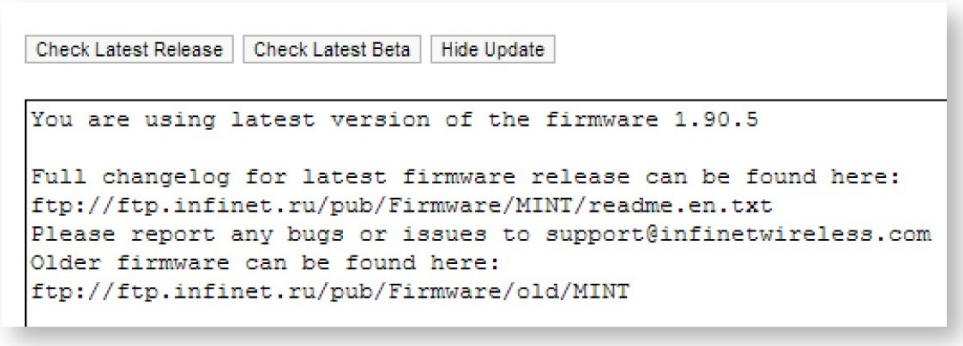


Figure - Latest firmware change log

The process above is the same in case of Beta firmware version. Click the «**Check Latest Beta** » button for it.

4.4.2 Upload

The "Upload" section allows you to upload other license, firmware and configuration files to the unit.

For each of the three options, click the «**Choose File**» button, followed by the «**Upload**» button after the file has been picked up.

After clicking the «**Upload**» button, the system performs three operations: uploading, saving and validating the new file uploaded and indicates if each of the operation succeeded or failed. In case that the process succeeded, you have to reboot the unit in order to apply the new changes.

4.4.3 Download

The "Download" section allows you to download locally, to the management PC, the current license, firmware and configuration files, by clicking the corresponding buttons: «**Download License**», «**Download Firmware**» and «**Download Configuration**».

4.4.4 Bottom section of the page

The following buttons are available:

- «**Reboot**» button - reboots the device. A warning message pops up asking for the permission before the operation to start. During the restart process, you are redirected to the login page and the timeout period of 35 seconds counts down before the new login:

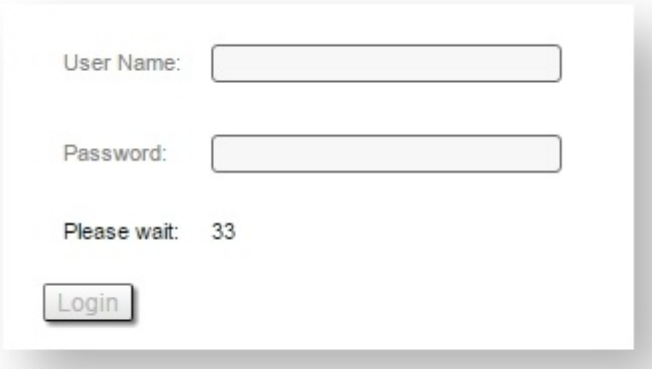


Figure - Unit reboot

- «**Restore Factory Settings**» button - restores the factory default configuration. A warning message pops up, asking for the permission before the operation to start. During the reset to factory process, you are redirected to the login page and the timeout period of 30 seconds counts down before the new login:
- «**View Current License**» button - shows the current device license parameters in a new window
- «**View Current Configuration**» button - shows the current device configuration in text format in a new window
- «**Create Diagnostic Card**» button - Tech Support Reports Generator. By clicking this button, the system downloads to the local PC a text file that contains the complete information (for the technical support specialists) set from the device such as: full device configuration listing, system log output, license information, "*mint map detail*" command output, interfaces statistics, etc.

4.5 Spectrum Analyzer menu

In the "Spectrum Analyzer" menu, you can perform a deep analysis of the radio emissions in the environment where the unit is placed. The unit scans the radio spectrum on all available frequencies. In order to obtain the information as accurate as possible, the scanning process may take a while.

CAUTION

When running spectrum scan on a unit accessible via the RF interface, connection will be lost during scan time (the radio-link will be disconnected). Use "**Last Snapshot** " button to see scan results.

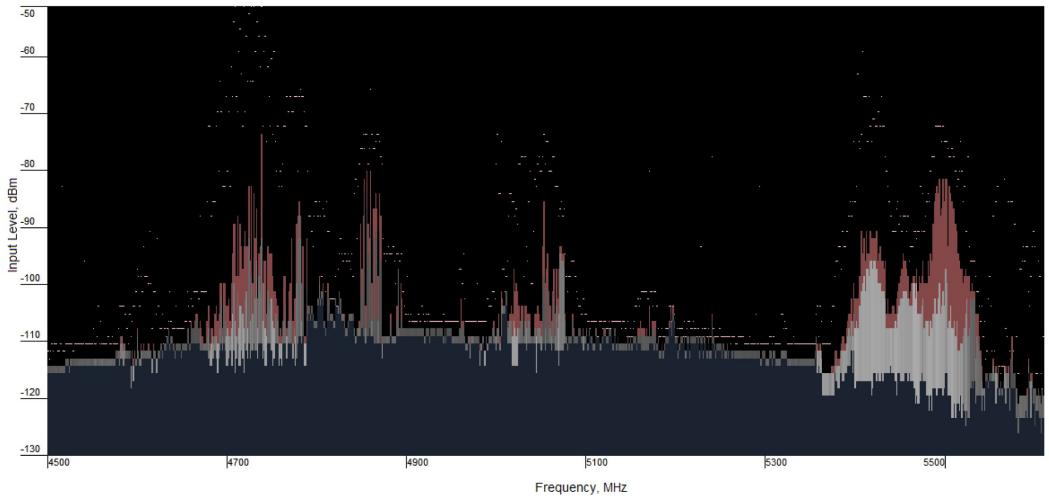


Figure - Spectrum analyzer

The following parameters are available in order to operate the Spectrum Analyzer:

Parameter	Description
Interface	▪ rf5.0 radio interface is the only option available, but it is showed for the backward compatibility with the dual radio legacy products
Start Frequency	▪ Set the first frequency for scanning (in MHz)
Stop Frequency	▪ Set the last frequency for scanning (in MHz)
Band	▪ Set the bandwidth (in MHz)

Parameter	Description
Step	▪ Set the scanning frequency step (in MHz) ▪ It is recommended to set 1 MHz “*step*” value to get more precise scanning results
Channel Mask	▪ Select which antenna to be used for scanning the radio environment ▪ “*Auto*” parameter is set by default. In this case scanning is perfomed by both antennas ▪ "1" - scanning is perfomed by antenna "1" ▪ "2" - scanning is perfomed by antenna "2" ▪ Parameter "3" means scanning is perfomed by both antennas
Scan Duration	▪ Set the time period for the scanning process (in seconds) ▪ After the end of this time period, scanning is stopped and the radio interface will be back to its normal mode operation
Enable Grid	▪ Mark/unmark the corresponding checkbox to display/hide the grid lines and highlight the special frequency channel on the scan output ▪ The highlighted frequency channel can be used to mark the channel which the device is currently working on or which it plans to use
Grid Width	▪ Set the bandwidth value for the highlighted frequency channel (in MHz)
Grid Frequency	▪ Set the central operating frequency for the highlighted frequency channel

Parameter	Description
RSSI mode	▪ Select the gradient-color type for the “*Max RSSI*” values to be displayed on the Spectrum Analyzer output screen ▪ The options are: ○ Normal (by default) ○ Gradient ○ Max Hold ○ Peak Hold

Table - Spectrum Analyzer

Start/stop Spectrum Analyzer by clicking the «**Start Sensor Test**»/«**Stop Sensor Test**» buttons.

By clicking the «**Last Snapshot**» button, you get the final scanning results. The most common usage of this feature is when you perform a spectrum scan at the remote unit on the other side of the radio link. When running a spectrum scan at such a unit (accessible via the RF interface), connection to this unit will be lost for a scan time. "*Last Snapshot*" option allows viewing scan results when the connection gets up again.

When you run spectrum scan on a local unit and the link is interrupted, the remote unit will not disappear from the spectrum picture. So you should silence the remote unit in order to have a real picture without it, otherwise you will always see noise signal on the operating frequency generated by the remote unit.

You can get detailed information about the scanned radio signals on a specific frequency. Just point a cursor on the needed frequency and you will see a hint with exact Signal level (dBm), Frequency (MHz), Noise Floor (dBm), RSSI (dBm), High RSSI (dBm), Max RSSI (dBm) values.

4.6 DFS menu

The "DFS" page provides the monitoring and management of the DFS operation. The DFS status and availability indicators are shown for each frequency for the given band and grid. The indicators are described in the Legend at the bottom of the page.

By clicking the «**Clear NOL**» button, you clear the non-occupation list with the blocked frequencies (due to the radars detected on these frequencies). The DFS subsystem rescans those frequencies and if they are still not available, the scanning starts after the time period displayed in the right bottom corner of the frequency indicator.

By clicking the «**Re-select Channel**» button, you restart the DFS scanning.

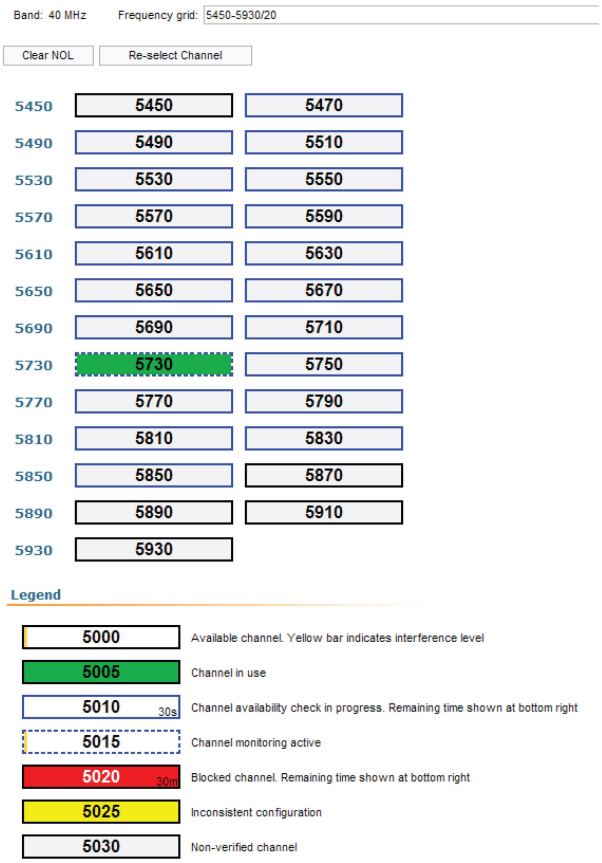


Figure - DFS

4.7 Command Line menu

The "Command Line" page emulates CLI (command line interface) in the Web interface. This allows managing and monitoring the device by using all the commands and functions that are available via standard CLI.

In order to run one or a set of **WANFleX** commands, type them in the command field and then click the «**Execute**» button. The output of the commands is displayed in the section above the command field:

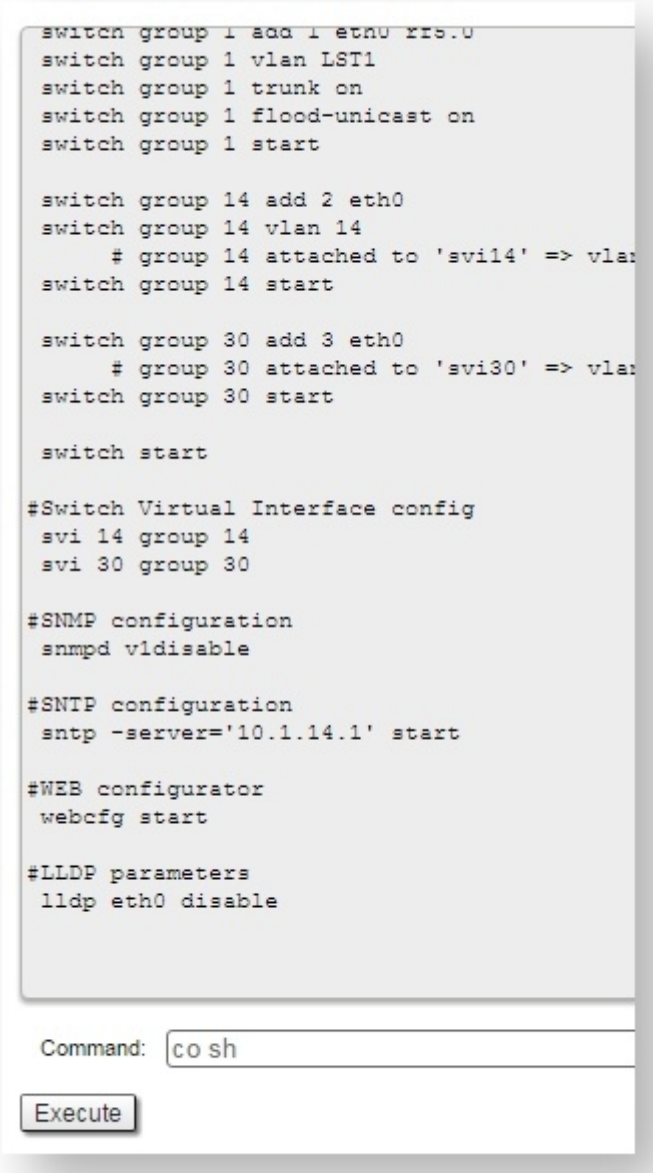


Figure - Command line

In the "Command Line" menu, the commands are only executed, but not saved into the configuration, while in "Extra commands" section from "Basic Settings" menu, the commands are executed and saved into the configuration.

