InfiLINK Evolution / InfiMAN Evolution product families were designed thanks to a combination of innovative technology, high reliability and the advanced functionality of the field-proven InfiLINK 2x2 and InfiMAN 2x2 families. **InfiLINK Evolution / InfiMAN Evolution** wireless solutions are ideal for deployment in Point-to-Point and Point-to-Multipoint network topologies, especially to ensure seamless connection of nomadic and mobile units to central office.

The new base station provides a sector capacity of up to 800 Mbps, enabling wireless operators of all sizes to not only deploy new infrastructures but also to extend the capacity of their existing networks. **InfiLINK Evolution / InfiMAN Evolution** devices have full backward compatibility with previous generation of InfiLINK 2x2 and InfiMAN 2x2 families wireless systems.

1 About This Manual

This manual provides detailed technical information for the **InfiLINK Evolution / InfiMAN Evolution** families devices, including system specifications, installation, commissioning, maintenance and troubleshooting.

The document is intended to be used by qualified RF engineers/technicians and IT professionals. Qualified personnel should have skills and experience with:

- Outdoor/indoor radio equipment installation
- Outdoor wireless networks
- TCP/IP networking protocols
- Safety procedures and instructions for installing antenna equipment
- Professional manipulation with electrical equipment and accessories
- Safety procedures and instructions for working at height.

2 Important Notice

2.1 Legal Rights

The information contained in this document is originated by, proprietary, confidential and owned by Infinet Wireless. No part of this document should be disclosed, reproduced or distributed without the express written permission of Infinet Wireless Ltd.

Infinet Wireless Ltd. reserves the right to change the information contained in this document without prior notice. No part of this document may be considered as a part of any contract or warranty.

2.2 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.

2.3 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.

2.4 Indication of the countries

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

2.5 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).

2.6 Disposal instructions

This symbol means that this product is subject to Waste of electrical and electronic equipment (WEEE) regulations. Do not dispose of your product with other regular/household waste. Instead, hand over your waste equipment to a designated collection point for recycling.

2.7 Compliance Information

This equipment has been tested and found to comply with the limits for a Class B digital device[1], pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference[2] in a residential installation. This equipment generates, uses and can radiate radio frequency energy[3] and, if not installed and used in accordance with the instructions, may cause harmful interference[4] to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference[5] to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator&human body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

In accordance FCC 15.21, changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

[1] https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=cccf00e7a4dc5e6289fe4d5da8d952d7&term_occur=999&term_src=Title:47:Chapter:I:Subchapter:A:Part:15:Subpart:B:15.105

[2] https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=5d78fa6c752a5326f26a026c51cd5136&term_occur=999&term_src=Title:47:Chapter:I:Subchapter:A:Part:15:Subpart:B:15.105

[3] https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=c3872b7fd20c05e83d69f0a8b42cd86e&term_occur=999&term_src=Title:47:Chapter:I:Subchapter:A:Part:15:Subpart:B:15.105

[4] https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=5d78fa6c752a5326f26a026c51cd5136&term_occur=999&term_src=Title:47:Chapter:I:Subchapter:A:Part:15:Subpart:B:15.105

[5] https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=5d78fa6c752a5326f26a026c51cd5136&term_occur=999&term_src=Title:47:Chapter:I:Subchapter:A:Part:15:Subpart:B:15.105

3 Introduction

3.1 Document structure

This document consists of the following chapters:

- Introduction - presents the information about this document's purpose and structure.
- Planning considerations - describes the principles of wireless system planning.
- Installation - describes the steps to be taken when installing the equipment at the installation sites and installation site requirements.
- Operation & Administration - presents the functionalities of the web interface, a simple and efficient way to monitor the device status, configure and maintain the equipment.
- Troubleshooting - describes the actions to be taken during occured problems investigation.

3.2 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.

3.3 Key Features

InfiLINK Evolution is a wireless point-to-point solution with an impressive maximal performance of up to 670 Mbps, InfiMAN Evolution is a wireless point-to-multipoint solution with an impressive maximal performance of up to 800 Mbps. It operates in 5 and 6 GHz frequency ranges: from 4900 to 6425 MHz and supports the channel width 20, 40, 80 MHz with exception for models E5-BSI-L and E5-BSE-L that support 20 and 40 MHz.

Base Stations can be used with:

- a dual polarization integrated antenna with an antenna gain 16 dBi and 21 dBi;
- an external antenna connected to two N-type ports using low-loss RF cables.

Subscriber terminals and PTP devices can be used with:

- a dual polarization integrated antenna with an antenna gain 18 dBi, 23 dBi, 25 dBi and 28 dBi;
- an external antenna connected to two N-type ports using low-loss RF cables.

and operates in LOS and non-LOS conditions. OFDM radio technology is used for data transmission.

3.3.1 Radio

- **Automatic Modulation Control (AMC)** – modulation control algorithm selects the most appropriate modulation-coding scheme in order to maximize the link performance.

- **Automatic Repeat Request (ARQ)** – a technology which enables packet re-transmission in case of previous unsuccessful delivery, allows to achieve reliable connectivity even in highly congested spectrum.
- **Automatic Transmit Power Control (ATPC)** – a technology which allows to extend the life of devices and optimize energy consumption.
- **Automatic range detection** - the guard interval optimal for the actual distance is automatically determined.

3.3.2 Networking

- MAC/IP filtering.
- RIPv2 / OSPFv2 /static routing.
- Tunneling (Ethernet-over-IP, IP-over-IP).
- L2/L3 Firewall.
- NAT (multipool, H.323-aware).
- DHCP client/server/relay.
- Stacked VLAN support (Q-in-Q) avoids the limitation in the number of available VLANs (4096), which can be useful for large networks. In addition, Q-in-Q allows you to organize L2 channels within a limited VLAN list, which is widely used in provider networks and on leased communication channels.

3.3.3 Quality of Service

- 17 priority queues.
- IEEE 802.1p support.
- IP TOS / DiffServ support.
- Full voice support.
- Traffic limiting (absolute, relative, mixed).
- Traffic redirection.

3.3.4 Environment

- Operating temperature range -40 ... +60 °C.
- Dust and water protection in compliance with IP66/IP67.
- Wind load up to 160 kph - operation, 200 kph - survival.

3.3.5 Power

The device has following electrical parameters:

- Consumption is up to 30 W for base station sectors and up to 15 W for subscriber terminals.
- Power options: 90-240 VAC~ @ 50/60 Hz, ±43..56 VDC.
- 802.3at support or Infinet Wireless proprietary passive PoE.
- AC/DC injector:
  - IDU-BS-G(60W) is included to the packing list of base station sectors.
  - IDU-CPE-G(24W) is included to the packing list of subscriber terminals.

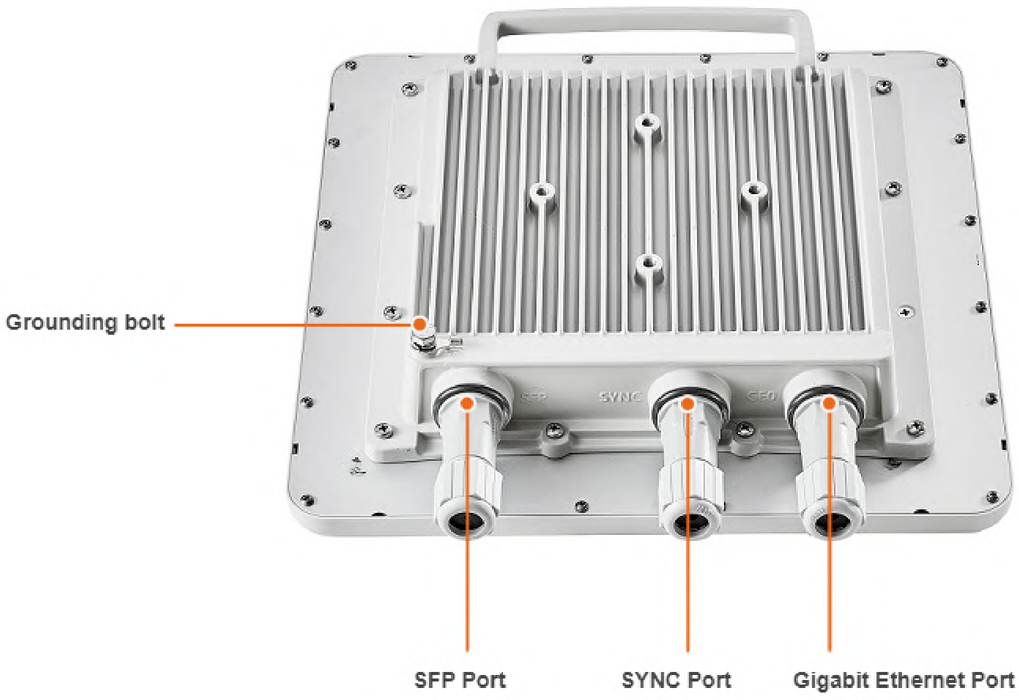
3.4 Hardware Platform

3.4.1 Wireless device

The wireless device contains both the radio and networking electronics. Implemented in a robust all-weather metal enclosure, this equipment can be used to create point-to-point and point-to-multipoint wireless links at long distances. The wireless device is supplied in the following configurations:

Base Station Sectors

- with integrated antenna 16 dBi (E5-BSI, E6-BSI);
- with integrated antenna 21 dBi (E5-BSQ);
- with two N-type ports for an external antenna (E5-BSE, E6-BSE).



Base Station Sectors Interfaces

Base station sectors have ports:

- 1x Gigabit Ethernet port (10/100/1000 Base-T), RJ-45 connector: Data + Power.
- 1x SFP port: Data.
- 1x SYNC port for AUX-ODU-SYNC connection.

Interface	Description

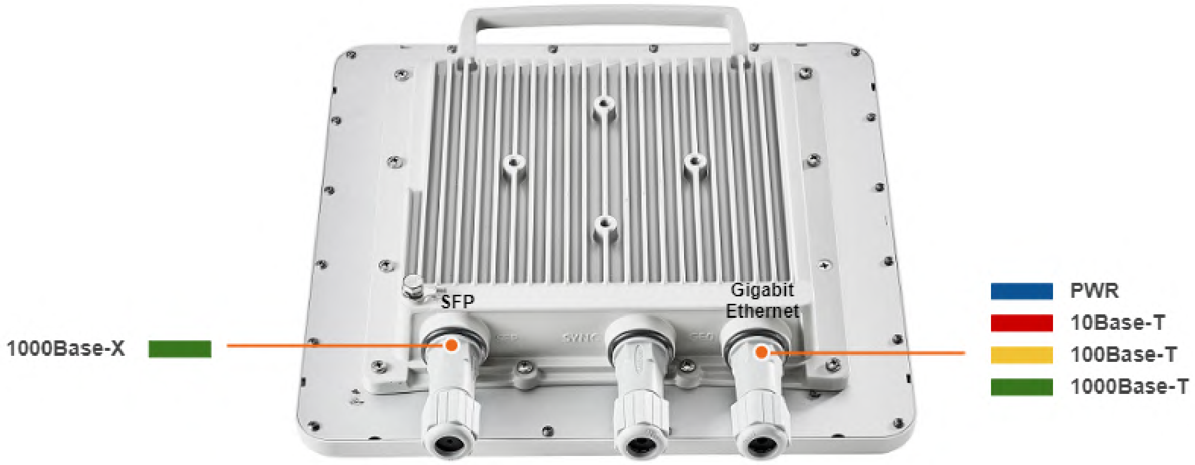
Gigabit Ethernet	RJ-45 socket for connecting to power supply and data transmission. The network connection to the wireless device is made via a 1000Base-T (Gigabit) Ethernet connection. Power is provided to the device over the 1000Base-T Ethernet connection using a standard IEEE 802.3at passive PoE power supply.
SFP	External optical Gigabit port for plugging of the optical SFP transceiver module.
SYNC	RJ-45 socket for connecting to synchronization unit AUX-ODU-SYNC.

LEDs

> ⚠ **NOTE**
>
> Power and wired statuses indication is performed via glassy plug of the cable gland.