5 Configuration scenarios

This chapter provides step by step instructions for some basic configurations of the **InfiNet Wireless R5000** units.

5.1 Setting up a basic PtP link

For this example, we have two **InfiNet Wireless R5000** units with the default factory configuration.

- **Step 1**

In order to access each of the units, we have to make sure that there is network connectivity between the PC used for the configurations and the units on their default Ethernet IP address which is 10.10.20.1/24.

- **Step 2**

Connect to the first unit using a Web browser and type any username and any password in the corresponding fields. Let's use in this example "test" for both username and password. After the authentication, a warning message pops up and requests us to change these initial authentication credentials:

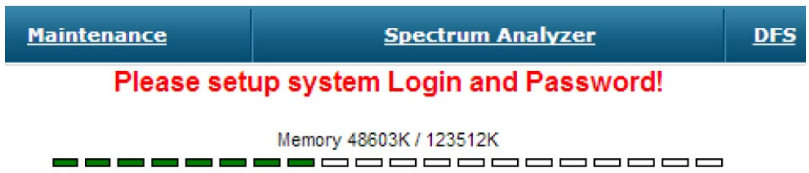


Figure - Warning message – setup system login & password

- **Step 3**

In order to change the initial credentials, we have to go to "Basic Settings" → "System Settings" and fill in the "*User Name*" and "*Password*" fields with the permanent authentication credentials. Let's use in this example "*Node1*" user name and "*Infi1*" password for the first unit and "*Node2*" user name and "*Infi2*" password for the second unit.

In the same section, we set the "*Device Name*" parameter for each unit. Let's name in this example "*Node1*" the first unit and "*Node2*" the second unit:

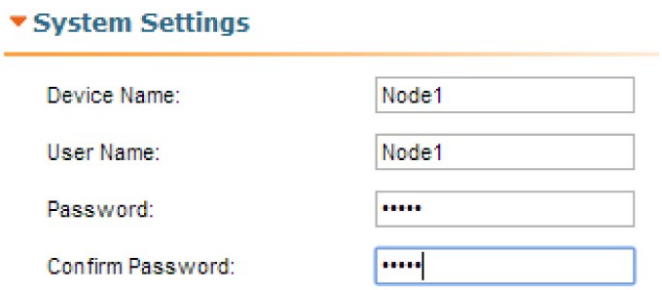


Figure - Edit system settings

- **Step 4**

In "Basic Settings" → "Network Settings" section, we can change the default IP address of the svi1 interface. Let's add the IP 192.168.1.1/24 for the first unit and the IP 192.168.1.2/24 for the second unit:

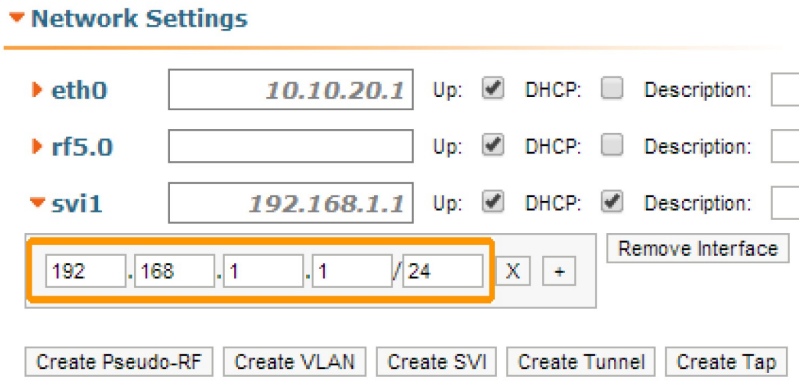


Figure - Add IP address on svi1 interface

- **Step 5**

In order to establish a wireless link between the two units, we have to set one of them as Master. By default, both units are configured as Slave.

In "Basic Settings" → "Link Settings" section let's configure the following radio parameters for the first unit:

- Type: Master
- Polling: On
- DFS: Off
- Node ID: 1
- Channel width: 40 MHz
- Frequency: 5870 MHz

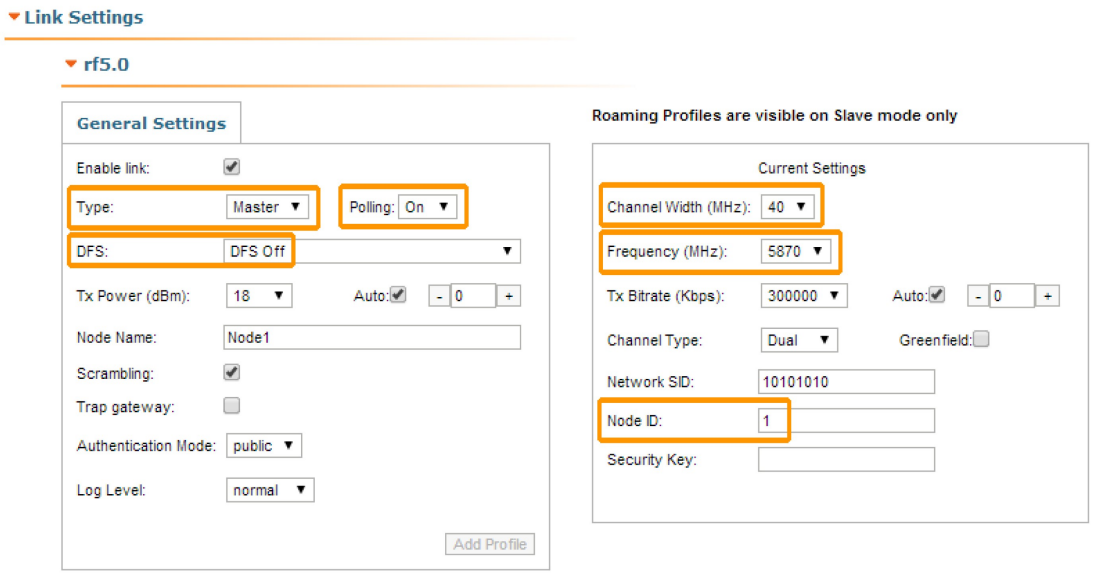


Figure - Set the radio parameters for the Master unit

- **Step 6**

Now we can save all settings performed in "Basic Settings" menu by clicking the «**Apply**» button at the bottom of the page.

- **Step 7**

We have now to connect to the second unit to its default IP address and to perform the configuration below:

- In "System Settings" section
  - Device Name: Node2
  - User Name: Node2
  - Password: Infi2
- In "Network Settings" section
  - svi1 IP address: 192.168.1.2/24
- In "Link Settings" section
  - Type: Slave
  - Node ID: 2
  - Channel width: 40 MHz
  - Frequency: 5870 MHz

We have to save all settings performed in "Basic Settings" menu by clicking the «**Apply**» button at the bottom of the page.

- **Step 8**

We connect now back to the first unit at the IP 192.168.1.1/24, and go to "Device Status" menu in order to check the link establishment between our two units and all real-time parameters provided by Web interface:

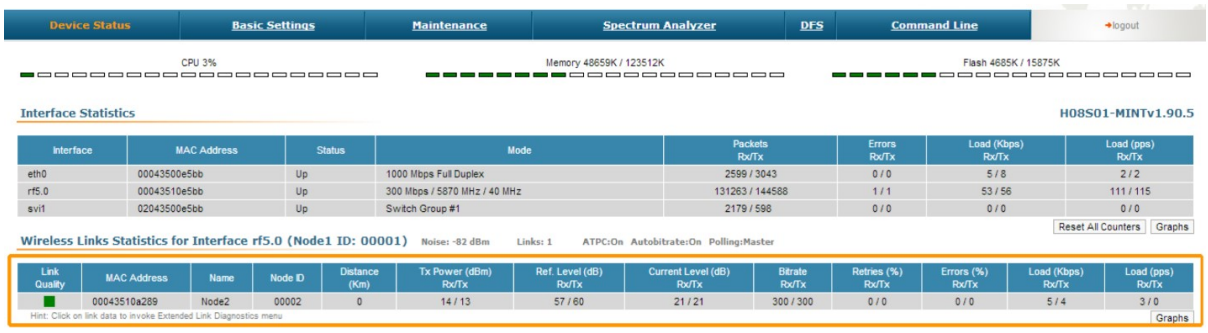


Figure - Wireless link establisment

5.2 Creating a basic PtMP configuration

One of the most common solutions to separate data traffic from the BS to the CPEs and vice versa is to create VLAN filters within different switching groups. For the management traffic, we have to create a separate switching group and VLAN. In this case, the CPEs cannot communicate between them and they cannot access the management VLAN:

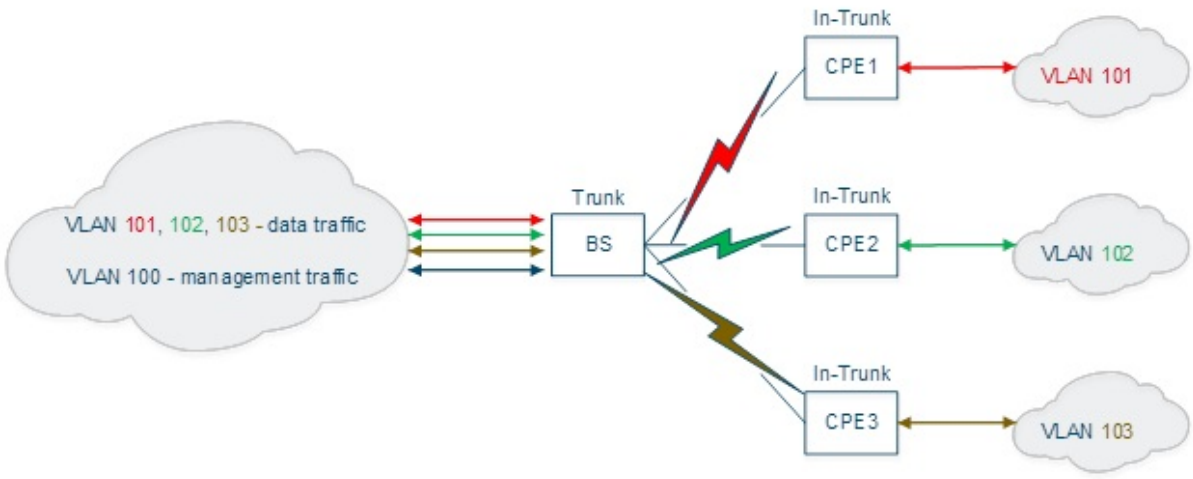


Figure - PtMP configuration

For this example, we have four **InfiNet Wireless R5000** units with the default factory configuration and we are going to configure one of them to work as BS and the other three to work as CPEs (in this example, from the traffic point of view).

- **Step 1**

Let's log in to one of the four units and configure it as BS. We have to go to "Basic Settings" → " MAC Switch" section and modify the configuration for the default Switch Group #1 in order to accommodate the traffic from all CPEs:

- Select Trunk mode for the Switch Group #1
- Add a new rule for this switch group and select VLAN mode for it
- Configure all VLANs that must be processed within this Switch Group #1: let's configure VLAN101, VLAN102 and VLAN103

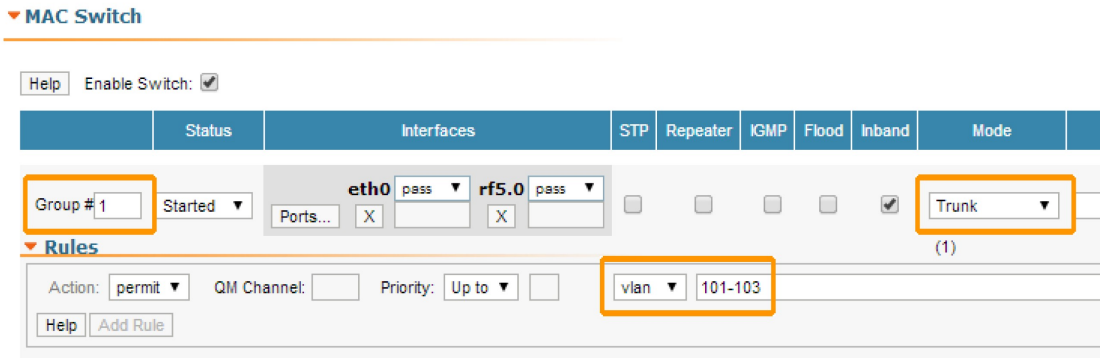


Figure - Create a VLAN rule

- **Step 2**

We have to create a second Switch Group for the management traffic to the unit:

- Click the «**Create Switch Group**» button and then enter a Switch Group number in the pop-up window (we strongly recommend using your management VLAN number as the management Switch Group number to avoid confusion)
- Click the «**Ports**» button and select Ethernet and RF interfaces in the pop-up window and then click the «**OK**» button
- Create a new rule: select VLAN mode and enter the VLAN numbers that must be processed within this Switch Group; let's configure VLAN100 for the management traffic.

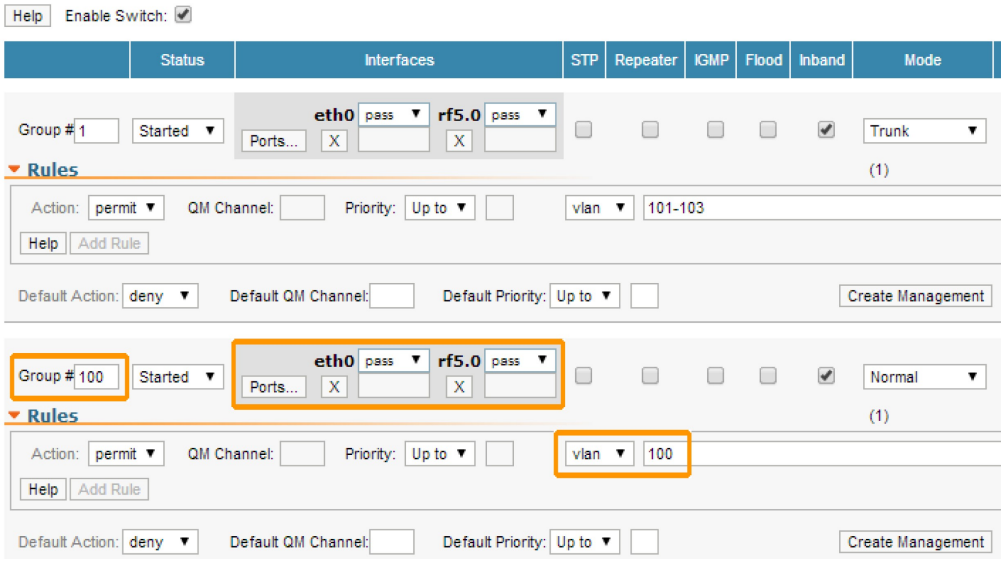


Figure - Create a management VLAN

- **Step 3**

We have to create an SVI interface for the management traffic to the unit:

- Open the "Network Settings" section
- Click the «**Create** SVI» button
- Enter the SVI interface number in the pop-up window and then Click the «**OK**» button (we strongly recommend using your management VLAN number for SVI interface number to avoid confusion)
- Select the Switch Group (the management Switch Group created in Step 2) that will be associated with this SVI interface.

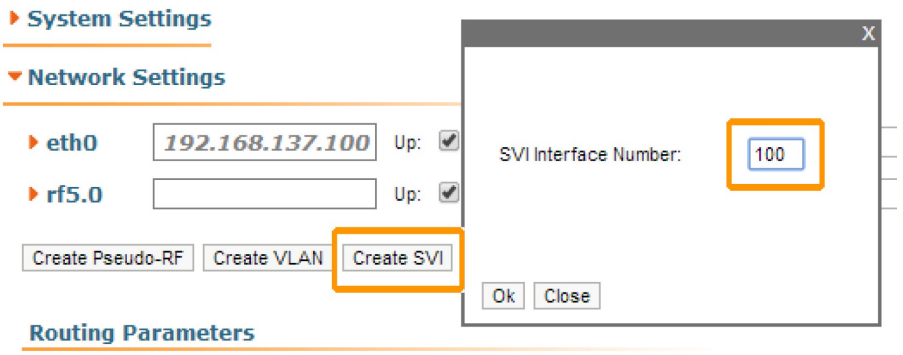


Figure - Create an SVI interface

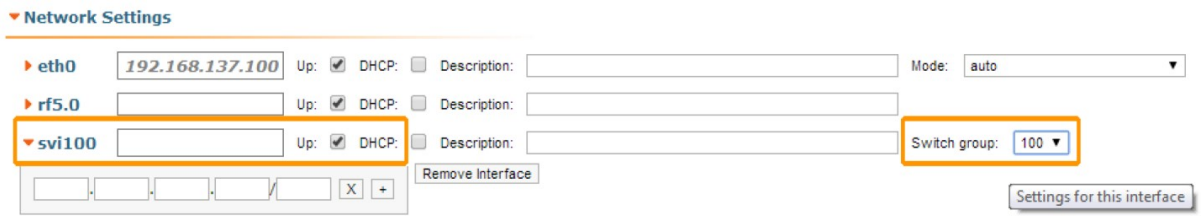


Figure - Associate a Switch group to the SVI interface

- **Step 4**

The management traffic in our network belongs to VLAN 100 and therefore, it is tagged. In order to access the unit through the management network, an L3-interface is needed to be accessible via VLAN 100.

For this purpose, we have to create a VLAN interface (it will act as a sub-interface of the SVI interface created in Step 3):

- Click the «**Create** VLAN» button
- Configure the "*svi100*" interface as the Parent interface for the "*vlan100*" interface
- Configure the "*Vlan ID*" parameter for the management VLAN 100
- Configure the IP address and the network mask for the management interface (let's set for this example the IP and mask 10.10.10.10/24).

Figure - VLAN interface associated to the SVI interface

- **Step 5**

Let's log in to one of the remained three units and configure it as CPE (in this example, from the traffic point of view). We have to configure two Switch Groups, as well: one for the data traffic and another one for the unit management. However, the default Switch Group #1 cannot be used for any of these purposes, so we are going to remove it in order to simplify the configuration:

- Go to the "Basic Settings" → "MAC Switch" section
- Click the «**Remove Group**» button on the Switch Group #1 subsection and then click the «**OK**» button:

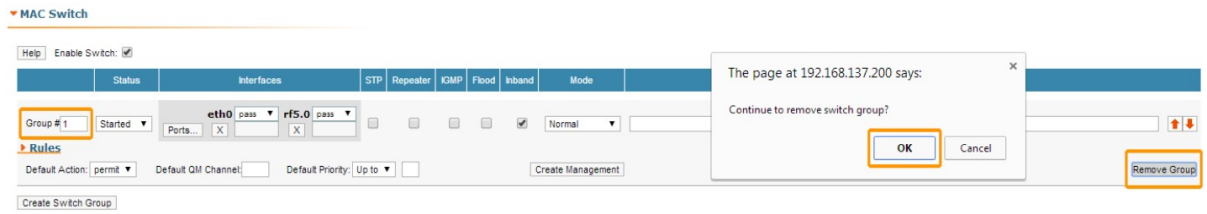


Figure - Remove the default Switch group

- **Step 6a**

We have to create another Switch Group that will handle all the data traffic that crosses through the CPE. The data traffic received by the CPE could be untagged (the scenario covered in this step) or tagged (the scenario covered in Step 6b).

The process is the same as the one described in the previous sections, however, there are two important differences:

- The Switch Group number must correspond with the VLAN number used by this client. We are going to configure VLAN 101 for the CPE 1 and the Switch Group #101.
- The Switch Group operation mode must be set to "*In-Trunk*". This mode requires a numerical parameter which is the Switch Group number (set in the BS) containing the necessary VLAN corresponding to the CPE. In our case, the client data traffic that goes to the BS from the upstream equipment is placed into Switch Group #1, so "*In-Trunk*" mode parameter must be set to 1.
- The Ethernet interface must act as an access port in this scenario, so the VLAN tag must be stripped (removed) from all egress packets and all inbound traffic should be tagged.

We are going to perform the following configuration:

- Click the «**Create Switch Group**» button
- Configure Switch Group 101 in the pop-up window
- Click the «**Ports**» button
- Select both Ethernet and RF interfaces in the pop-up window and then click the «**OK**» button
- Select strip from the drop-down menu of the eth0 operation modes to strip the VLAN tag
- Select In-Trunk mode for the Switch Group #101
- Set the In-Trunk value to 1, as our BS has the Switch Group 1 configured to process all CPEs data traffic.

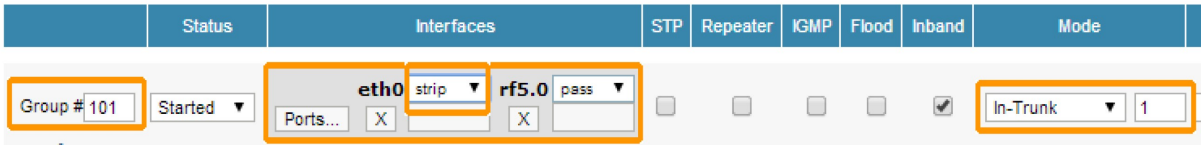


Figure - In-Trunk mode, untagged traffic

- **Step 6b**

The Ethernet interface must act as a trunk port in this scenario, so we have to create a filter rule for the Switch group #101.

In case the client has multiple VLANs, a separate Switch Group should be created for each VLAN.

We are going to perform the following configuration:

- Click the «**Create Switch Group**» button
- Configure Switch Group 101 in the pop-up window
- Click the «**Ports**» button
- Select both Ethernet and RF interfaces in the pop-up window and then click the «**OK**» button
- Select In-Trunk mode for the Switch Group #101
- Set the In-Trunk value to 1, as our BS has the Switch Group 1 configured to process all CPEs data traffic
- Open the Rules zone and click the «**Add Rule**» button
- Select VLAN mode and configure the VLAN 101 that must pass within this Switch Group.

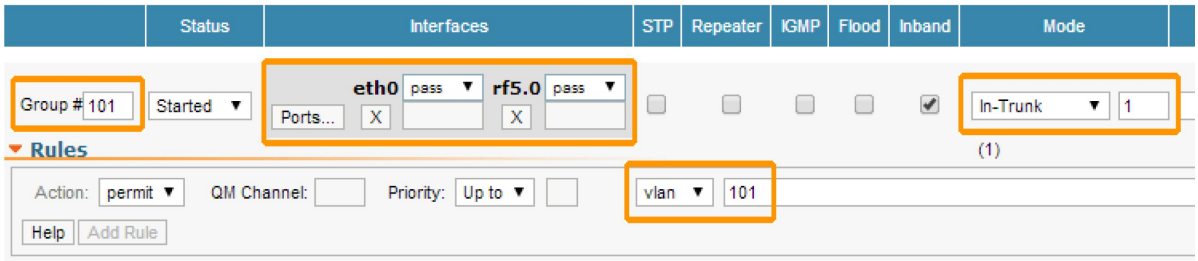


Figure - In-Trunk mode, tagged traffic

- **Step 7**

For the management traffic to the CPE, we have to configure a dedicated Switch Group, SVI and VLAN interfaces.

- Click the «**Create Switch Group**» button
- Configure Switch Group 100 in the pop-up window (we strongly recommend using your management VLAN number as a management Switch Group number to avoid confusion)
- Click the «**Ports**» button
- Select RF interface only and click «**OK**»
- This Switch Group contains only the RF interface, as the management interface needs to be accessible only from the uplink direction
- Create a rule: select VLAN mode and enter the VLAN numbers that must be processed within this Switch Group; let's configure VLAN100 for the management traffic.

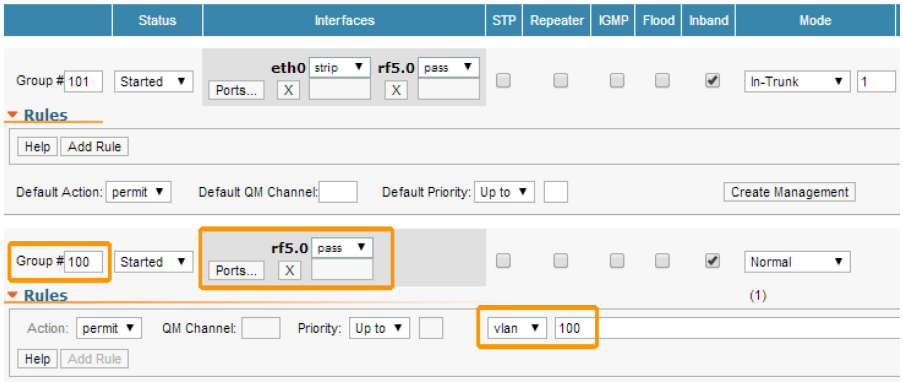


Figure - Management Switch group

- **Step 8**

We have to create an SVI interface for the management traffic to the unit:

- Open the "Network Settings" section
- Click the «**Create** SVI» button
- Enter the SVI interface number in the pop-up window and then click the «**OK**» button (we strongly recommend using your management VLAN number for SVI interface number to avoid confusion)
- Select the Switch Group (the management Switch Group created in Step 7) that will be associated with this SVI interface.