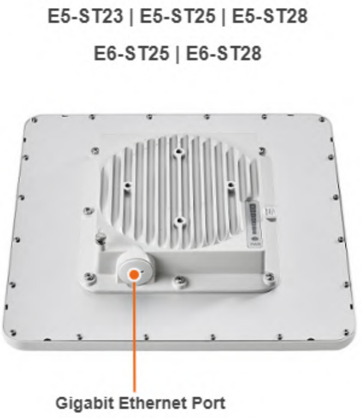
LED	State	Status	Description
Gigabit Ethernet **SFP**	Flash	Initialization	The LEDs on both ports light up with white on second. Then LEDs check is performed: red, blue, green are lightened up sequentially.
	Flash	Loading	Only for Gigabit Ethernet port: at the beginning green is lightened a few seconds, on the second loading stage switches to blue.
	ON/Blue	Power	Only for Gigabit Ethernet port.
	ON/Red	Speed 10 Mbps	Only for Gigabit Ethernet port.
	ON/Yellow	Speed 100 Mbps	Only for Gigabit Ethernet port.
	ON/Green	Speed 1000 Mbps	

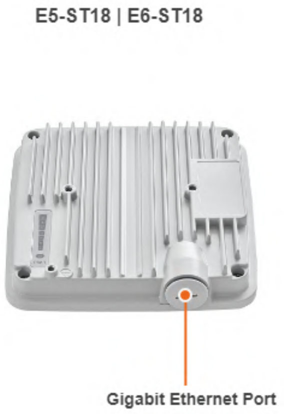
	ON/Green	ERConsole stage	Port with the established link lights up with green, the second port remains blue.

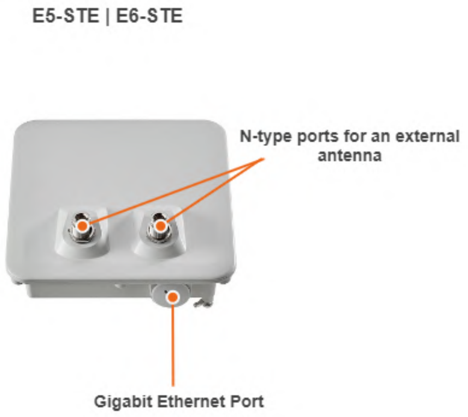


Subscriber Terminals and point-to-point devices

- with integrated antenna 18 dBi;
- with integrated antenna 23 dBi;
- with integrated antenna 25 dBi;
- with integrated antenna 28 dBi;
- with two N-type ports for an external antenna.





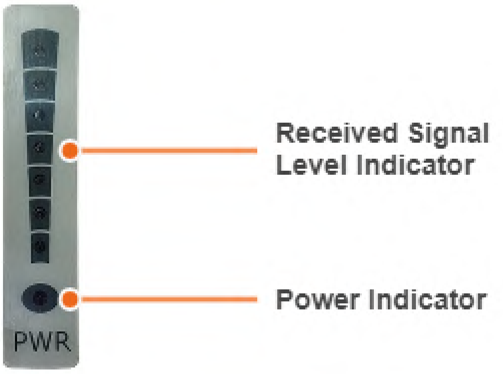


Subscriber Terminals and PTP devices Interfaces

RJ-45 socket for connecting to power supply and network via the PoE power supply. The network connection to the ODU is made via a 1000Base-T (Gigabit) Ethernet connection. Power is provided to the ODU over the 1000Base-T Ethernet connection using a standard IEEE 802.3at passive PoE power supply.

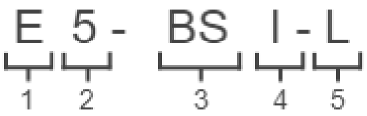
LED Panel

PWR - power indicators will light red when the device is connected to a power source, yellow when 10/100 Mbps wired connection appears and green when 1000 Mbps wired connection appears. Other indicators are used to perform coarse antenna alignment. The more indicators are on, the better wireless connection is established. The blinking indicator means an intermediate state. The more often the indicator blinks the higher level connection is established.



3.4.2 Part number description

InfiLINK Evolution / **InfiMAN Evolution** part number has the following structure



Structure items are described below

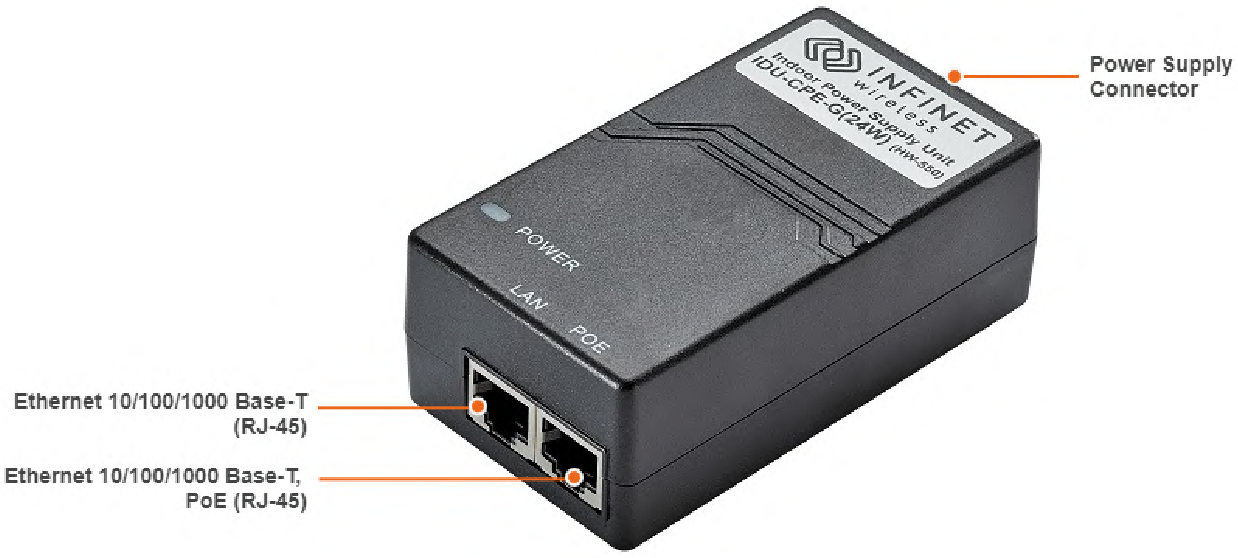
Item	Description
1	Product family name: • **E** - InfiLINK Evolution / InfiMAN Evolution.
2	Frequency range: • **5** - device in the range of 5 GHz. • **6** • base station sector in the range of 6 GHz . • subscriber terminal in the ranges of 5 and 6 GHz.

3	• **BS** - base station sector. • **ST** - subscriber terminal or PTP device.
4	Antenna gain. Base Station Sectors: • **I** - integrated antenna with 16 dBi gain; • **Q** - integrated antenna with 21 dBi gain; • **E** - devices for an external antenna connection. Subscriber Terminals and PTP devices: • **18** - integrated antenna with 18 dBi gain; • **23** - integrated antenna with 23 dBi gain; • **25** - integrated antenna with 25 dBi gain; • **28** - integrated antenna with 28 dBi gain; • **E** - devices for an external antenna connection.
5	Base Btation Sectors version • **L** - lite version with limited functionality: • Throughput: up to 360 Mbps. • Channel width: 20, 40 MHz. • Maximum number of simultaneous subscribers supported: 10.

3.5 Power supply

- Indoor AC/DC injector IDU-CPE-G(24W)(see page 11)
- Indoor AC/DC injector with integrated lightning protection IDU-BS-G(60W)(see page 13)
- Indoor DC/DC injector for all InfiNet Wireless' units with integrated lightning protection IDU-LA-G(V.01)(see page 15)
- Lightning Protection Unit with Injector AUX-ODU-INJ-G(see page 18)

3.5.1 Indoor AC/DC injector IDU-CPE-G(24W)



1 Figure - IDU-CPE-G(24W)

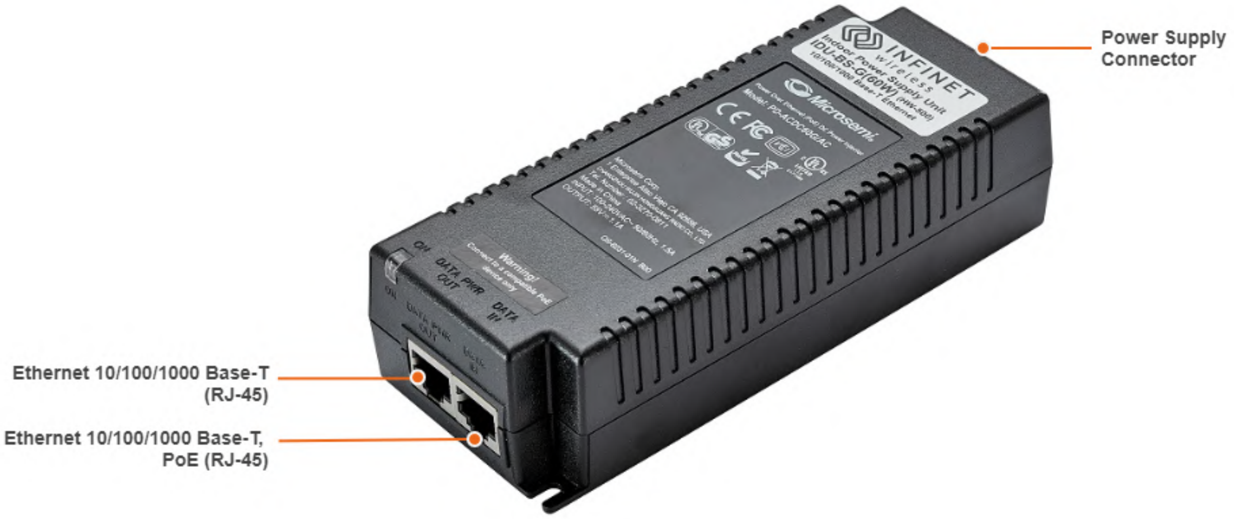
IDU-CPE-G(24W) is an indoor Gigabit PoE injector which supports 100-240 V input range from the AC mains. IDU-CPE-G(24W) feeds 48 VDC power to the device by injecting it to the CAT5 Ethernet cable.

Parameter	Description
Compatible models	Quanta 5, Quanta 6, Quanta 70, InfiLINK 2x2 LITE, InfiMAN 2x2 STE, InfiMAN Evolution STE, InfiLINK Evolution, AUX-ODU-SYNC
Size and weight	97*53.5*33.5 mm, 0.133 kg
Connectors and Interfaces	• "LAN" - Ethernet input (Data only) • "POE" - Ethernet output (Data+VDC), PASSIVE PoE • "PWR" - AC Input
Supported Ethernet Modes	• 10/100/1000 Mbps
Standards	• IEEE 802.3 10Base-T • IEEE 802.3U 100Base-TX • IEEE 802.3ab 1000Base-T
Input Power Requirements	• AC Input Voltage: 100 ... 240 VAC • AC Input Current: 0.75 A • AC Frequency: 50 to 60 Hz
Consumption	• 28 W

<table>
<tr><th>Parameter</th><th colspan="10">Description</th></tr>
<tr><td><b>Operating temperature range</b></td><td colspan="10">• -10 °C ... +40 °C</td></tr>
<tr><td><b>Operating humidity</b></td><td colspan="10">• Maximum 95 %, Non-condensing</td></tr>
<tr><td><b>Storage temperature</b></td><td colspan="10">• -40 °C ... +70 °C</td></tr>
<tr><td><b>Output Power Voltage</b></td><td colspan="10">• 48 VDC, 0.5 A</td></tr>
<tr><td rowspan="4"><b>Ethernet Connectors Pin-out</b></td><td rowspan="2"><b>LAN</b></td><td><b>Pin</b></td><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td><td><b>5</b></td><td><b>6</b></td><td><b>7</b></td><td><b>8</b></td></tr>
<tr><td><b>Description</b></td><td>A+</td><td>A-</td><td>B+</td><td>C+</td><td>C-</td><td>B-</td><td>D+</td><td>D-</td></tr>
<tr><td rowspan="2"><b>POE</b></td><td><b>Pin</b></td><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td><td><b>5</b></td><td><b>6</b></td><td><b>7</b></td><td><b>8</b></td></tr>
<tr><td><b>Description</b></td><td>A+</td><td>A-</td><td>B+</td><td>+VDC / C+</td><td>+VDC / C-</td><td>B-</td><td>-VDC / D+</td><td>-VDC / D-</td></tr>
<tr><td><b>Safety</b></td><td colspan="10">• UL cUL, CE, GS, CCC, FCC, S-MARK, PSE, C-tick, KC(48V0.5A) BIS（24V1A）</td></tr>
</table>

1 Table - IDU-CPE-G(24W) Specification

3.5.2 Indoor AC/DC injector with integrated lightning protection IDU-BS-G(60W)


Power Supply Connector
Ethernet 10/100/1000 Base-T (RJ-45)
Ethernet 10/100/1000 Base-T, PoE (RJ-45)

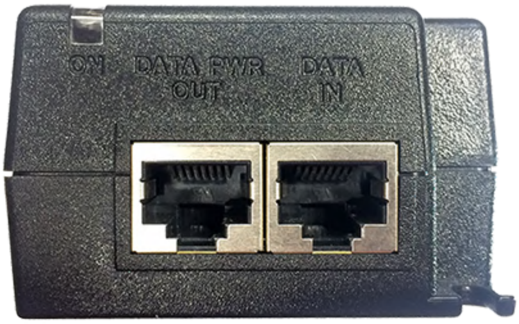
2 Figure - IDU-BS-G(60W)

IDU-BS-G(60W) is an indoor AC/DC PoE injector with built-in lightning protection. PoE injector is powered by an AC supply in the 100-240 V range.