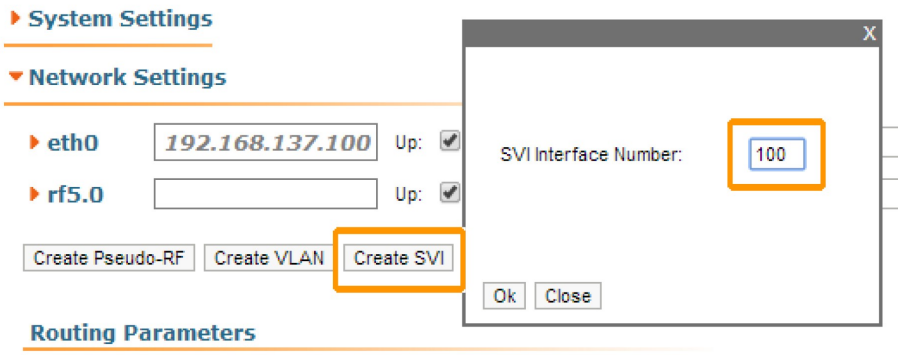


Figure - Create an SVI interface

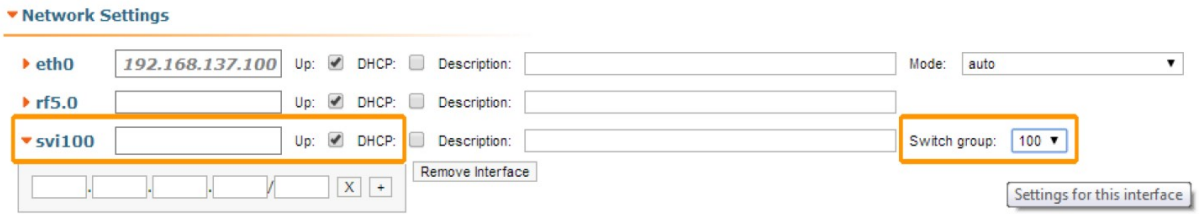


Figure - Associate a Switch group to the SVI interface

- **Step 9**

All management traffic in our network belongs to VLAN 100 and therefore, it is tagged. In order to access the unit through the management network, an L3-interface is needed to be accessible via VLAN 100.

For this purpose, we have to create a VLAN interface (it will act as a sub-interface of the SVI interface created in Step 8:

- Click the «**Create** VLAN» button
- Configure the "*svi100*" interface as the Parent interface for the "*vlan100*" interface
- Configure the "*Vlan ID*" parameter for the management VLAN 100
- Configure the IP address and the network mask for the management interface (for this example, let's set the IP and mask 10.10.10.101/24).

Figure - VLAN interface associated to the SVI interface

Please repeat the steps from 5 to 9 in order to configure the other two CPEs. Configure Switch groups 102 and 103, filter rules for the VLANs 102 and 103 (in case of tagged traffic) and management IP addresses on "*vlan100*" interface as 10.10.10.102/24 and 10.10.10.103/24, accordingly.

- The BS configuration file, as a result of the settings described in steps above:

```
#System parameters
#Factory password mode: single
sys name Node1
sys prompt Node1
sys user admin
setpass $1$5ieEa$9sTTnyEx4/1thTlmfb/S6.

#Radio module parameters
rf rf5.0 grid 40 4930-5930/20
rf rf5.0 grid 20 4920-5940/20
rf rf5.0 grid 10 4915-5945/5
rf rf5.0 grid 5 4915-5945/5
rf rf5.0 band 20
rf rf5.0 mimo
rf rf5.0 freq 5860 bitr 130000 sid 10101010 burst
rf rf5.0 txpwr -5 pwrctl distance auto(4)

#DFS configuration
dfs rf5.0 dfsoff
dfs rf5.0 freq auto
dfs rf5.0 cot off

#Interfaces parameters
ifc lo0  127.0.0.1/32
ifc eth0 media auto mtu 1500 up
ifc eth0 192.168.137.100/24
ifc rf5.0 mtu 1500 up
ifc svi100 mtu 1500 up
           # group 100
ifc vlan100 mtu 1500 up
ifc vlan100 10.10.10.10/24
ifc vlan100 vlan 100 vlandev svi100
           # group 100

#QoS manager
qm option rtp dot1p notos noicmp notcpack nostrict

#MINT configuration
mint rf5.0 -name "Node1"
mint rf5.0 -nodeid 00001
mint rf5.0 -type master
```

```
mint rf5.0 -mode fixed
mint rf5.0 -key "12345678"
mint rf5.0 -scrambling
mint rf5.0 -autobitrate
mint rf5.0 -minbitrate 13000
mint rf5.0 -hiamp 2 -loamp 0
mint rf5.0 -log
mint rf5.0 prof 1 -freq auto -sid 10101010 -bitr 130000 -band 20 \
            -nodeid 22363 -type slave -netid 0 \
            -minbitr 13000 -autobitr -mimo \
            -key "12345678"
mint rf5.0 -roaming leader
mint rf5.0 -authmode public
mint rf5.0 -airupdate passive normal
mint rf5.0 -rcmdserver enabled
mint rf5.0 poll start
mint rf5.0 start

#MAC Switch config
switch list LST1 numrange add 101-103

switch group 1 add 1 eth0 rf5.0
switch group 1 vlan LST1
switch group 1 trunk on
switch group 1 start
switch group 100 add 2 eth0 rf5.0
switch group 100 vlan 100
     # group 100 attached to 'svi100' => vlan100
switch group 100 start

switch start

#Switch Virtual Interface config
svi 100 group 100

#WEB configurator
webcfg start

#LLDP parameters
lldp eth0 enable txrx
```

- The CPE1 configuration file, as a result of the settings described in steps above (the trunk port scenario):

```
#System parameters
#Factory password mode: single
sys name Node2
sys prompt Node2
```

```
sys user admin
setpass $1$TC3kB$oILIriOiwU/knH3a5EkH70

#Radio module parameters
rf rf5.0 band 20
rf rf5.0 mimo
rf rf5.0 freq 5860 bitr 130000 sid 10101010 burst
rf rf5.0 txpwr 10 pwrctl distance auto(4)

#DFS configuration
dfs rf5.0 dfsonly

#Interfaces parameters
ifc lo0 127.0.0.1/32
ifc eth0 media auto mtu 1500 up
ifc eth0 192.168.137.200/24
ifc rf5.0 mtu 1500 up
ifc svi100 mtu 1500 up
            # group 100
ifc vlan100 mtu 1500 up
ifc vlan100 10.10.10.101/24
ifc vlan100 vlan 100 vlandev svi100
            # group 100

#QoS manager
qm option rtp dot1p notos noicmp notcpack nostrict

#MINT configuration
mint rf5.0 -name "Node2"
mint rf5.0 -nodeid 00002
mint rf5.0 -type slave
mint rf5.0 -mode fixed
mint rf5.0 -key "12345678"
mint rf5.0 -scrambling
mint rf5.0 -autobitrate
mint rf5.0 -minbitrate 13000
mint rf5.0 -hiamp 2 -loamp 0
mint rf5.0 -log
mint rf5.0 prof 1 -freq 5860 -sid 10101010 -bitr 130000 -band 20 \
            -nodeid 00002 -type slave -netid 0 \
            -minbitr 13000 -autobitr -mimo \
            -key "12345678"
mint rf5.0 -roaming enable
mint rf5.0 -authmode public
mint rf5.0 -airupdate passive normal
mint rf5.0 -rcmdserver enabled
mint rf5.0 start

#MAC Switch config
switch group 101 add 1 eth0 rf5.0
switch group 101 vlan 101
```

```
switch group 101 in-trunk 1
switch group 101 start

switch group 100 add 2 rf5.0
switch group 100 vlan 100
      # group 100 attached to 'svi100' => vlan100
switch group 100 start

switch start

#Switch Virtual Interface config
svi 100 group 100

#WEB configurator
webcfg start

#LLDP parameters
lldp eth0 enable txrx

#end
```

5.3 Remote management of the R5000 units

In this section procedure about remote management of the **InfiNet Wireless R5000** units, using network logical interface SVI and auxiliary network logical interface VLAN, is described.

- Switching process in WANFleX
- Create a management interface

5.3.1 Switching process in WANFleX

InfiNet Wireless units use proprietary protocol MINT above Layer 2 and lower than Layer 3 in reference to OSI Layer model.

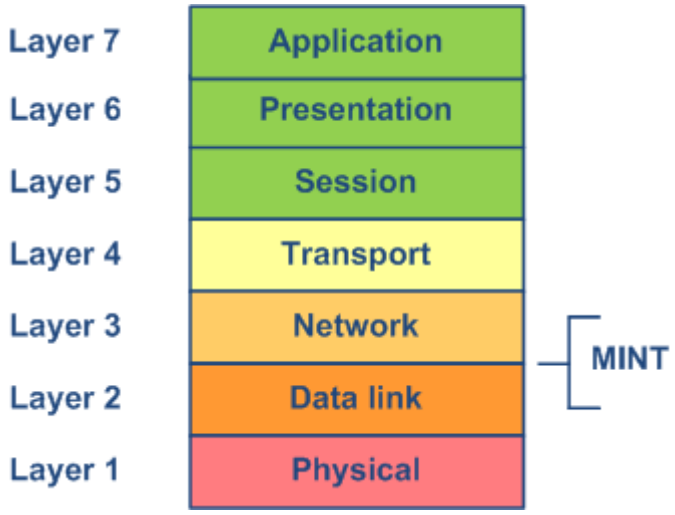


Figure - MINT position in OSI model

MINT stands for Mesh Interconnection Network Technology which points to the technology for networks based on arbitrary connections. The most important feature of MINT architecture is its ability to present any wireless (or even sometimes wired) network as a flat Ethernet segment, and radio interface connected to this network will act as usual Ethernet interface (virtual).

MINT protocol has built-in capability to establish connections to MINT neighbors and share information of other connected MINT neighbors. There is no need to configure and adjust MINT protocol settings. MINT unique feature is the ability to choose optimal paths in a network with multiple nodes and connections. Each neighbor connection can be evaluated as special value – i.e. "*Cost*". Its physical meaning – an estimated time for packet delivery measured in conventional units. The less the "*Cost*", the higher probability that this path will be chosen. The "*Cost*" of each connection is constantly changing according to link parameters including radio values (signal-to-noise levels), type of modulation speed used, number of errors and retries, link load and other parameters thus allowing quickly switching to an alternative route if its cost will be lower than for the current one.

So, the switching process is done by MINT protocol. The switching in MINT is done ONLY between two units or more. Each time you have some data for switching you should consider at least two devices as single switch path. Right now lets treat two InfiNet Wireless units as virtual “spatial” switch which has only two physical Ethernet ports, so you can just simply switch all traffic between two Ethernet ports (each port belongs to different unit).

However, in order to differentiate between traffic and its destination when you have more than two devices or more than one traffic type is to use VLAN tagging. In MINT we use Switch Group ID to make traffic differentiation. That is why all VLAN tags (or any other filter criteria) should be used to assign traffic to different Switch Group. While traffic resides in MINT domain it will be transferred only between InfiNet units with configured and same fixed Switch Group ID number. Switch Group is a logical entity which allows switching between physical ports binded to Switch Group.

So, all traffic destined for switching is transported by MINT protocol in special Switch Groups. Switch Groups are mostly used as container to transport VLAN tagged traffic through MINT network. Therefore, MINT network can be viewed as one virtual distributed switch where border nodes act as external ports of the virtual switch. Switch task is to transparently transport packets from one external port to another one (other ones). Important to understand that switching groups should be created only on the nodes where packets enter from "outside" network ("outside" relative to MINT).

Therefore, if the Switch Group was created and Ethernet port (for example, "*eth0*") and Radio port (for example, "*rf5.0*") were added then the switching from "*eth0*" to "*rf5.0*" and vice versa has been enabled.

SVI is special logical interface that can be assigned to Switch Group therefore one can access and manage the unit via dedicated Switch Group and via dedicated VLAN.

NOTE

Detailed information about MINT is described in the document "R5000 - MINT & Mobility" - White paper, which is available via http://infinetwireless.com/products/materials#white-papers (free registration is required).

5.3.2 Create a management interface

Initially it is required to select Switch Group to transfer management traffic. In default configuration, in "MAC Switch" section, Switch group #1 is available with "*eth0"* and "*rf5.0"* interfaces added and with no additional rules. In this case, all frames coming to the unit from local Ethernet interface will be delivered to the opposite side of the link and sent out the remote Ethernet interface and vice versa. This simple configuration will enable transparent switching - all packets will go through the link unchanged; "*VLAN tags*", "*QoS*" fields, etc. will be preserved.

Nevertheless, in case of remote VLAN management in order to separate customers traffic and management at least two switch groups should be used: one Switch Group for management, another Switch Group for customers traffic.

- **Step 1**

In "Basic Settings" → "MAC Switch" section, we have to delete the svi1 interface (which is available in the default configuration) by clicking the «**Remove Management**» button:

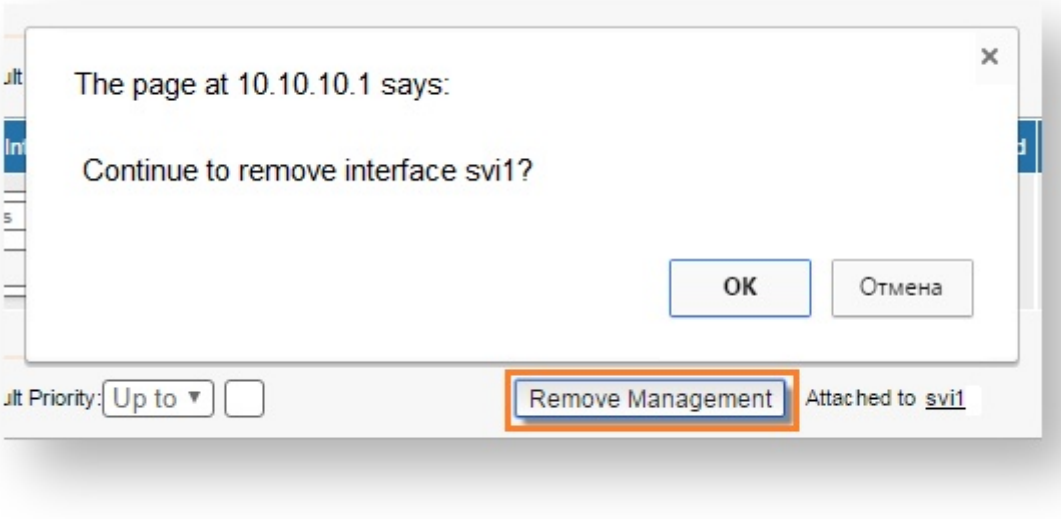


Figure - "Remove Management" button

- **Step 2**

In order to create two Switch Groups (or only add additional Switch Group for management traffic) go to the "Basic Settings" → "MAC Switch" section and click "**Create Switch Group**" button.

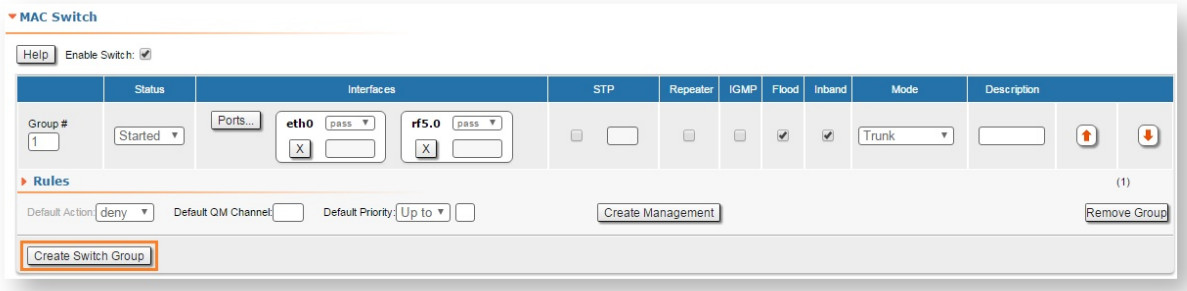


Figure - Create Switch Group

- **Step 3**

Add both wired "*eth0*" and radio "*rf5.0*" interfaces to this switch group

Figure - Add interfaces to the switch group

- **Step 4**

Move management switch group to the top using arrows on the right

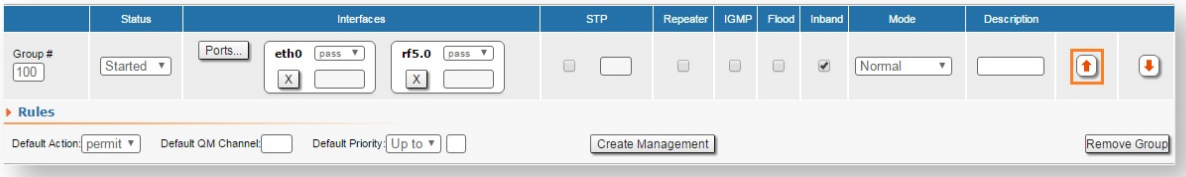


Figure - Move switch group to the top

- **Step 5**

We have to create a VLAN interface and to assign it an ID. Let's create VLAN 100 interface by clicking the «**Create Management**» button and setting the ID 100:

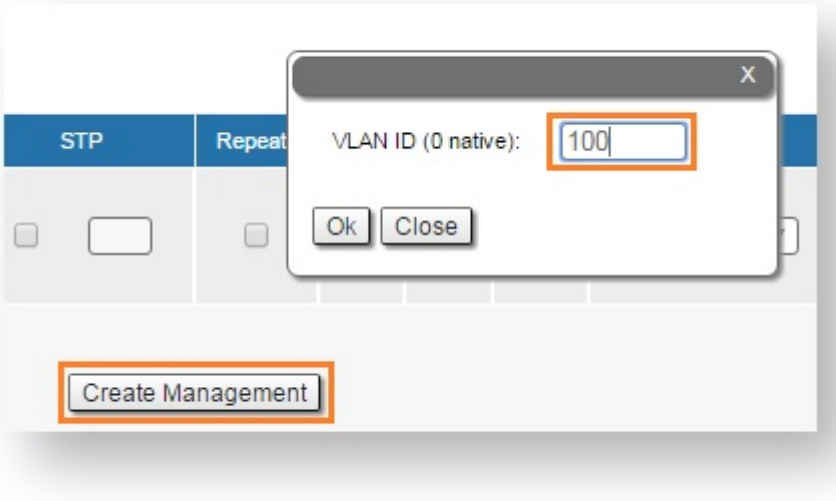


Figure - Create Management button

NOTE

For tagged management choose the appropriate vlan tag for management traffic. For untagged management choose "*0*" tag value in case you don't need vlan management.

- **Step 6a (In case to enable capability to work with VLAN tagged management traffic)**

In "Basic Settings" → "Network Settings" section set IP-address to the unit on auxiliary VLAN interface (don't forget about netmask).

NOTE

Please first remove the IP-address from "*eth0*" interface by just clicking the "**X**" box.

You can leave factory IP-address on "*eth0*" interface in case it does not belong to any of your production network subnets. IP-address on "*eth0*" will remain local for wired Ethernet segment only.

Figure - Set IP-address to VLAN interface

In "Basic Settings" → "MAC Switch" section, we can observe that a new rule has been created automatically for VLAN 100 within Switch group 100:

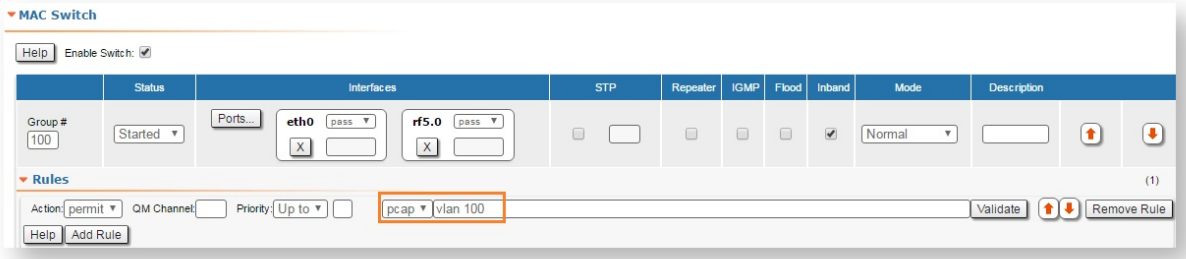


Figure - Create a MAC switch rule

For the data traffic, we have to create a separate Switch group.

- **Step 6b (In case there is no need in VLAN tagged management interface)**

In "Basic Settings" → "Network Settings" section set IP-address to the unit on SVI interface (don't forget about netmask).

NOTE

Please first remove the IP-address from "*eth0*" interface by just clicking the "**X**" box.

You can leave factory IP-address on "*eth0*" interface in case it does not belong to any of your production network subnets. IP-address on "*eth0*" will remain local for wired Ethernet segment only.

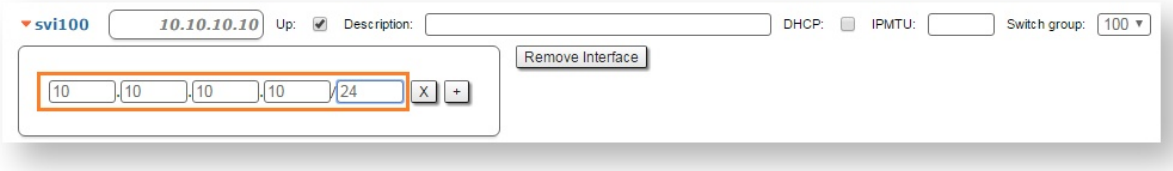


Figure - Set IP-address to SVI interface

- **Step 7 (Optional)**

Set the default gateway IP-address

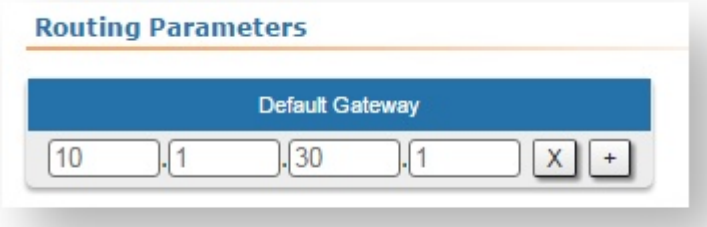


Figure - Gateway IP-address

- **Step 8**

Before saving the current configuration, please make sure that you can access the unit on VLAN 100. If you connect the PC directly to the unit, you have to set VLAN 100 for the outgoing traffic at the network interface.

- **Step 9**

Try the new configuration temporarily by clicking on the "**Test**" button

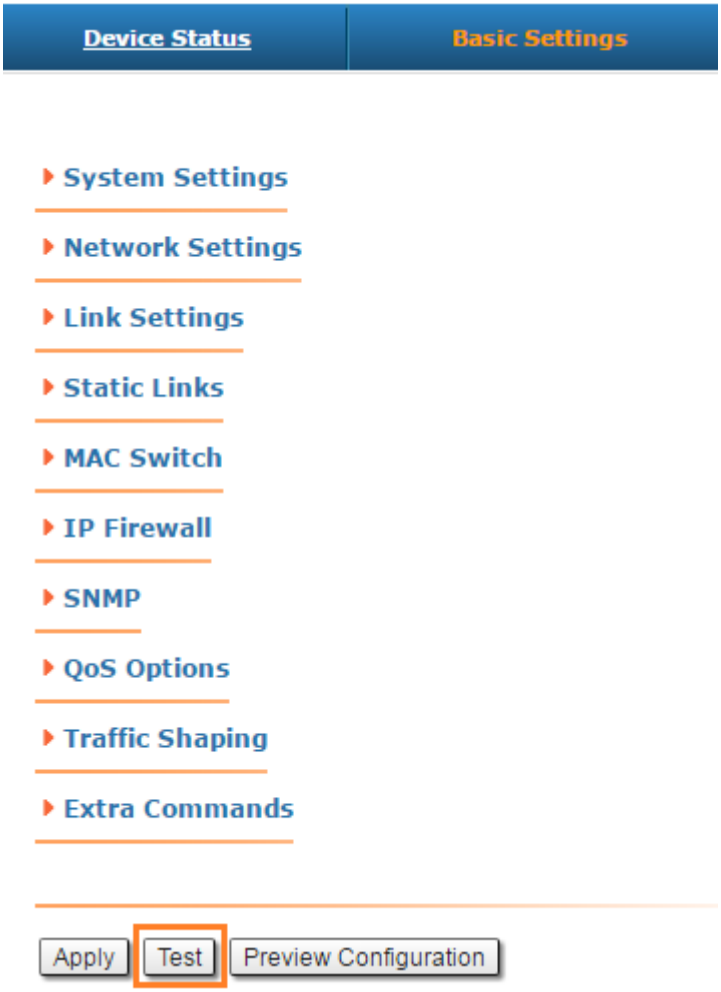


Figure - "Try" button

- **Step 10**

If everything works properly, you can save the settings performed in all sections of the "Basic Settings" page, by clicking the «**Commit**» button.

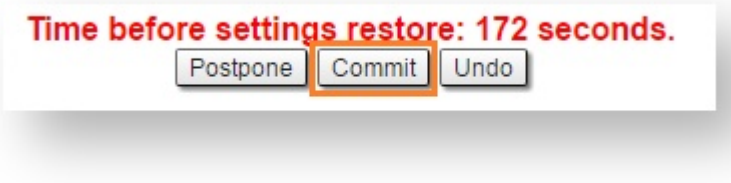


Figure - "Commit" button

NOTE

Read information at the "Apply, Test and Preview buttons for the configuration" section in order to find out the output of the «**Apply**», «**Test**» and «**Preview**» buttons for the new configuration performed.

We have created switch group for management traffic, special interfaces for vlan management and we have set an IP-address to the vlan management interface. Now there should be connection to unit through VLAN 100.

We have to perform the same settings for the second unit and check the connectivity with VLAN 100 to each unit.

NOTE

If you have firmware version "*MINTv1.89.0*" or lower please follow procedure described in the "Remote management of the R5000 units with firmware "MINTv1. 89.0" or lower" section.

5.4 Configuring an SNMP v3 account

The SNMP protocol exposes the management data as variables of the managed units which are queried and set by the network management systems, like **InfiMONITOR**. In order to be managed and monitored, each unit in the network must run the “agent” software component for reporting the information via SNMP.

By default, the "*SNMP agent*" is disabled, so the first action to be done before connecting the **InfiNet Wireless R5000** unit (with the default configuration) into the network for the monitoring purpose is to enable the "*SNMP agent*".