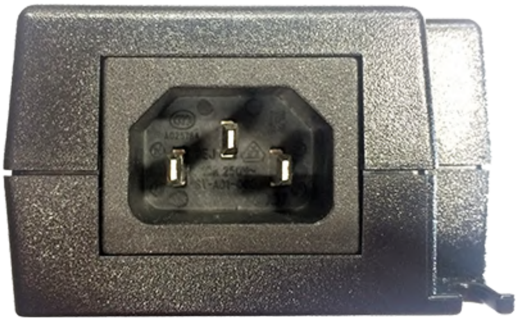
Parameter	**Description**
Compatible models	InfiLINK XG, InfiLINK XG 1000, InfiLINK 2x2 PRO, InfiMAN 2x2 BS, Quanta 70, Quanta 5, Quanta 6, InfiMAN Evolution BS
Size	151*62*38 mm (L*W*H)
Weight	0.32 kg
Connectors and Interfaces	• "ETH IN" - Ethernet input (Data only) • "ETH OUT" - Ethernet output (Data+VDC), PASSIVE PoE • "PWR" - AC Input
Supported Ethernet Modes	• 10/100/1000Mbps (Gigabit Ethernet pass-through)
Input Voltage	• 100 ... 240 V
Output Voltage & Current	• +55 V, 1.5 A
Consumption	• 60 W over 4-pairs (Guaranteed)
Operating temperature range	• -10 °C ... +40 °C
Pin Assignment and Polarity	• Data Pairs 1/2 (-) and 3/6 (+) • Spare Pairs 7/8 (-) and 4/5 (+)

Parameter	Description
EMC	Meet: • FCC Part 15, Class B • EN 55022 Class B (Emissions) • EN 55024 (Immunity), VCCI
Lightning Protection	In compliance with: • IEC 61000-4-2 (ESD) 15kV (air), 8kV (contact) • IEC 61000-4-4 (EFT) 40A (tp = 5/50ns) • IEC 61000-4-5 (Lightning) L5, 95A (tp = 8/20us)

2 Table - IDU-BS-G(60W) Specification



3 Figure - IDU-BS-G(60W) Front Panel



4 Figure - IDU-BS-G(60W) Rear Panel

3.5.3 Indoor DC/DC injector for all InfiNet Wireless' units with integrated lightning protection IDU-LA-G(V.01)

IDU-LA-G(V.01) is an indoor DC/DC injector. It greatly reduces complexity of the deployment in the cases where DC source is available thus reducing both capital expenditures and total cost of ownership.

IDU-LA-G(V.01) may be used for the following purposes:

- To serve as a line protection unit for indoor network equipment connected to the second Ethernet port on ODU.
- To connect third-party DC power sources to ODU (for example, to power the unit from solar power or wind power sources).

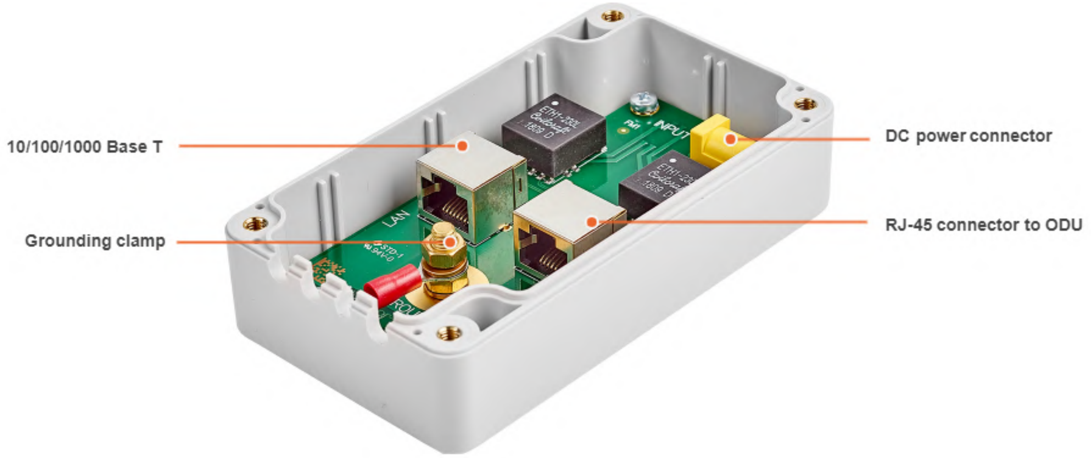
Technical parameters

Parameter	Description
Compatible models	InfiLINK XG, InfiLINK XG 1000, InfiLINK 2x2, InfiMAN 2x2, Quanta 5, Quanta 6, Quanta 70, InfiLINK Evolution, InfiMAN Evolution
Output Voltage	The same as input
Supported Ethernet Modes	10/100/1000 Mbps (Gigabit Ethernet pass-through)
Pin assignment and polarity	1/2 (+), 3/6 (-), 4/5 (+), 7/8 (-)
DC Range	Acceptable input DC range depends on the specific ODU model: • InfiLINK XG, InfiLINK XG 1000, InfiLINK 2x2 PRO, InfiMAN 2x2 BS, Quanta 70, Quanta 5, Quanta 6, InfiLINK Evolution, InfiMAN Evolution models: ±43... ±56 VDC • InfiLINK 2x2 Lite, InfiMAN 2x2 STE models: +9... +56 VDC (positive voltage only)
Size and Weight	115×65×40 mm, 0.15 kg
Operating temperature range	from 0°C to +40°C

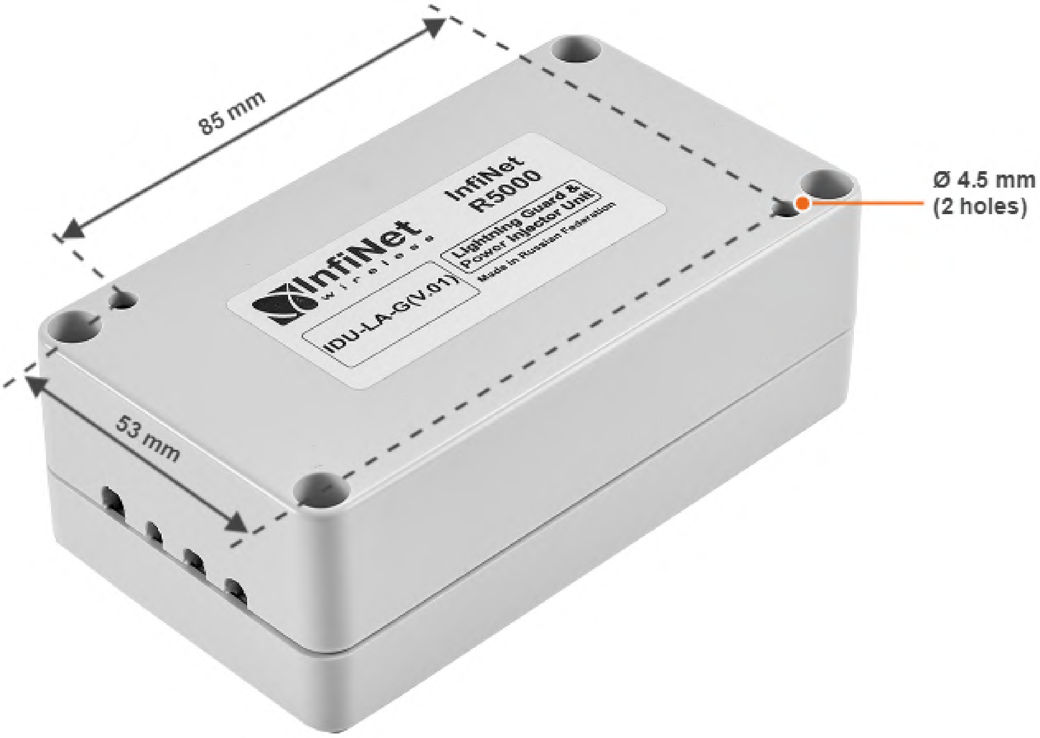
CAUTION

Exposing unit to the unsupported voltage will result in irreparable damage to the unit! Always observe power requirements!

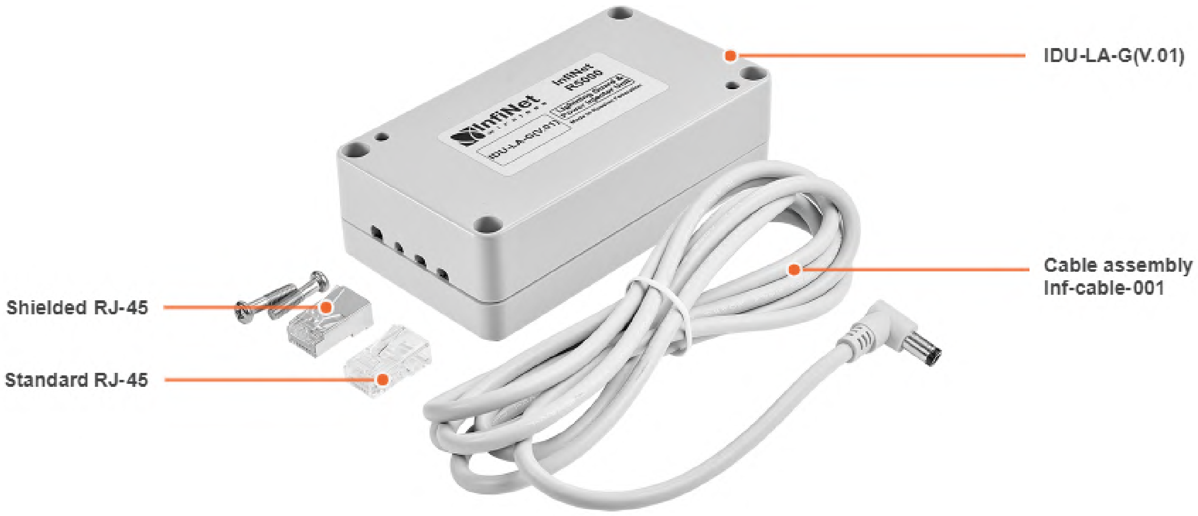
Connectors description



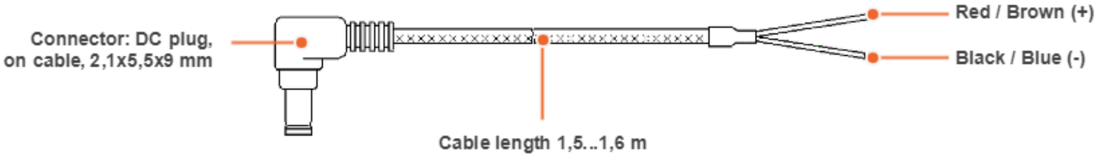
Mounting holes sizes



IDU-LA-G(V.01) Packing List



Cable assembly



3.5.4 Lightning Protection Unit with Injector AUX-ODU-INJ-G

PWR
ETH IN
GND
ETH OUT
Power over Ethernet DC Injector
! WARNING THIS UNIT MUST BE GROUNDED

5 Figure - AUX-ODU-INJ-G

Optional indoor/outdoor DC injector with built-in lightning protection. It greatly reduces complexity of the deployment in the cases where DC source is available on the rooftop eliminating the need of weather-sealed cabinets. AUX-ODU-INJ-G is compatible with all Infinet Wireless devices.