This is the first setting that we have to perform within this configuration example. After the authentication, let’s go to "Basic Settings" → "SNMP" menu and then click on the "*Access"* option:

Figure - SNMP access

In this section, we select the "*Start SNMP*" corresponding checkbox (in order to enable the "*SNMP agent*") and unselect "*Version 1 enable*" corresponding checkbox (in order to disable the SNMPv1, which is enabled in the default configuration). Then click the «**Add** SNMP**v3 User**» button and insert your desired SNMP login and password into the "*User Name*" and "*Password*" fields and leave the rest of the parameters available in this section with their default values:

Figure - Create SNMPv3 account

In order to finalize the SNMP configuration, click the «**Apply**» button (at the bottom of the page).

Now, we have the "*SNMP agent*" active and the SNMPv3 account already created for our unit.

5.5 Configuring radio profiles

One of the most common situations when we configure more than one radio profile for a CPE is when it can establish a wireless link to more than one base station, depending on the link quality. The CPE can switch the communication with other base stations in order to be operational and to provide services in the situation when the wireless link with the main BS is dropped.

For this example, we have three units with the default configuration.

- **Step 1**

After the authentication on the first unit, let's go to "Basic Settings" → "Link Settings" menu and let's do the following configuration in "General Settings" section:

- Enable link: selected
- Type: slave (for the CPE)
- MultiBS: selected (this option tells the CPE to search automatically for another BS when the link with the main BS is lost)
- Auto Tx Power: selected
- Node name: Node2

Click the «**Add Profile**» button, set the profile number 2 and then click the «**OK**» button:

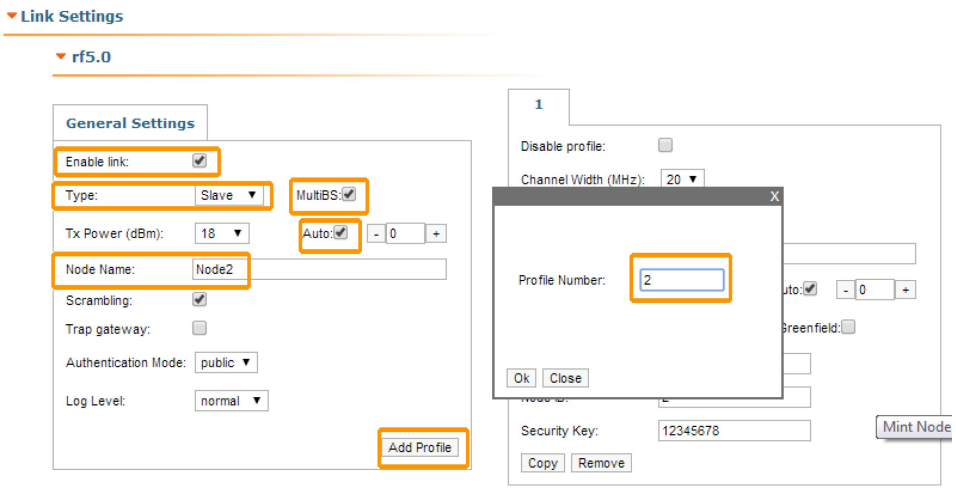


Figure - Add radio profile

Thus, the second radio profile is created with the same settings as the first profile (except the frequency, which is set to "*Auto*").

Let's do the following configuration for the first radio profile:

- Disable profile: unselected
- Channel Width: 20 MHz
- Frequency: 5860 MHz
- Node ID: 2
- Security Key: 12345678

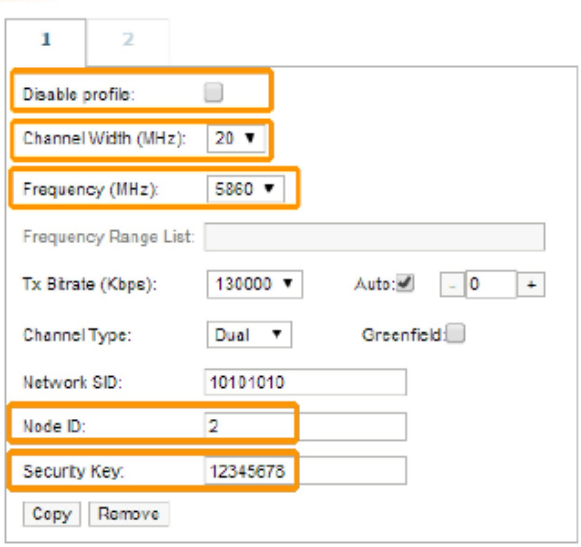


Figure - Radio profile 1 configuration

Let's do the following configuration for the second radio profile:

- Disable profile: unselected
- Channel Width: 10 MHz
- Frequency: 4920 MHz
- Node ID: 2
- Security Key: 11111111

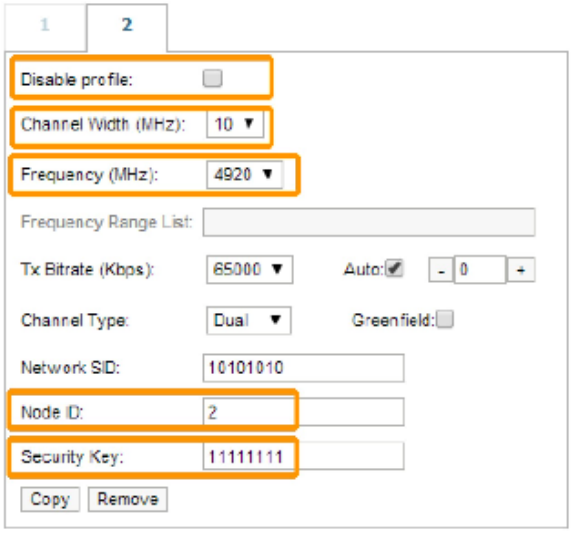


Figure - Radio profile 2 configuration

We have to click the «**Apply**» button at the bottom of the page, in order to save the settings performed in "Link Settings" menu.

- **Step 2**

Let’s now connect to the second unit and after the authentication step, let’s go to "Basic Settings" → "Link Settings" menu and let’s do the following configuration in the "General Settings" section:

- Enable link: selected
- Type: master (for the BS configuration)
- Polling: On
- Auto Tx Power: selected
- Node name: Node1

Let’s do the following configuration in the "Current Settings" section:

- Channel Width: 20 MHz
- Frequency: 5860 MHz
- Node ID: 1
- Security Key: 12345678

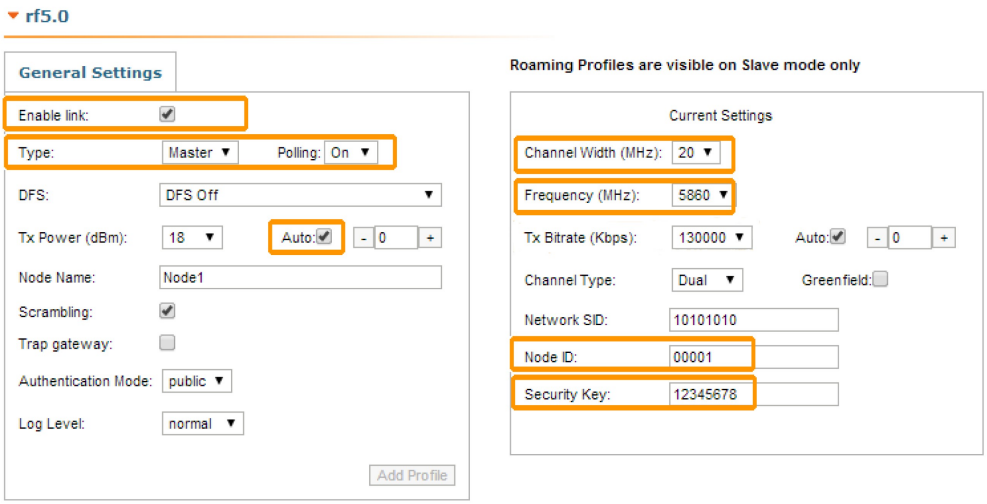


Figure - First BS radio configuration

Click the «**Apply**» button at the bottom of the page, in order to save the settings performed in the "Link Settings" menu.

- **Step 3**

Let’s now connect to the third unit and after the authentication step, let’s go to "Basic Settings" → "Link Settings" menu and let’s do the following configuration in "General Settings" section:

- Enable link: selected
- Type: master (for the BS configuration)
- Polling: On
- Auto Tx Power: selected
- Node name: Node3.

Let's do the following configuration in the "Current Settings" section:

- Channel Width: 10 MHz
- Frequency: 4920 MHz
- Node ID: 3
- Security Key: 11111111.

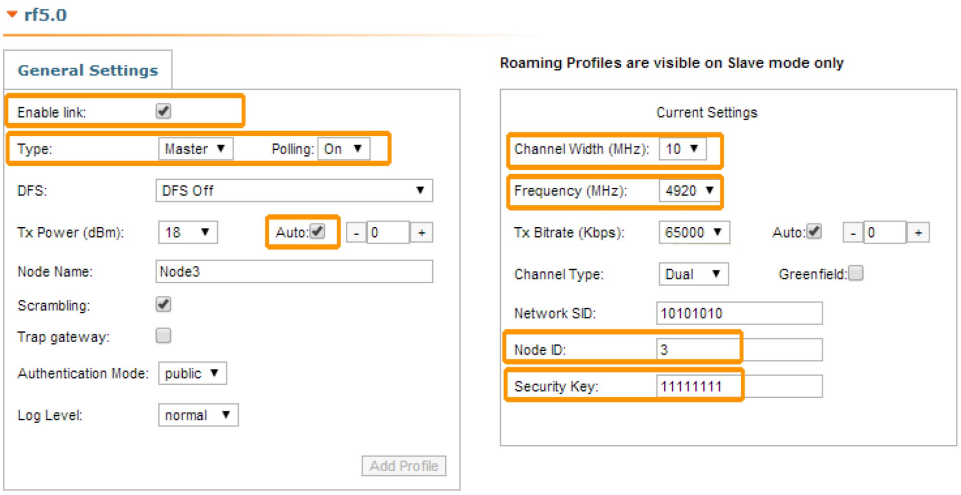


Figure - Second BS radio configuration

Click the «**Apply**» button at the bottom of the page, in order to save the settings performed in the "Link Settings" menu.

We have now two base stations (nodes 1 and 3) configured and one CPE (node 2) with two radio profiles configured: profile 1 has the radio parameters of the BS1 and profile 2 has the radio parameters of the BS2.

We can see now that the CPE can establish a wireless link with any of the two base stations, depending on the link quality.

5.6 Connection to the synchronization unit

The external synchronization unit allows to synchronize the time (the beginning of each second) across multiple devices (up to 7) with an accuracy less than a microsecond, so all the connected units can enable transmitters at the same time. This entirely eliminates mutual interference of the neighboring sectors, when one transmitting unit with its power signal interferes to the neighbor unit to receive weak signal of its customers.

The synchronization unit can be used only for "**H08**" hardware platform**, Omx** and **Mmx** models.

In order to connect to the synchronization unit TDMA firmware version must be installed on InfiNet Wireless R5000 devices.

NOTE

You can download TDMA firmware version via ftp://ftp.infinet.ru/pub/Firmware/beta/TDMA/.

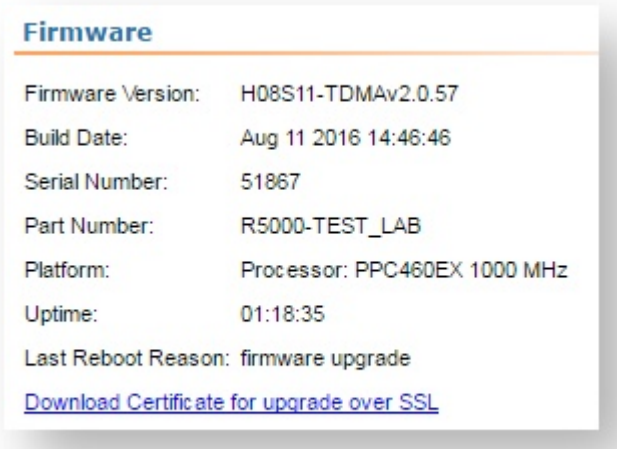


Figure - TDMA firmware version

In order to enable the synchronization mode:

via Web interface:

- Go to the section "Basic Settings" -> "Link Settings" -> "rf5.0"
- Check the box "*Use AUX-ODU-SYNC*"
- Click "**Apply**" button.

via CLI**:**

- Go to the section "Command Line"
- In the field "*Command*" enter the following command

```
tsync enable
```

- Click "**Execute**" button.

CAUTION

The device coordinates are transmitted via the standard NMEA sequences in ASCII code. The false definition of control characters to enter to the boot monitor service mode can occur during synchronization signal receiving since the synchronization unit is connected to the console port of the base station on a non-standard rate.

In order to avoid this, in case the device with:

1) **MINT** firmware:

- Upgrade the device boot monitor via command

```
_upgrade -q
```

NOTE

"*_upgrade -q*" command is available starting with firmware version "*MINTv1.90.17*". It is recommended to install the firmware version not lower than "*MINTv1.90.25"* before the boot monitor upgrade. The command can be executed via a web interface in the section "Command Line".

- Connect the synchronization unit to the device console port.
- Upgrade to **TDMA** firmware version.
- Reboot the device.

2) **TDMA** firmware:

- Make sure you have the latest firmware version and then connect the synchronization unit.
- Otherwise, update the firmware to the latest version and after reboot connect the synchronization unit.