Parameter	Description
Size and Weight	34x94x121 mm, 0.28 kg
Connectors and Interfaces	• ETH IN - Ethernet input • ETH OUT - Ethernet output (data+VDC, protected leg) • PWR - DC Input • GND - Ground clamp
Supported Ethernet Modes	• 10/100/1000 Mbps (Gigabit Ethernet pass-through)
Water and Dust Protection	• IP66 and IP67
Operating temperature range	• -55 °C ... +60 °C
DC Range	• InfiLINK XG, InfiLINK XG 1000, InfiLINK 2x2 PRO, InfiMAN 2x2 BS, Quanta 70, Quanta 5, Quanta 6, InfiLINK Evolution, InfiMAN Evolution: ±43...±56 VDC • InfiLINK 2x2 Lite, InfiMAN 2x2 STE: +9... +56 VDC (positive voltage only)

CAUTION

Using inappropriate DC source will damage the ODU, which will be not covered by warranty

Ethernet Connectors Pin-out	**ETH IN**	**Pin**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
		Description	Data pair A+	Data pair A-	Data pair B+	Data pair C-	Data pair C+	Data pair B-	Data pair D+	Data pair D-
	ETH OUT	**Pin**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
		Description	Data pair A+	Data pair A-	Data pair B+	+VDC + Data pair C-	+VDC + Data pair C+	Data pair B-	-VDC + Data pair D+	-VDC + Data pair D-

Parameter	Description
Lightning Protection	In compliance with: • GR-1089 • IEC 61000-4-2 (ESD) 15kV (air), 8kV (contact) • IEC 61000-4-4 (EFT) 40A (tp = 5/50ns) • IEC 61000-4-5 (Lightning) L5, 95A (tp = 8/20us) • ETSI ETS 300 386

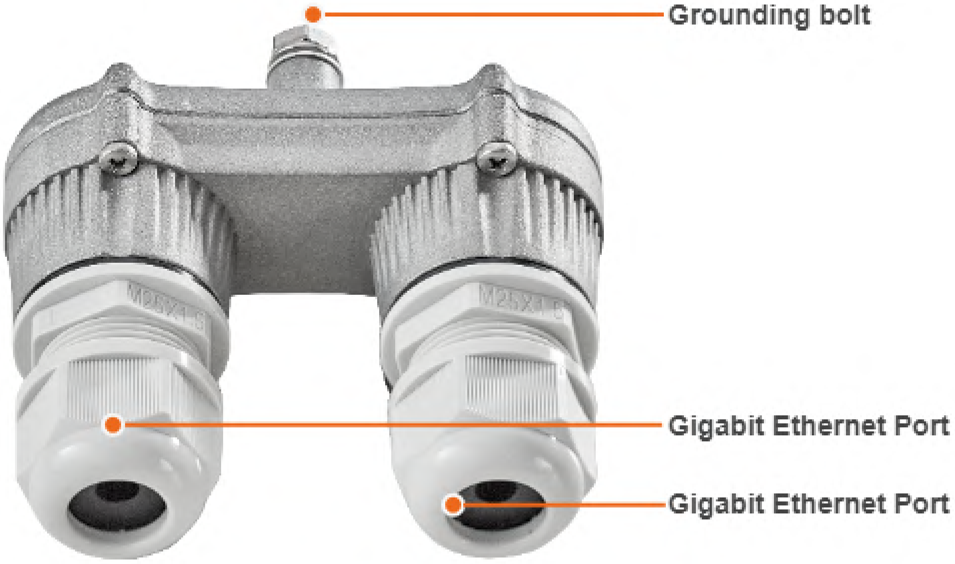
3 Table - AUX-ODU-INJ-G Specifications

Packing List

3.6 Lightning protection unit

- AUX-ODU-LPU-L(see page 20)
- AUX-ODU-LPU-G(see page 22)

3.6.1 AUX-ODU-LPU-L



6 Figure - AUX-ODU-LPU-L

AUX-ODU-LPU-L is a bidirectional external outdoor lightning protection unit for Infinet Wireless systems designed to withstand the toughest conditions and protect the outdoor unit or the 3rd party networking equipment installed indoors from sudden power surges induced by lightning strikes. Despite the fact every Infinet wireless device has a built-in lightning protection. AUX-ODU-LPU-L, thanks to its superior GR-1089-grade protection, greatly reduces the risk of damage for the systems operating in harsh environments or difficult-to-reach locations. AUX-ODU-LPU-L is compatible with all Infinet Wireless devices.

⚠ **NOTE**

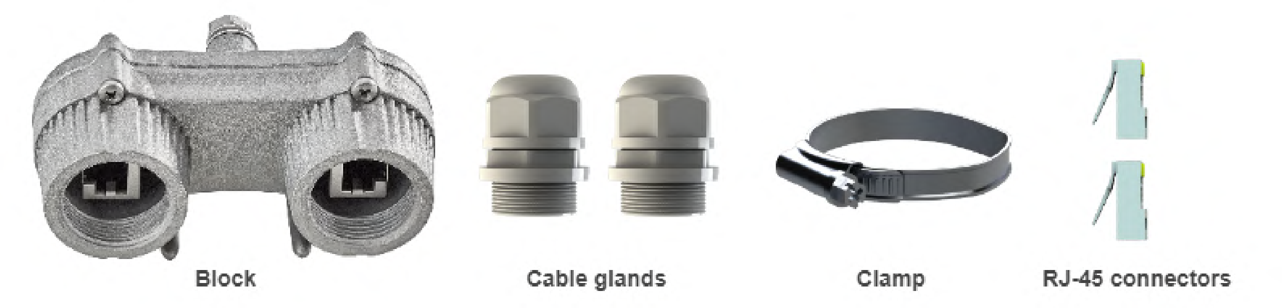
The device is not supplied by default and must be ordered separately.

<table>
<tr><th>Parameter</th><th colspan="9">Description</th></tr>
<tr><td><b>Size and Weight</b></td><td colspan="9">• 45x92x55.5 mm, 0.13 kg</td></tr>
<tr><td><b>Connectors and Interfaces</b></td><td colspan="9">• 2 x Ethernet ports
• Ground clamp</td></tr>
<tr><td><b>Supported Ethernet Modes</b></td><td colspan="9">• 10/100/1000 Mbps (Gigabit Ethernet pass-through)</td></tr>
<tr><td><b>Water and Dust Protection</b></td><td colspan="9">• IP66 and IP67</td></tr>
<tr><td><b>Operating temperature range</b></td><td colspan="9">• -55 °C ... +60 °C</td></tr>
<tr><td rowspan="2"><b>Ethernet pinout</b></td><td><b>Pin</b></td><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td><td><b>5</b></td><td><b>6</b></td><td><b>7</b></td><td><b>8</b></td></tr>
<tr><td><b>Data pair</b></td><td>A+</td><td>A-</td><td>B+</td><td>C-</td><td>C+</td><td>B-</td><td>D+</td><td>D-</td></tr>
</table>

Parameter	Description
Lightning Protection	In compliance with: • GR-1089 • IEC 61000-4-2 (ESD) 15kV (air), 8kV (contact) • IEC 61000-4-4 (EFT) 40A (tp = 5/50ns) • IEC 61000-4-5 (Lightning) L5, 95A (tp = 8/20us) • ETSI ETS 300 386

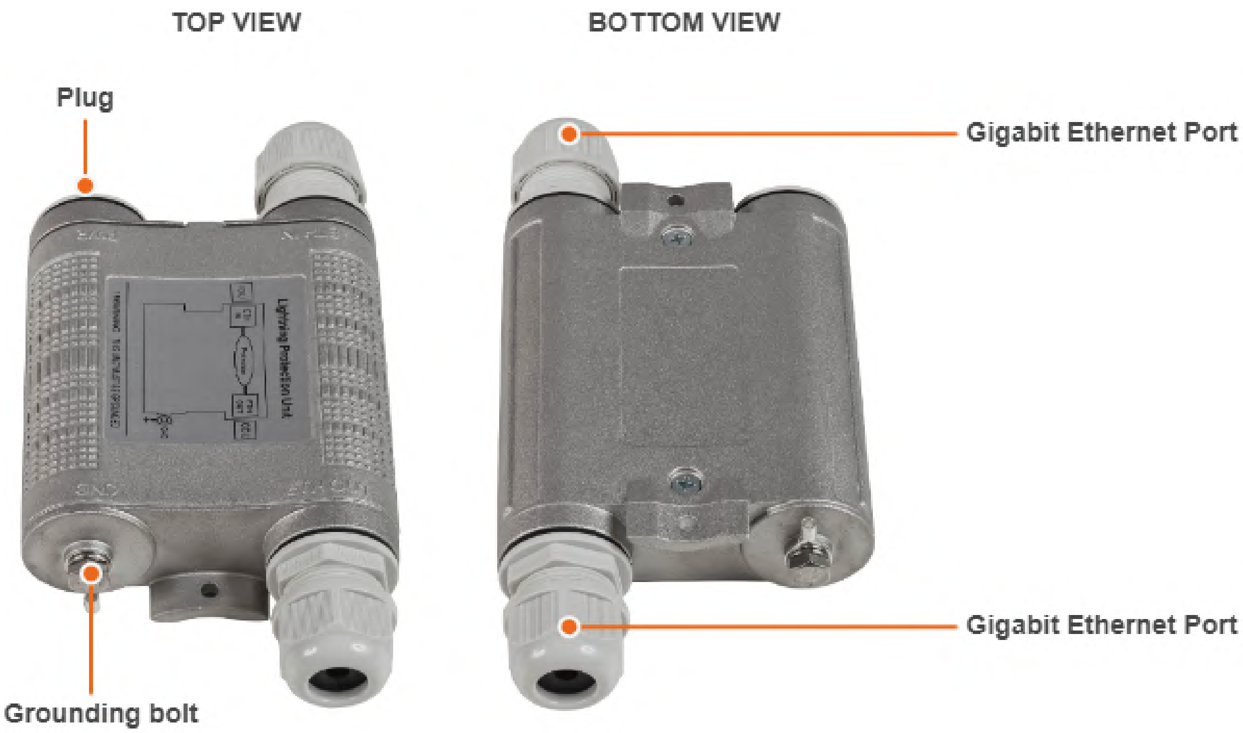
4 Table - AUX-ODU-LPU-L Specification

Packing list



7 Figure - Packing list AUX-ODU-LPU-L

3.6.2 AUX-ODU-LPU-G



8 Figure - AUX-ODU-LPU-G

Optional indoor/outdoor Lightning Protection Unit for Infinet Wireless systems designed to withstand the toughest conditions and protect the outdoor or the indoor unit from sudden power surges induced by lightning strikes. It provides the same level of protection as AUX-ODU-INJ-G. AUX-ODU-LPU-G is compatible with all Infinet Wireless devices.

Despite the fact every Infinet Wireless unit has a built-in lightning protection, AUX-ODU-LPU-G, thanks to its superior GR-1089-grade protection, greatly reduces the risk of replacing damaged devices operating in harsh environments or difficult-to-reach locations.

NOTE

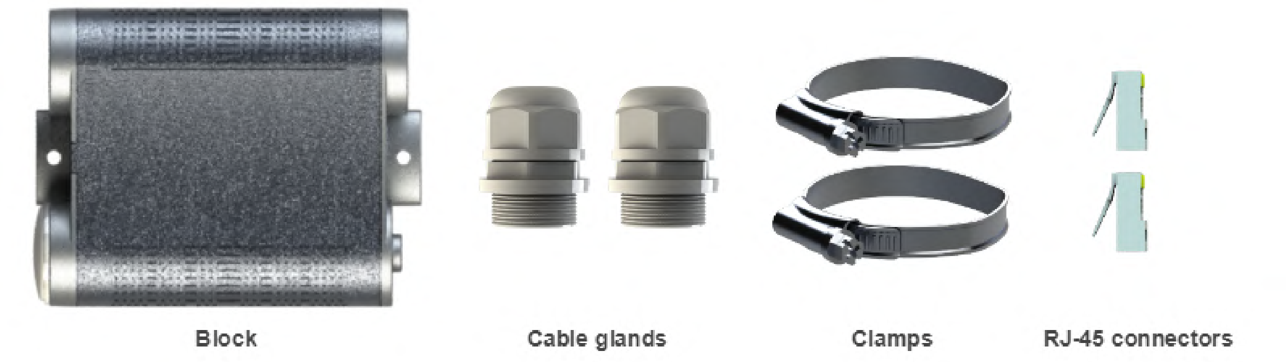
The device is not supplied by default and must be ordered separately.

Parameter	Description
Size and Weight	• 34x94x121 mm, 0.28 kg
Connectors and Interfaces	• ETH IN - Ethernet input • ETH OUT - Ethernet output (protected leg) • GND - Ground clamp
Supported Ethernet Modes	• 10/100/1000 Mbps (Gigabit Ethernet pass-through)
Water and Dust Protection	• IP66 and IP67

<table>
<tr><th>Parameter</th><th colspan="9">Description</th></tr>
<tr><td><b>Operating temperature range</b></td><td colspan="9">• -55 °C ... +60 °C</td></tr>
<tr><td rowspan="2"><b>ETH IN and ETH OUT pin-out</b></td><td><b>Pin</b></td><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td><td><b>5</b></td><td><b>6</b></td><td><b>7</b></td><td><b>8</b></td></tr>
<tr><td><b>Data pair</b></td><td>A+</td><td>A-</td><td>B+</td><td>C-</td><td>C+</td><td>B-</td><td>D+</td><td>D-</td></tr>
<tr><td><b>Lightning Protection</b></td><td colspan="9">In compliance with:
• GR-1089
• IEC 61000-4-2 (ESD) 15kV (air), 8kV (contact)
• IEC 61000-4-4 (EFT) 40A (tp = 5/50ns)
• IEC 61000-4-5 (Lightning) L5, 95A (tp = 8/20us)
• ETSI ETS 300 386</td></tr>
</table>

5 Table - AUX-ODU-LPU-G Specification

Packing list



9 Figure - Packing list AUX-ODU-LPU-G

3.7 Synchronization unit

AUX-ODU-SYNC is a TDD synchronization hub, which has been designed to provide a timing reference to Base Stations sectors of InfiMAN 2x2, InfiMAN Evolution families and InfiLINK 2x2 PRO devices. In combination with Infinet's proprietary TDMA-based wireless architecture, AUX-ODU-SYNC completes the solution, providing TDD synchronization to its systems, both legacy and newly deployed.