3) Just upgraded from **MINT** to **TDMA** firmware:

- Reboot the device and only after that connect the synchronization unit to the device console port.

In the section "Device Status" -> "Link Statistics" the information about synchronization status and the number of visible satellites is displayed.

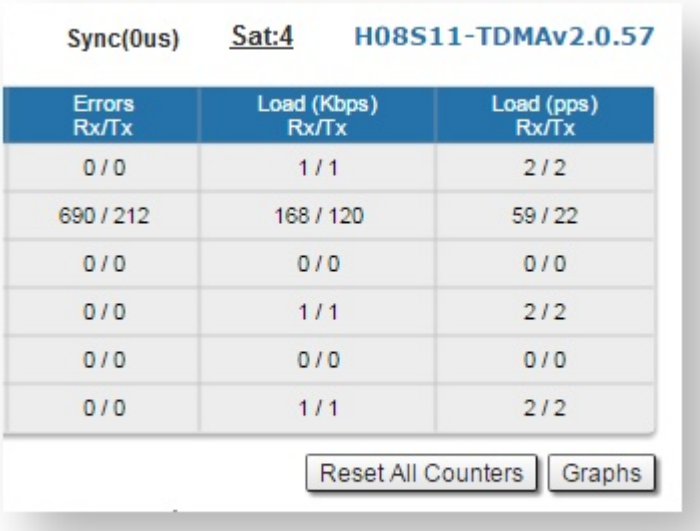


Figure - Sync status with the number of visible satellites

The synchronization mode information can be obtained in the "Command Line" section via command:

```
tsync
```

Time offset histogram is displayed below.

The limiting values of the time offset and jitter are in the bottom of the histogram.

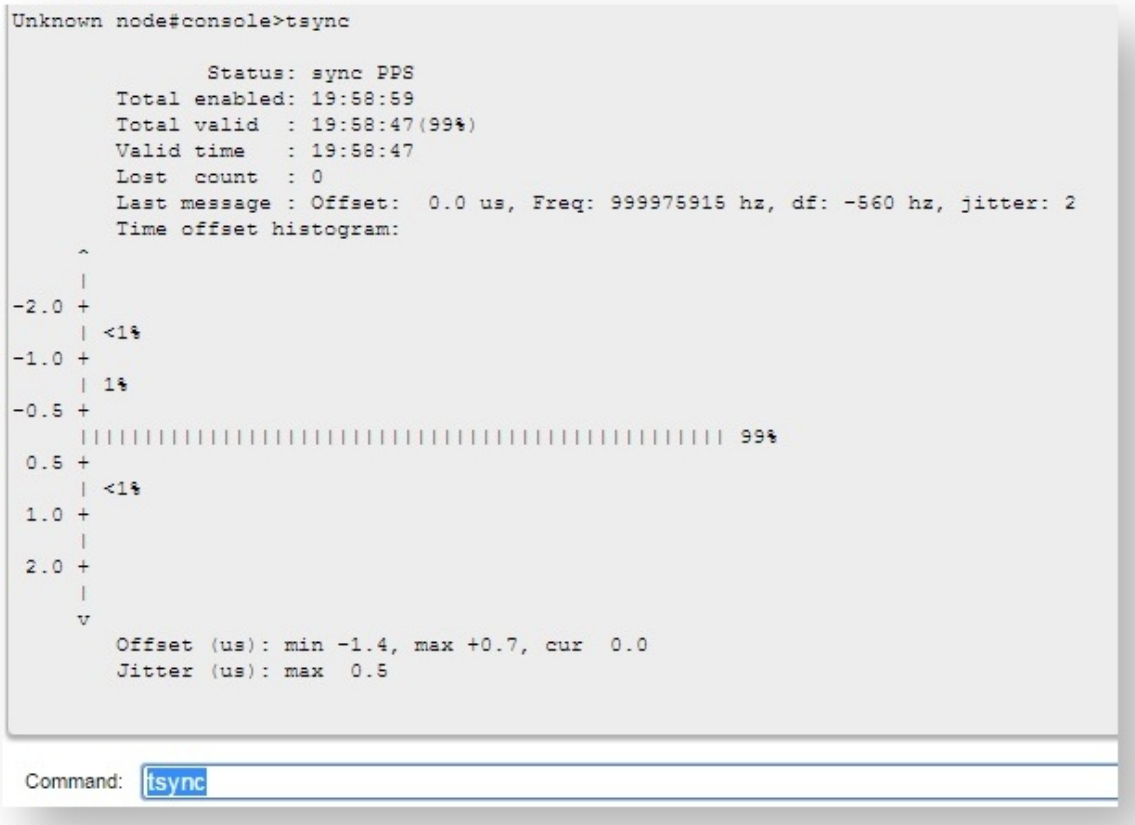


Figure - Time offset histogramm

Parameter	Description
Status	Current device status
Total enabled	Total time during which the synchronizaion unit was enabled
Total valid	Total time during which the timing accuracy was better than 10 microseconds
Valid time	Time during which the timing accuracy was better than 10 microseconds
Last message	Last message from synchronization software

Table - Synchronization mode information

Additionally in order to determine the device coordinates GNSS position can be enabled:

via Web interface:

- Go to the section "Basic Settings" -> "System Settings"
- Check the box "*Use GNSS Position*"
- Click "**Apply**" button.

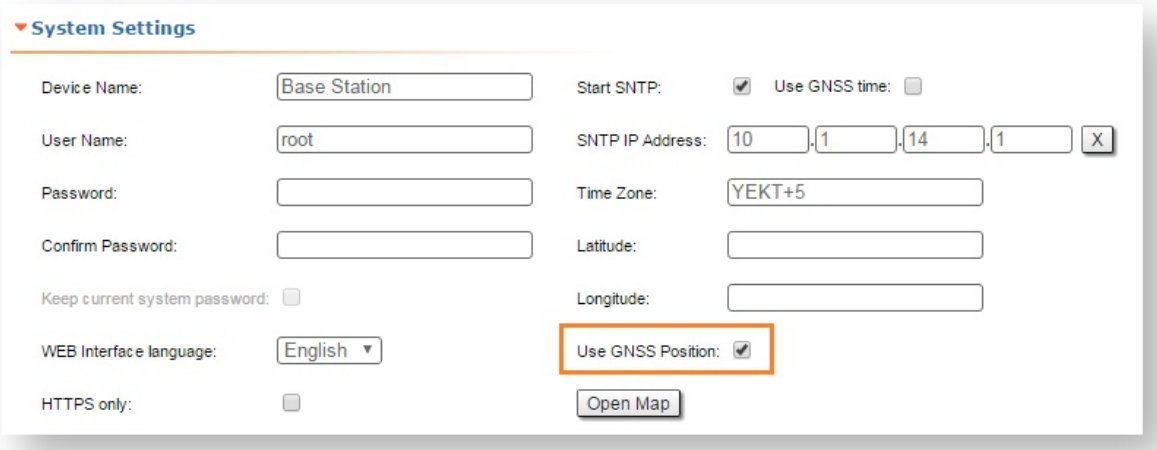


Figure - Use GNSS Position

via CLI**:**

- Go to the section "Command Line"
- In the field "*Command*" enter the command

```
gps start
```

Click "**Open map**" to view the device location.

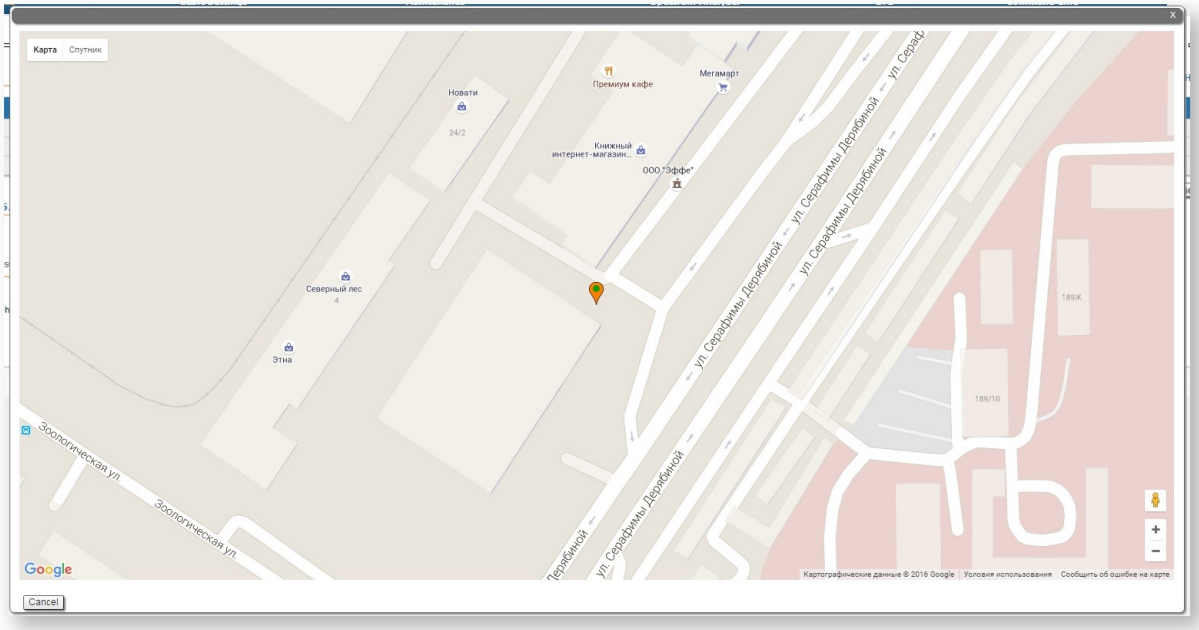


Figure - Device location

The map is updated in real time that allows to monitor the movement of the device mounted on the mobile object.

More detailed GNSS statistic can be obtained via command

```
gps stat
```

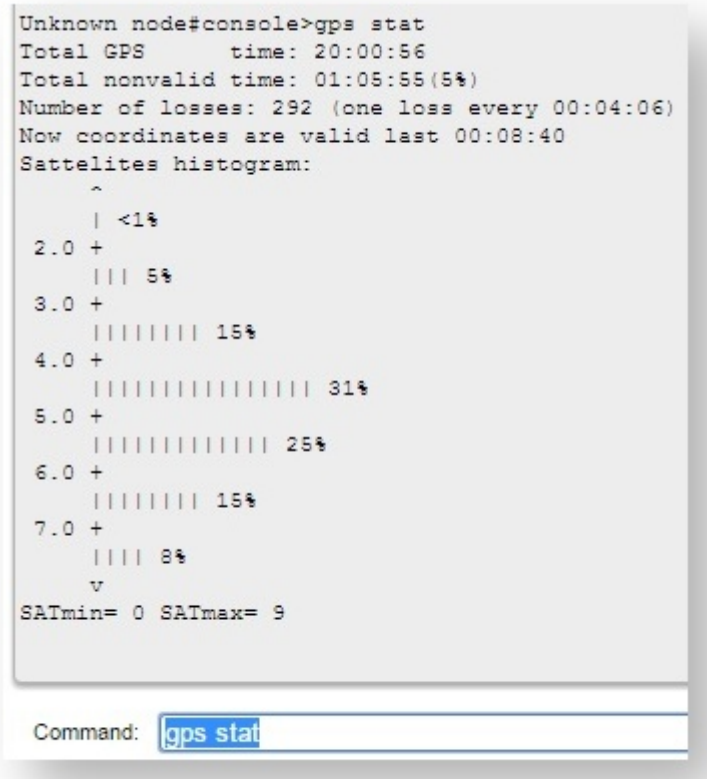


Figure - GNSS statistic

Параметр	Описание
Total GPS time	Total time of GPS operation
Total nonvalid time	Total time during which the information about coordinates was unavailable
Number of losses	Quantity of cases when the information about coordinates had become unavailable
Now coordinates are valid last ...	Time of GPS operation since last coordinates discovering
Sattelites histogram	Histogram of visible satellites quantity
SATmin	Minimum of visible satellites (since the last time you cleared the statistic)
SATmax	Maximum of visible satellites (since the last time you cleared the statistic)

Table - GNSS statistic description

5.7 VLAN configuration

By default **InfiNet Wireless R5000** devices have a single switch group configured. Such configuration allows for unrestricted management access and transparent forwarding of all traffic.

"*config show switch"* command output:

```
#MAC Switch config
switch group 1 add eth0 rf5.0
     # group 1 attached to ‘svi1’
switch group 1 start

switch start
```

Command	Description
switch group GROUP_ID add eth0 rf5.0	▪ Assigns interfaces to a switch group
switch list VLANS_LIST numrange add 10 20	▪ Creates a list of VID, named "*VLANS_LIST*", including VID 10 and 20
switch group GROUP_ID vlan VLANS_LIST	▪ Creates a rule for the switch group “*GROUP_ID*” that only allows VID from "*VLANS_LIST*"
switch group GROUP_ID start	▪ Enables switch group
switch start	▪ Enables switching

Table - Basic VLAN configuration commands

5.7.1 Configuration scenario

This document uses the following network setup:

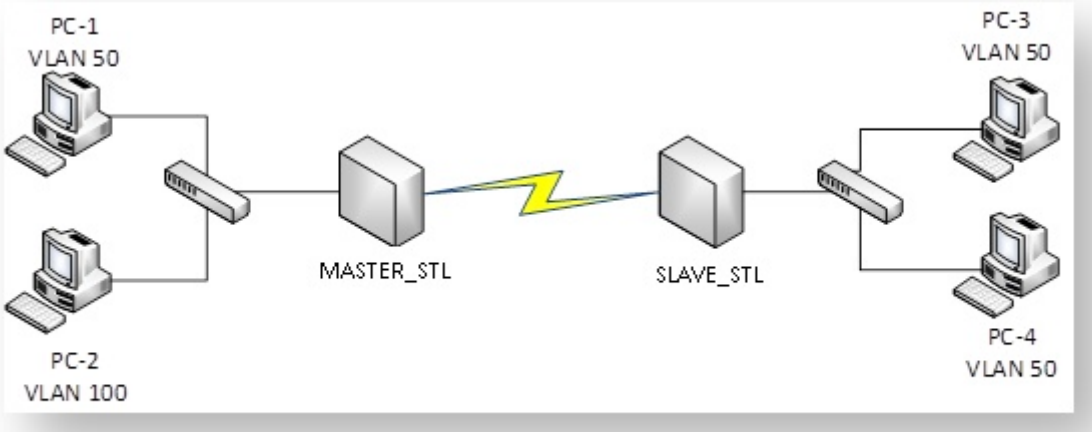


Figure - Connection scheme

- VLAN 100 is a management vlan
- VLAN 50 is a data vlan.

Configuration steps:

- Prepare
- Set up management
- Set up traffic forwarding
- Verify
- View configurations.

Prepare

Make sure the radio link between the devices is up using “*mint map*” command.

NOTE

In case you have difficulties establishing a wireless link, please refer to “Setting up a basic PtP link” for detailed instructions.

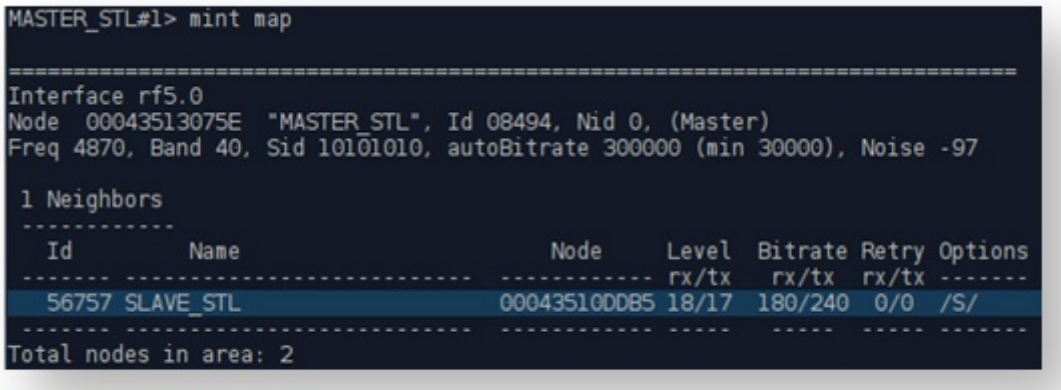


Figure - "mint map" command output

The highlighted string indicates that the radio link between "MASTER_STL" and "SLAVE_STL" devices is active.

Set up management

Configure «*sviX*" and «*vlanX*" interfaces. Refer to «Network Settings» for detailed description.

By default, all **InfiNet Wireless R5000** devices have a management interface “*svi1*” configured. You can change this interface’s parameters, add a new SVI interface, or replace the current interface with a new one.

For the purpose of this article, interface "*svi1*" and switch group 1 will be replaced by the interface "*svi100*" and switch group "*100*".

To set up a new SVI interface and a new switch group issue the following commands:

Command	Description
ifc sviX up	▪ Creates SVI interface. “X” is an interface identifier ranging from 0 to 4095
ifc vlanX vlan Y vlandev eth0 up	▪ Creates “*vlanX*” interface: ○ "*X*" - interface identifier ranging from 0 to 4095 ○ "*Y*" - VID ○ "*eth0*" - physical parent interface
switch group Y add vlanX rf5.0	▪ Assigns interfaces to a switch group
svi X group Y	▪ Assigns "*sviX*" interface to a switch group "*Y"*
sw group 1 remove; ifc svi1 destroy; ifc sviX IP/mask; sw group Y start	▪ All commands entered as a single line separated by “*;*” symbol will be executed sequentially. This feature is used to avoid losing access to the device, when the default management interface is deleted: ○ "*sw group 1 remove*" – removes switch group 1 ○ "*ifc svi1 destroy*" – removes interface "*svi1*" ○ "*ifc sviX IP/mask*" – assigns an IP address and a subnet mask to an interface
config save	▪ Saves the configuration

Command line configuration example:

- MASTER_STL

```
ifc svi100 up
ifc vlan100 vlan 100 vlandev eth0 up
sw group 100 add vlan100 rf5.0
svi 100 group 100
sw group 1 remove; ifc svi1 destroy; ifc svi100 10.10.10.1/24; sw
group 100 start
config save
```

- SLAVE_STL

```
ifc svi100 up
ifc vlan100 vlan 100 vlandev eth0 up
sw group 100 add vlan100 rf5.0
svi 100 group 100
sw group 1 remove; ifc svi1 destroy; ifc svi100 10.10.10.2/24; sw
group 100 start
config save
```

NOTE

In case a switch group has a vlan interface assigned, all traffic with respective VID will be forwarded within this switch group (no need to configure any additional rules). 802.1q tag will be stripped.

For detailed instructions on configuring management via Web GUI please refer to "Remote management of the R5000 units".

Set up traffic forwarding

Configuring data vlan:

Command	Description
switch group GROUP_ID add eth0 rf5.0	▪ Creates a new switch group and assigns interfaces to it
sw group GROUP_ID vlan X	▪ Creates a rule for the switch group "*GROUP_ID*" that only allows VID "*X*" to be forwarded by this switch group
sw group GROUP_ID start	▪ Enables switch group
config save	▪ Saves the configuration

Command line configuration example:

```
sw group 50 add eth0 rf5.0
sw group 50 vlan 50
sw group 50 start
config save
```

NOTE

In order to forward two or more VLANs within a single switch group create a VLAN list and add a respective rule to a switch group:

```
switch list LISTNAME numrange add VALUE
sw group GROUP_ID vlan LISTNAME
```

Example:

```
switch list DATA numrange add 50-99
sw group 50 vlan DATA
```

Verify

After you apply the above configurations only devices from VLAN 100 will be able to access **InfiNet Wireless R5000** management interface.

To verify the operation use «*switch group GROUP_ID dump*».

Example: use «*switch group 50 dump*» to make sure that only frames with VID 50 are being forwarded within switch group 50 and MAC addresses belong to the devices from VLAN 50.

```
MASTER_STL#1> switch group 50 dump
Bridge group 50(normal), READY STARTED  Interfaces : eth0(F) rf5.0(F)
Total records 4
  DST MAC    L   Int.    Gateway MAC  Cost  UsCNT Dead  Vlan
============ = ======== ============ ===== ===== ==== =====
00043503075E * eth0      --    --    --      0     0    0    0
00043513075E * rf5.0     --    --    --      0     0    0    0
7C05071D392F   rf5.0     00043510DDB5      0     0  298   50
3417EB6AEA85   eth0      --    --    --      0     0  182   50
```

```
SLAVE_STL#1> switch group 50 dump
Bridge group 50(normal), READY STARTED  Interfaces : eth0(F) rf5.0(F)
Total records 4
  DST MAC    L   Int.    Gateway MAC  Cost  UsCNT Dead  Vlan
============ = ======== ============ ===== ===== ==== =====
7C05071D392F   eth0      --    --    --      0     0  291   50
00043500DDB5 * eth0      --    --    --      0     0    0    0
00043510DDB5 * rf5.0     --    --    --      0     0    0    0
3417EB6AEA85   rf5.0     00043513075E      0     0  239   50
```

Figure - "switch group 50 dump" command output

The same for the switch group 100:

```
MASTER_STL#1> switch group 100 dump
Bridge group 100(normal), READY STARTED  Interfaces : rf5.0(F) vlan100(F)
Total records 3
  DST MAC    L   Int.    Gateway MAC  Cost  UsCNT Dead  Vlan
============ = ======== ============ ===== ===== ==== =====
00043503075E * vlan100   --    --    --      0     0    0    0
00043513075E * rf5.0     --    --    --      0     0    0    0
7C05071D392F   rf5.0     00043510DDB5      0   136  300    0
```

```
SLAVE_STL#1> switch group 100 dump
Bridge group 100(normal), READY STARTED  Interfaces : rf5.0(F) vlan100(F)
Total records 4
  DST MAC    L   Int.    Gateway MAC  Cost  UsCNT Dead  Vlan
============ = ======== ============ ===== ===== ==== =====
02043503075E   rf5.0    00043513075E     0     1  257    0
7C05071D392F   vlan100  --    --   --     0   143  300    0
00043500DDB5 * vlan100  --    --   --     0     0    0    0
00043510DDB5 * rf5.0    --    --   --     0     0    0    0
```

Figure - "switch group 100 dump" command output

The displayed VIDs in the “Vlan” are “0” because the 802.1q tag “100” was stripped by the vlan interface.

View configurations

Use “config show” command to view and verify the configurations:

- MASTER_STL

```
#System parameters
#Factory password mode: single
sys name MASTER_STL
sys prompt MASTER_STL
sys user root
setpass

#Radio module parameters
rf rf5.0 band 40
rf rf5.0 mimo greenfield
rf rf5.0 freq 4870 bitr 300000 sid 10101010 burst
rf rf5.0 txpwr 10 pwrctl distance 1

#DFS configuration
dfs rf5.0 dfsoff
dfs rf5.0 freq auto
dfs rf5.0 cot off

#Interfaces parameters
ifc lo0 127.0.0.1/32
ifc eth0 media auto mtu 1500 up
ifc rf5.0 mtu 1500 up
ifc svi100 mtu 1500 up
        # group 100
ifc svi100 10.10.10.1/24
ifc vlan100 mtu 1500 up
ifc vlan100 vlan 100 vlandev eth0
```

```
#QoS manager
qm option rtp dot1p notos icmp notcpack nostrict

#MINT configuration
mint rf5.0 -name "MASTER_STL"
mint rf5.0 -nodeid 08494
mint rf5.0 -type master
mint rf5.0 -mode fixed
mint rf5.0 -scrambling
mint rf5.0 -autobitrate
mint rf5.0 -minbitrate 30000
mint rf5.0 -hiamp 2 -loamp 0
mint rf5.0 -log
mint rf5.0 -roaming disable
mint rf5.0 -authmode public
mint rf5.0 -airupdate passive normal
mint rf5.0 -rcmdserver enabled
mint rf5.0 poll start
mint rf5.0 start

#MAC Switch config
switch group 100 add 1 rf5.0 vlan100
      # group 100 attached to 'svi100'
switch group 100 start

switch group 50 add 2 eth0 rf5.0
switch group 50 vlan 50
switch group 50 start

switch start

#Switch Virtual Interface config
svi 100 group 100

#WEB configurator
webcfg start

#LLDP parameters
 lldp eth0 enable txrx
```

- SLAVE_STL

```
#System parameters
#Factory password mode: single
sys name SLAVE_STL
sys prompt SLAVE_STL
sys user root
setpass
```

```
#Radio module parameters
rf rf5.0 band 40
rf rf5.0 mimo greenfield
rf rf5.0 freq 4870 bitr 300000 sid 10101010 burst
rf rf5.0 txpwr 10 pwrctl distance 1

#DFS configuration
dfs rf5.0 dfsoff
dfs rf5.0 freq auto
dfs rf5.0 cot off

#Interfaces parameters
ifc lo0 127.0.0.1/32
ifc eth0 media auto mtu 1500 up
ifc rf5.0 mtu 1500 up
ifc svi100 mtu 1500 up
        # group 100
ifc svi100 10.10.10.2/24
ifc vlan100 mtu 1500 up
ifc vlan100 vlan 100 vlandev eth0

#QoS manager
qm option rtp dot1p notos icmp notcpack nostrict

#MINT configuration
mint rf5.0 -name "SLAVE_STL"
mint rf5.0 -nodeid 56757
mint rf5.0 -type slave
mint rf5.0 -mode fixed
mint rf5.0 -scrambling
mint rf5.0 -autobitrate
mint rf5.0 -minbitrate 30000
mint rf5.0 -hiamp 2 -loamp 0
mint rf5.0 -log
mint rf5.0 -roaming disable
mint rf5.0 -authmode public
mint rf5.0 -airupdate passive normal
mint rf5.0 -rcmdserver enabled
mint rf5.0 start

#MAC Switch config
switch group 100 add 1 rf5.0 vlan100
     # group 100 attached to 'svi100'
switch group 100 start
switch group 50 add 3 eth0 rf5.0
switch group 50 vlan 50
switch group 50 start

switch start
```

```
#Switch Virtual Interface config
svi 100 group 100

#WEB configurator
webcfg start

#Add-on devices control
ctl heater -8

#LLDP parameters
 lldp eth0 enable txrx
```