TDD synchronization eliminates self-interference between multiple co-located units and enables frequency re-use within the same site. Infinet's implementation supports not only intra-, but inter-site synchronization too, thanks to the fact that the timing reference is GNSS-based.

Parameter	Description
Compatible models	• InfiMAN 2x2 BS: Mmxb(s), Omxb(s), Qmxb • InfiLINK 2x2 PRO family: Mmx(s), Omx(s) • InfiMAN Evolution BS: E5-BSI, E5-BSQ, E5-BSE, E6-BSI, E6-BSE
GNSS receiver	• Embedded, GPS/GLONASS
GNSS antenna	• Embedded, active
Water and Dust protection	• IP66 and IP67
Consumption, W	• up to 4
Input voltage, VDC	• ±19..±56
PoE type	• Passive PoE (4,5,7,8 Ethernet pins used)

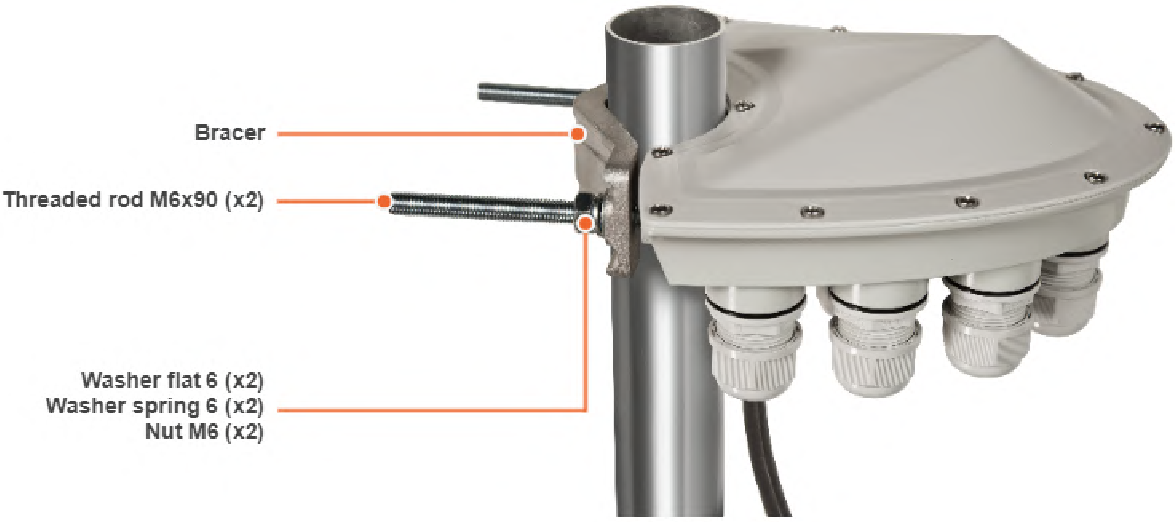
Parameter	Description
Interfaces and connectors	• Port 0-6: sync outs (7 RJ-45 connectors to connect to ODU with special cable CAB-SYNC or CAB-SYNC-E depends on model family) • Power: DC input (1 RJ-45 connector)
Compatible InfiNet Wireless power supplies	• IDU-CPE (supplied by default) • IDU-BS-G • IDU-BS-G(60W) • IDU-CPE-G(24W) • AUX-ODU-INJ-G • IDU-LA-G(V.01)
Temperature range	• ODU: -40…+60°C • IDU: 0...+40°C
Size and Weight	• 180x170x75mm, 0.65kg
Indicators	Indicators is located near the power port of AUX-ODU-SYNC: • POWER - power. • SYNC - TDD synchronization.

6 Table - AUX-ODU-SYNC specification

3.7.1 AUX-ODU-SYNC Mounting

AUX-ODU-SYNC can be installed on a pole, using fasteners from the delivery package:

1. Screw the threaded rod to the unit case.
2. Tighten the device and the bracer on the pole and fix them by the threaded rod using the nuts and washers as shown at the picture
3. Attach the grounding cable to the unit case using the grounding bolt.



CAUTION

Missing or bad grounding may leave the unit vulnerable to lightning damage.

3.7.2 AUX-ODU-SYNC Cable gland Assembling

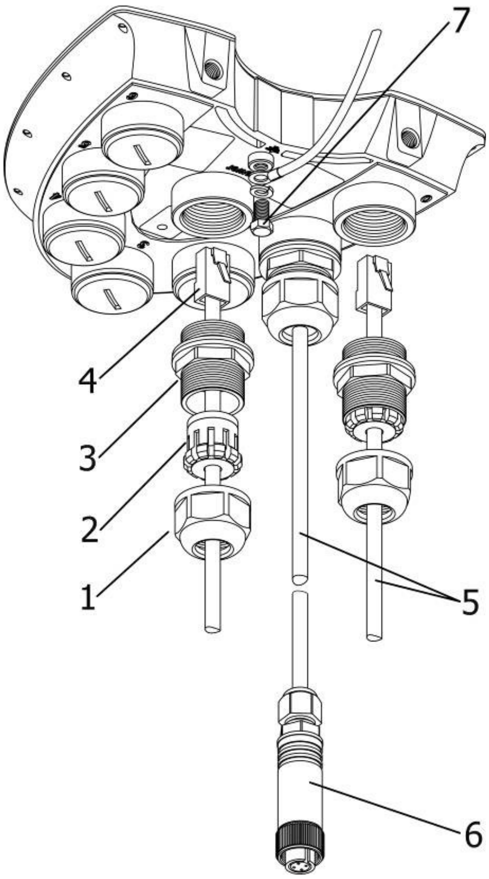
In order to ensure that the cable gland remains sealed under any environmental conditions, please, follow the assembly sequence according to the procedure below:

1. Put the cable gland nut (1), the split sealing grommet (2) and the cable gland threaded coupling (3) onto the cable
2. Crimp the connector onto the cable using the crimping tool:

   CAUTION

   Make sure that the connector is well-crimped. A loose connector can damage the device. Please note that such damage is not covered by the warranty.

   a. For connection to the port Power terminate the FTP Cat.5e cable with the unshielded RJ-45 connector (4) according to the EIA/TIA-568B. Do not use the shielded RJ-45 connector on this end of the cable as it should be attached on the IDU end (to provide grounding circuit)
   b. For connection to the ports 0-6 use the ready-assembled specialized CAB-SYNC or CAB-SYNC-E (5) cables
3. Insert the connector of the pre-terminated cable into the corresponding socket until you hear a click
4. Screw the cable gland threaded coupling (3) into the port and tighten it. Do not apply excessive force
5. Tighten the sealing grommet (2) by the cable gland nut (1). Do not apply excessive force.



10 Figure - Cable gland Assembling scheme

CAUTION

Please note that the pressure equalization system in Infinet devices is performed via gas exchange through a cable gland and Ethernet cable jacket with a dry room where the power supply is installed. In order to avoid AUX-ODU-SYNC failure due to moisture entering the device, for example, during the pressure drop during the rain, the cable gland assembly requirements should be met and there are should be no cracks in the Ethernet cable jacket.
In addition, you should avoid the Ethernet cable bending near the AUX-ODU-SYNC and pinching with clamps, that can bring to the pressure equalization system fault between the internal volume of the sealed AUX-ODU-SYNC and the external environment during a sudden air temperature change. This may lead to the leakage and device failures.

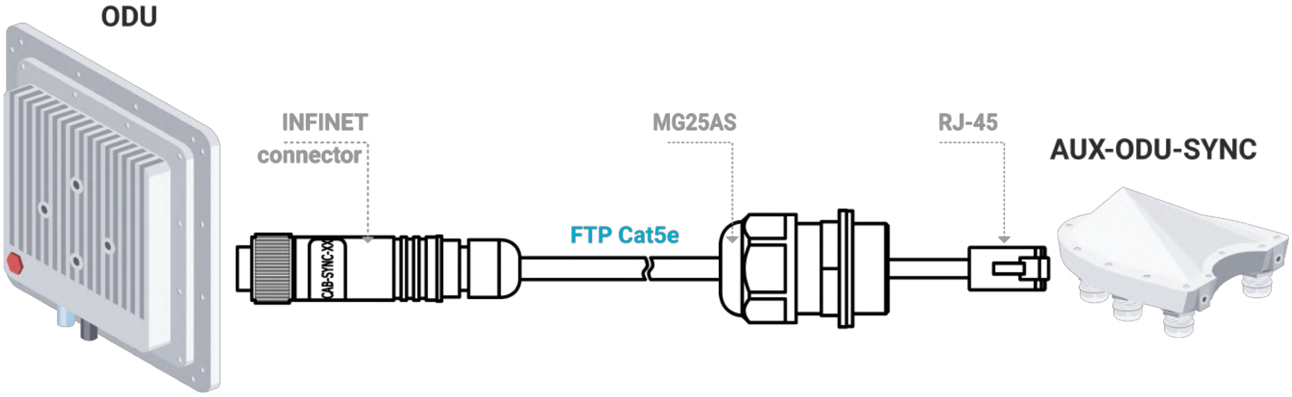
3.7.3 AUX-ODU-SYNC Connection to ODU

To connect AUX-ODU-SYNC to the units use the ready-assembled specialized CAB-SYNC cables for InfiMAN 2x2 and InfiLINK 2x2 PRO devices or CAB-SYNC-E cables for InfiMAN Evolution base station sectors. CAB-SYNC and CAB-SYNC-E must be ordered additionally. Information about CAB-SYNC and CAB-SYNC-E cables is available at Infinet web site in the "Accessories[6]" section.

[6] https://infinetwireless.com/products/accessories

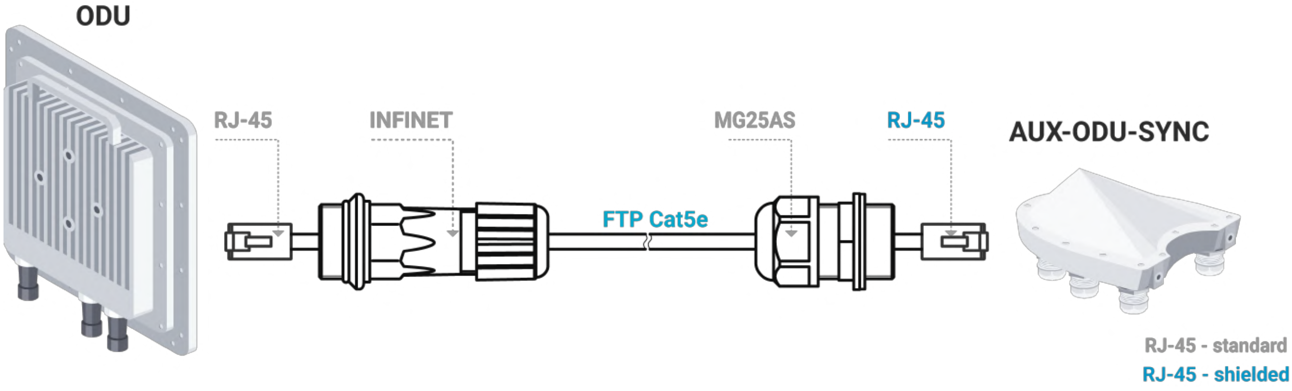
InfiMAN 2x2 and InfiLINK 2x2 PRO

To connect AUX-ODU-SYNC to ODU insert the INFINET connector of the CAB-SYNC cable to the console port of ODU and tighten the cap nut.



InfiMAN Evolution base station sector

To connect AUX-ODU-SYNC to ODU insert the RJ-45 connector with INFINET cable gland of the CAB-SYNC-E into the corresponding socket of the ODU until you hear a click. Perform the device port insulation with a cable gland as instructed above.



NOTE

Synchronization settings with AUX-ODU-SYNC is described in the document:

- InfiLINK 2x2 PRO, InfiMAN 2x2 BS[7].
- InfiMAN Evolution BS(see page 31).

3.8 Packing List

Before the installation, please make sure you have all necessary parts and accessories.

[7] https://wiki.infinetwireless.com/display/DR/Connection+to+the+synchronization+unit

3.8.1 InfiMAN Evolution BS packing list

- Outdoor unit (ODU).
- Power supply.
- Cable gland (x3).
- Shielded RJ-45 connector.
- Unshielded RJ-45 connector.
- Mounting kit - universal assembling kit for mounting the ODU on standard pole, wall or thick pipe (vertical/horizontal).
- Power cord - the model depends on the region, according to the Purchase Order.

3.8.2 InfiMAN Evolution STE and InfiLINK Evolution packing list (except devices with 18 dBi antenna gain)

- Outdoor unit (ODU).
- Power supply.
- Cable gland.
- Shielded RJ-45 connector.
- Unshielded RJ-45 connector.
- Mounting kit - universal assembling kit for mounting the ODU on standard pole, wall or thick pipe (vertical/horizontal).
- Power cord - the model depends on the region, according to the Purchase Order.

3.8.3 E5-ST18, E6-ST18 packing list

- Outdoor unit (ODU).
- Power supply.
- Cable gland.
- Shielded RJ-45 connector.
- Unshielded RJ-45 connector.
- Power cord - the model depends on the region, according to the Purchase Order.
- Nut M6 DIN 934 A4 (x2).
- Washer 6 flat (x2).
- Washer 6 spring (x2).
- Threaded rod M6x90 (x2).
- Bracer.

4 Planning considerations

Unable to render include or excerpt-include. Could not retrieve page.

4.1 Spectral aggregation

It is recommended to place base station sectors above the subscriber terminals as high as possible to provide proper antenna tilt in vertical direction and to minimize self-interference. The optimal antenna tilt is defined by the vertical beam width of the sectoral antenna and by the required sector coverage. It must cover all the area, where you plan to deploy the subscriber terminals.

Spectral aggregation should be taken into account when planning composite backhauling links, when installing devices in close proximity to each other on the same pole or in order to implement redundancy and link aggregation. For more information, proceed with the "Link aggregation, balancing and redundancy[8]" article. The devices located close to each other can cause mutual interference. Do not ignore the spectral aggregation rules, otherwise it can lead to a degradation of the wireless links.

The document will provide recommendations on distance and frequency separation for scenarios with and without an external synchronization hub. An external clock source allows you to synchronize the time (the beginning of each second) on multiple devices, up to 7 devices, with an accuracy of less than a microsecond so that all connected devices can turn on the transmitters at the same time. This completely eliminates the mutual influence of neighboring sectors, when one transmitting device with its powerful signal prevents the neighboring device from receiving weak signals from its terminals. Wireless devices synchronization using AUX-ODU-SYNC makes it possible to reuse the frequency within the same base station, that is, different sectors of the same base station can operate on the same frequency channels. When using synchronization, a four-sector base station can operate on only two frequency channels, significantly increasing the real spectral efficiency of the system.

Mutual interference occurs not only between sectors and subscriber terminals of one multi-sector base station, but also between different base stations when they are densely located in a limited frequency range. Synchronization of base stations prevents mutual interference of such base stations and subscriber terminals that working with them.

Recommendations for istance and frequency separation for a four-sector ABAB base station are given below.

4.1.1 Without synchronization

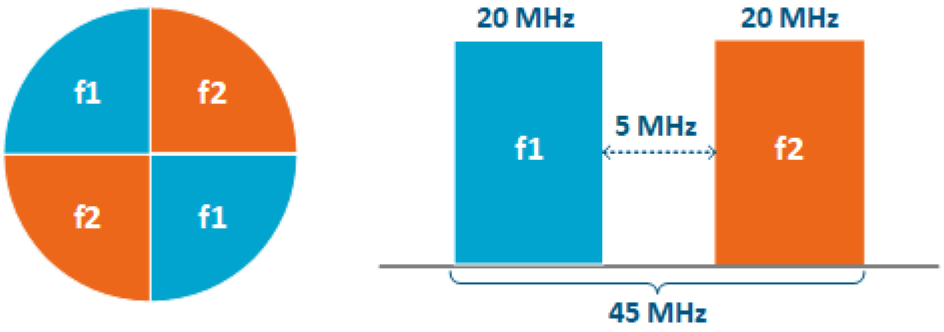
- Distance separation (vertical or horizontal) must be at least two meters between the edges of the antennas.
- Reduce the transmission power.

4.1.2 With synchronization

4 collocated base stations mounted back-to-back.

- The recommended guard interval between the end/boundary frequencies of the occupied bands of the neighboring sectors 5 MHz.

[8] https://wiki.infinetwireless.com/display/DR/InfiLINK+XG+and+InfiLINK+XG+1000



4.2 Synchronization settings

To perform synchronization using an external hub, each base station sector must be connected to an AUX-ODU-SYNC.

The following conditions should be met:

- Frame size and DL/UL ratio should be equal on all sync-end units.
- The automatic downlink ratio selection is not allowed.

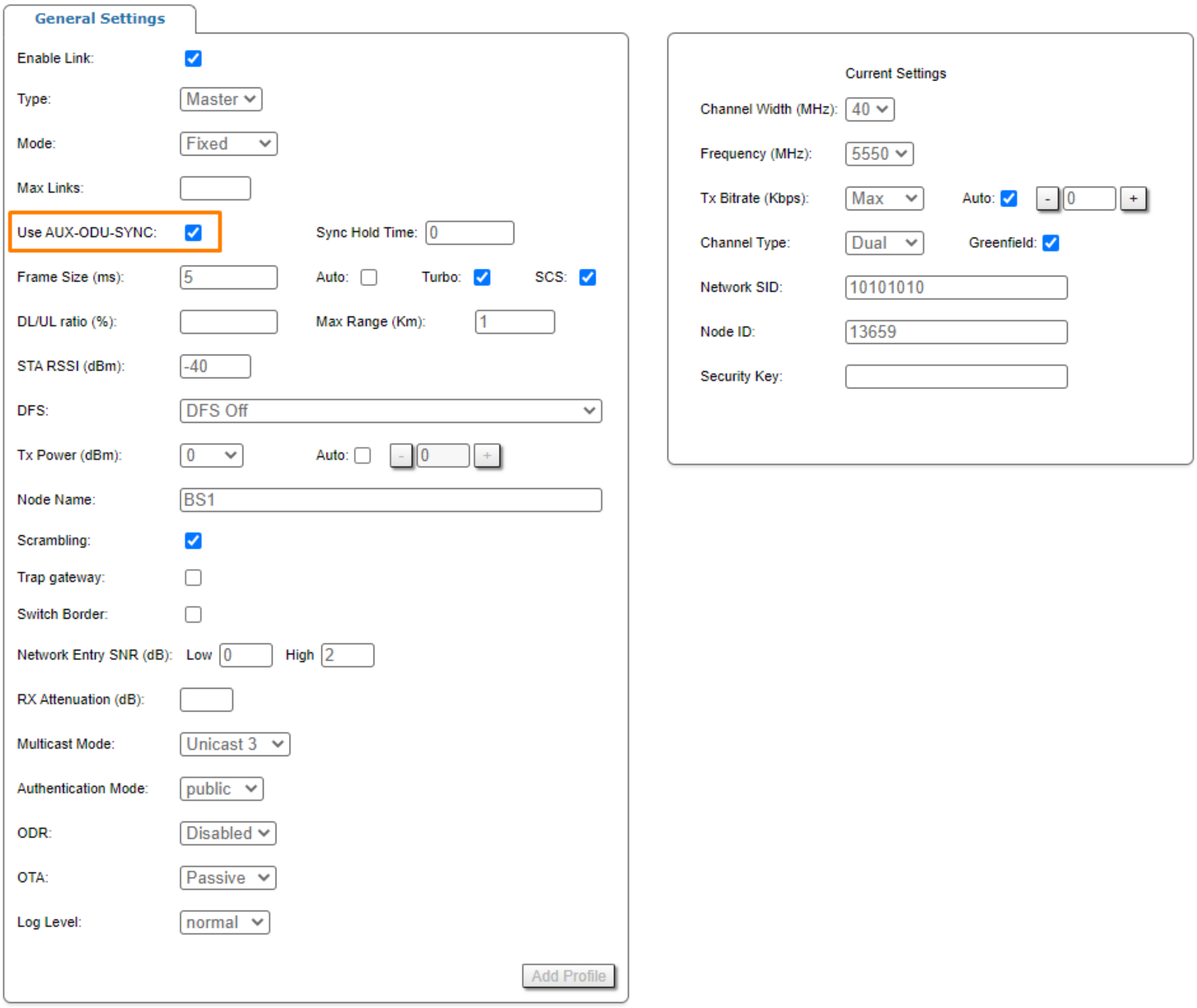
NOTE

The AUX-ODU-SYNC antenna is not included in the standard packing list. For more information about this antenna, proceed to the AUX-ODU-SYNC(see page 24) article.

4.2.1 Configuration via web interface

To enable synchronization via web interface:

- Go to the section "Basic Sttings" → "Link Settings" → "rf6.0".
- Check the box "Use AUX-ODU-SYNC" and click "Apply". Synchronization status and the number of visible satellites is displayed in the "Device Status" -> "Link Statistics" section.



General Settings

Enable Link: ☑

Type: Master

Mode: Fixed

Max Links:

Use AUX-ODU-SYNC: ☑ Sync Hold Time: 0

Frame Size (ms): 5 Auto: ☐ Turbo: ☑ SCS: ☑

DL/UL ratio (%): Max Range (Km): 1

STA RSSI (dBm): -40

DFS: DFS Off

Tx Power (dBm): 0 Auto: ☐ - 0 +

Node Name: BS1

Scrambling: ☑

Trap gateway: ☐

Switch Border: ☐

Network Entry SNR (dB): Low 0 High 2

RX Attenuation (dB):

Multicast Mode: Unicast 3

Authentication Mode: public

ODR: Disabled

OTA: Passive

Log Level: normal

Add Profile

Current Settings

Channel Width (MHz): 40

Frequency (MHz): 5550

Tx Bitrate (Kbps): Max Auto: ☑ - 0 +

Channel Type: Dual Greenfield: ☑

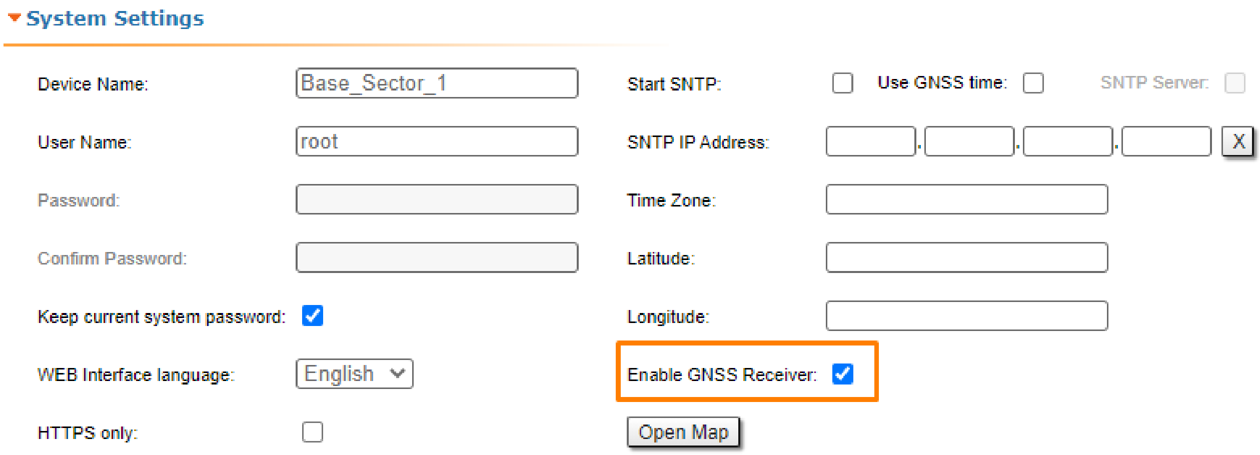
Network SID: 10101010

Node ID: 13659

Security Key:

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

- Go to the section "Basic Settings" -> "System Settings".
- Check the box "Enable GNSS Receiver" and click "Apply" button.



System Settings

Device Name: Base_Sector_1

User Name: root

Password:

Confirm Password:

Keep current system password: ☑

WEB Interface language: English

HTTPS only: ☐

Start SNTP: ☐ Use GNSS time: ☐ SNTP Server: ☐

SNTP IP Address: . . . X

Time Zone:

Latitude:

Longitude:

Enable GNSS Receiver: ☑

Open Map

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

4.2.2 Configuration via CLI

Enable synchronization:

Enable synchronization

```
tsync enable
```

The synchronization mode information:

Synchronization info

```
tsync
```

The following parameters will be displayed:

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

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

Receiving navigation information mode

```
gps start
```

Detailed GNSS statistic can be obtained:

GNSS statistic

```
gps stat
```

GNSS statistics parameters:

Parameter	Description
Total GPS time	Total time of GPS operation

Parameter	Description
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)

5 Link Pre-configuration in the lab

Usually, before going into the field, it is recommended to pre-configure in the lab the Infinet Wireless units to verify the link establishment. Take the units out of the package and place them on the table.

⚠ **NOTE**

A minimum set of requirements must be met during devices pre-configuration in the lab:

- Make sure that devices are positioned in such a way so that they are not directed right at each other to prevent device damage.
- In case of connectorized model configuration, it is recommended to connect the two devices in the link directly, with RF cables and RF attenuators with attenuation of at least 40 dB for each polarization (installation\deinstallation of the RF attenuators and RF cables should only be performed when the devices are switched off).
- In case an external antenna or the other unit in the link is connected to only one N-type connector do not switch on the unit.

Step 1: Scheme connection assembling

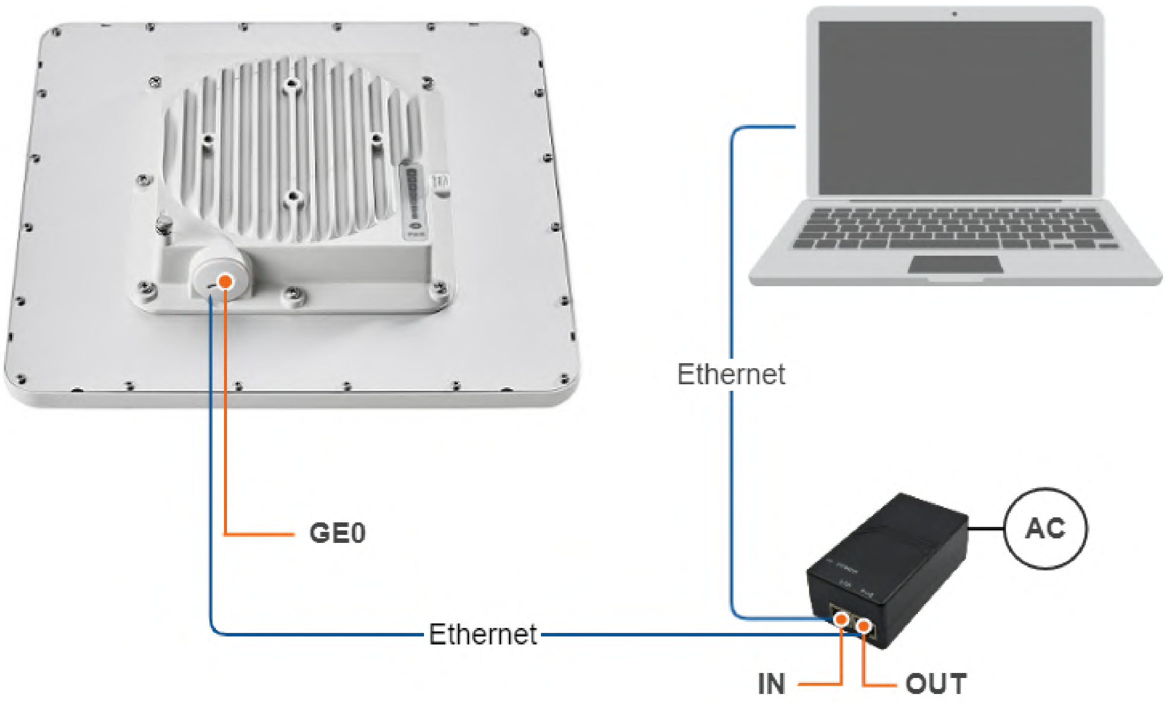
The equipment list required for the lab configuration:

1. Outdoor units - 2 pcs.
2. Power supply - 2 pcs.
3. Power cord - 2 pcs.
4. Ethernet cables - 4 pcs.
5. Laptop with Ethernet port available.

We will perform the settings mentioned below for each unit and check if the wireless link was established correctly.

Use the following instruction to assemble a test scheme:

1. Connect Gigabit Ethernet port at the ODU to the power supply port labeled as "OUT".
2. Connect Ethernet port at the laptop to the power supply port labeled as "IN".
3. Connect the power cord to power supply and plug it to AC mains.



Step 2: Access to the device

Let's access each unit to the default IP address 10.10.10.1 with mask 255.255.255.0 via a web browser. Before, make sure the Ethernet port of the Laptop has an IP address assigned from the same subnetwork as the one for the unit (e.g., set 10.10.10.10 with mask 255.255.255.0).

> ⚠ **NOTE**
>
> We assume that each unit used in this setup has not been configured before and runs with the factory settings.

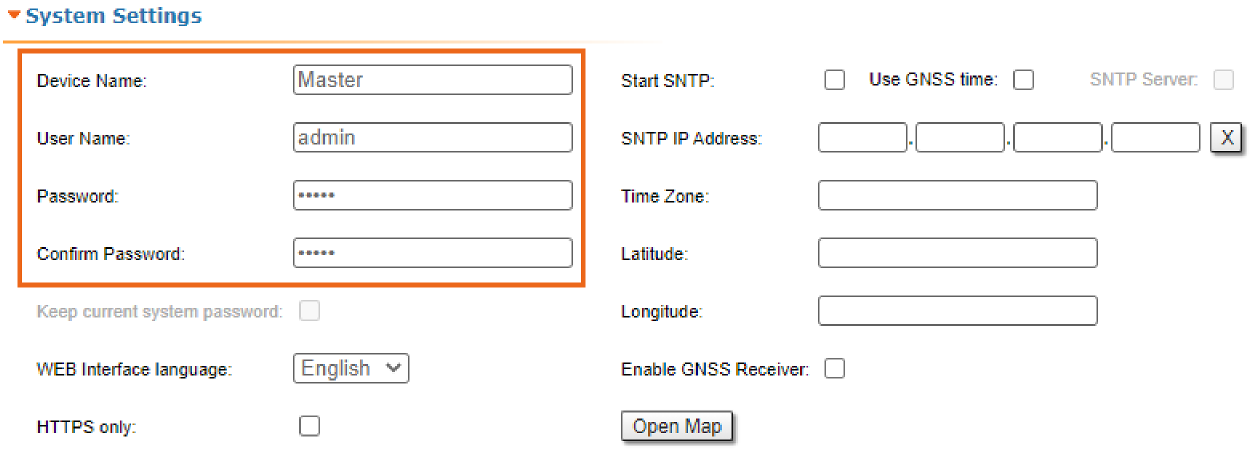
Use any letters or numbers for the initial authentication on each unit, for example:

- Login: login.
- Password: password.

> ⚠ **NOTE**
>
> We strongly recommend to change your login and password after the first login.

After the first login, let's configure a distinctive name for each unit and set a custom login and password. Go to the Basic Settings section, then to System Settings and configure::

- Device Name (e.g., Master/Slave).
- User Name (e.g., admin).
- Password (e.g., admin).



System Settings

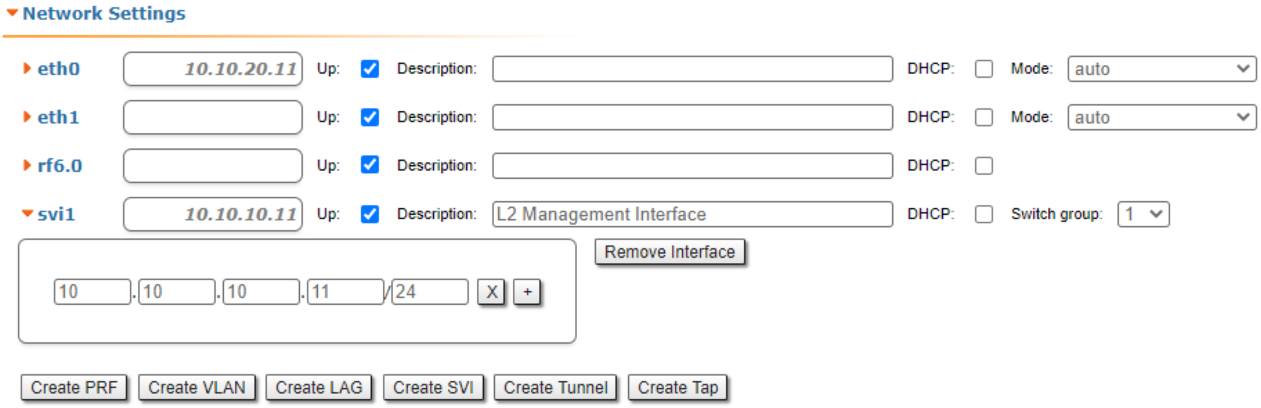
Device Name:	Master	Start SNTP:	□	Use GNSS time: □	SNTP Server: □
User Name:	admin	SNTP IP Address:	. . .	X	
Password:	•••••	Time Zone:			
Confirm Password:	•••••	Latitude:			
Keep current system password:	□	Longitude:			
WEB Interface language:	English	Enable GNSS Receiver:	□		
HTTPS only:	□	Open Map			

> **NOTE**
>
> At the next login set up login and password to access the unit in the privileged mode.

Step 3: Management IP change

Let's change the management IP of each unit. Go to the "Basic Settings" section, then to Network Settings and change the default IP address of the ‘svi’ interface which is a logical interface used for remote management access in MINT switching mode (MINT switching mode is enabled by default).

Network settings for Master:



Network Settings

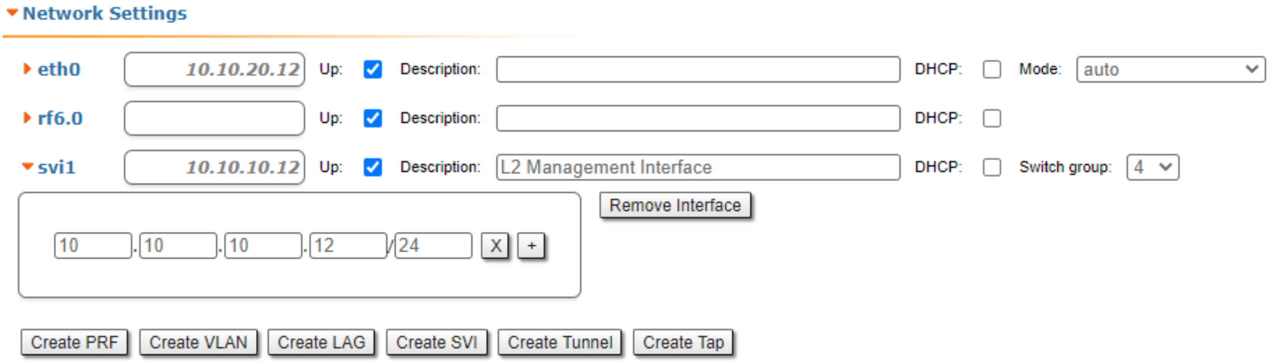
eth0	10.10.20.11	Up: ☑	Description:		DHCP: □	Mode:	auto
eth1		Up: ☑	Description:		DHCP: □	Mode:	auto
rf6.0		Up: ☑	Description:		DHCP: □		
svi1	10.10.10.11	Up: ☑	Description:	L2 Management Interface	DHCP: □	Switch group:	1

10 . 10 . 10 . 11 / 24 X +

Remove Interface

Create PRF | Create VLAN | Create LAG | Create SVI | Create Tunnel | Create Tap

Network settings for Slave:



Network Settings

eth0	10.10.20.12	Up: ☑	Description:		DHCP: □	Mode:	auto
rf6.0		Up: ☑	Description:		DHCP: □		
svi1	10.10.10.12	Up: ☑	Description:	L2 Management Interface	DHCP: □	Switch group:	4

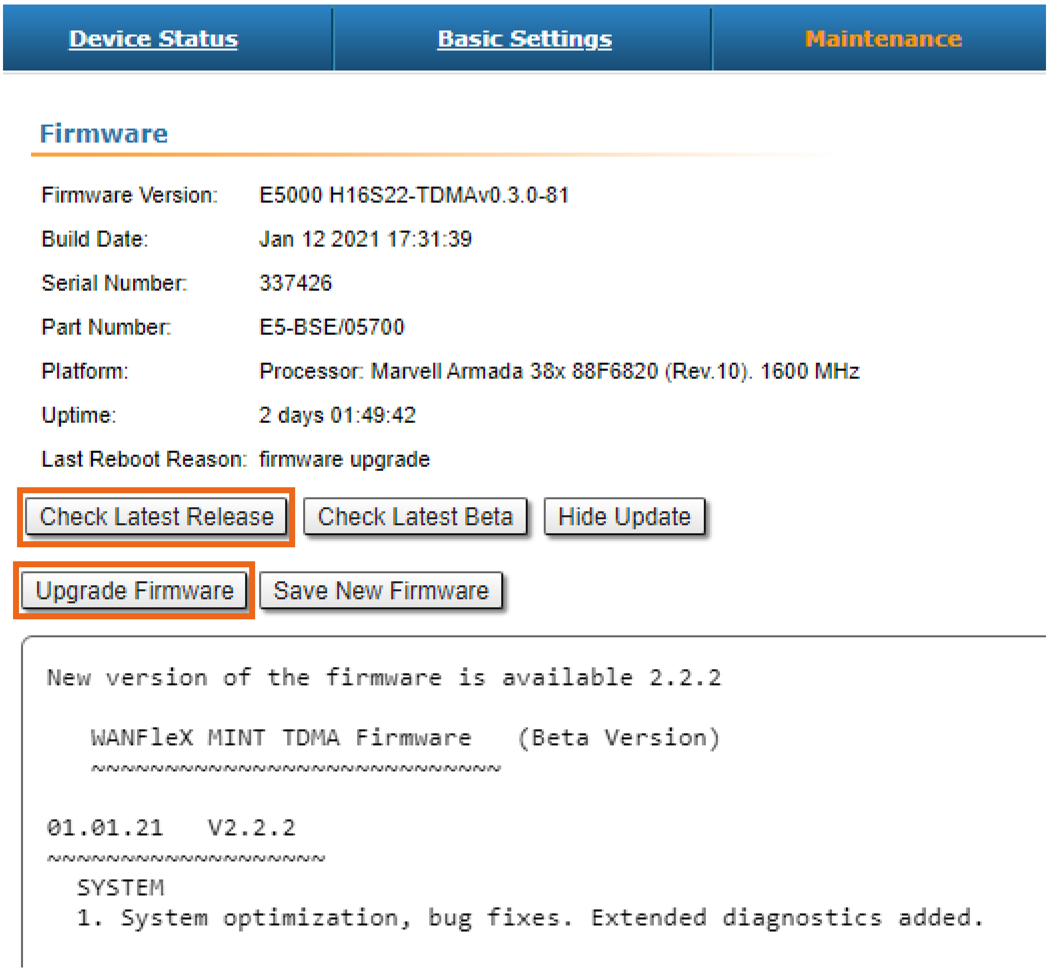
10 . 10 . 10 . 12 / 24 X +

Remove Interface

Create PRF | Create VLAN | Create LAG | Create SVI | Create Tunnel | Create Tap

5.1 Step 4: Software upgrade

Let's upgrade each unit to the latest stable firmware version. Go to the Maintenance section and click on the "Check Latest Release" button. In case a new software version is available, click on the "Upgrade Firmware" to initiate the firmware upgrade process. Before, make sure the laptop which is connected to the unit has an Internet connection, too. Otherwise, the manual firmware upgrade process should be performed.



Firmware

Firmware Version:	E5000 H16S22-TDMAv0.3.0-81
Build Date:	Jan 12 2021 17:31:39
Serial Number:	337426
Part Number:	E5-BSE/05700
Platform:	Processor: Marvell Armada 38x 88F6820 (Rev.10). 1600 MHz
Uptime:	2 days 01:49:42
Last Reboot Reason:	firmware upgrade

```
New version of the firmware is available 2.2.2

   WANFleX MINT TDMA Firmware   (Beta Version)
   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~

01.01.21   V2.2.2
~~~~~~~~~~~~~~~~~~~
  SYSTEM
  1. System optimization, bug fixes. Extended diagnostics added.
```

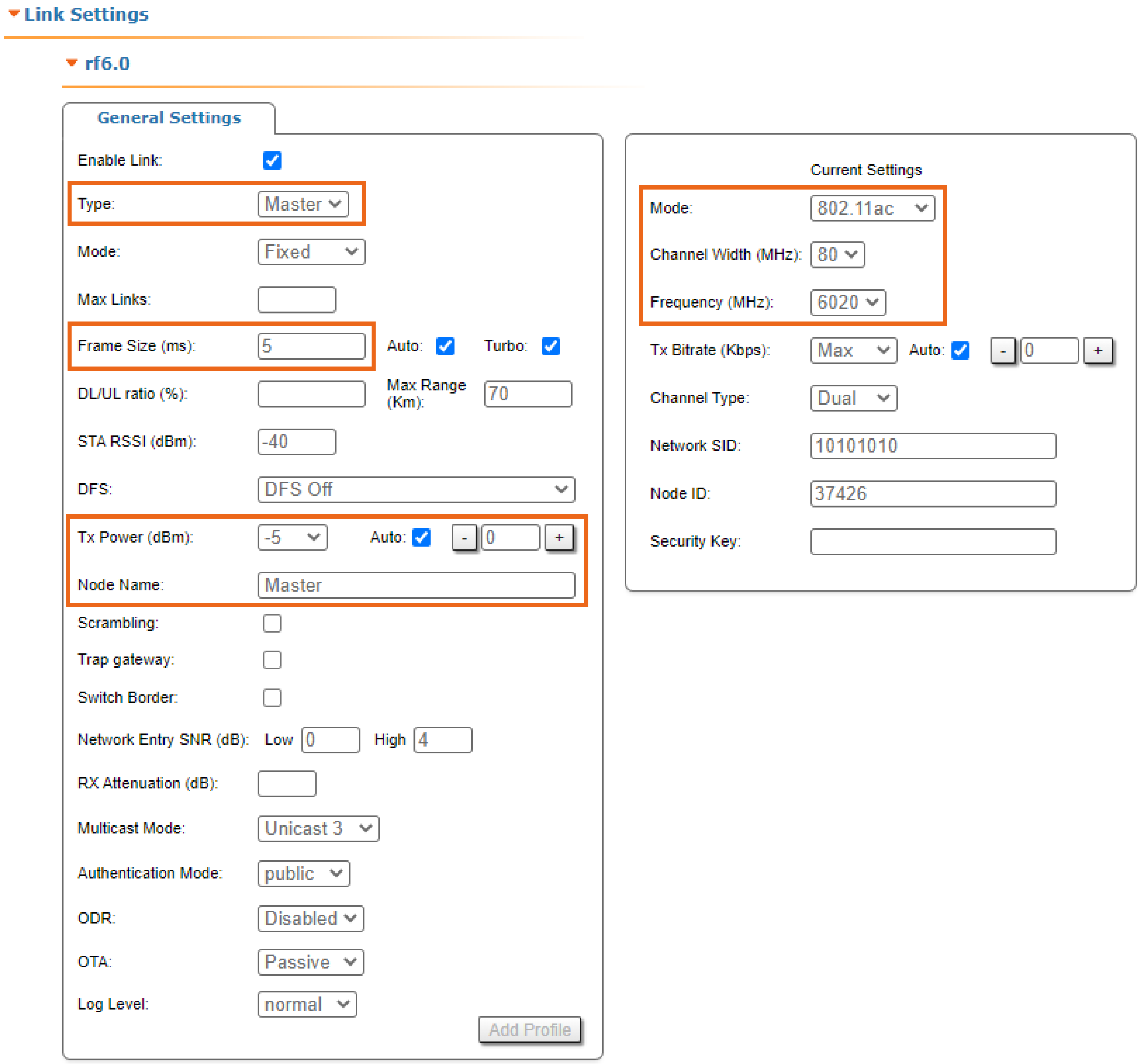
Step 5: Radio parameters configuration

Let's configure the minimum needed radio parameters to establish the link.

At the unit named Master at step #3 above, go to the "Basic Settings" section, then to "Link Settings" and set this unit with:

- Type: Master.
- Tx Power: e.g., -5 dBm (set the minimum value in the range, as currently, we are in the lab, and we don't need high output power anymore).
- Node Name: e.g., Master (it is the same as the value set at Device Name if this was saved before).
- Mode: 802.11ac (if compatibility with InfiLINK 2x2 / InfiMAN 2x2 families devices is not required).
- Channel Width: e.g., 80 MHz.
- Frequency: e.g., 6020 MHz.
- Frame size: e.g., 5 ms.

The rest of parameters remain with the default values.



Link Settings

rf6.0

General Settings

Enable Link: ☑
Type: Master
Mode: Fixed
Max Links:
Frame Size (ms): 5 Auto: ☑ Turbo: ☑
DL/UL ratio (%): Max Range (Km): 70
STA RSSI (dBm): -40
DFS: DFS Off
Tx Power (dBm): -5 Auto: ☑ - 0 +
Node Name: Master
Scrambling: □
Trap gateway: □
Switch Border: □
Network Entry SNR (dB): Low 0 High 4
RX Attenuation (dB):
Multicast Mode: Unicast 3
Authentication Mode: public
ODR: Disabled
OTA: Passive
Log Level: normal

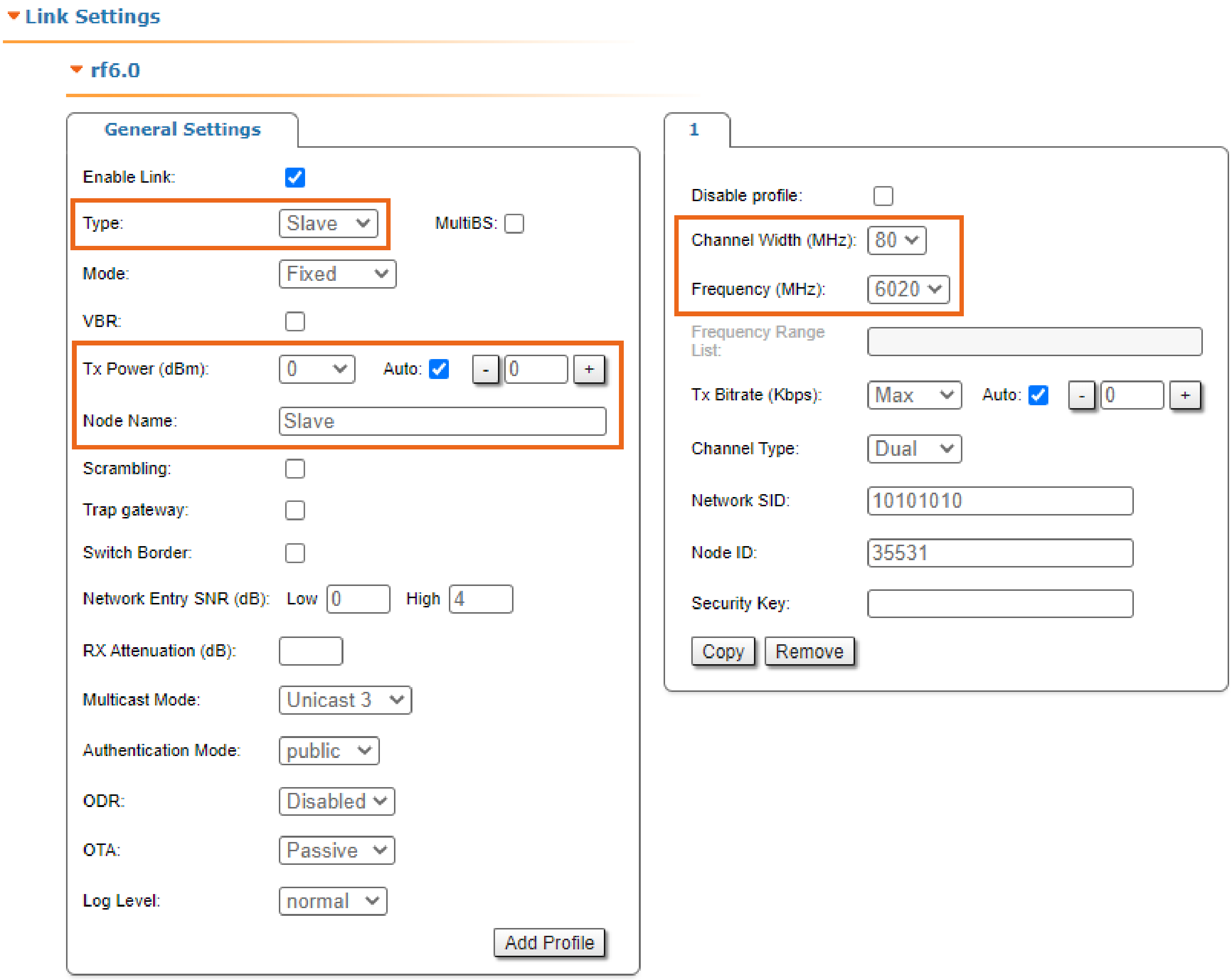
Current Settings

Mode: 802.11ac
Channel Width (MHz): 80
Frequency (MHz): 6020
Tx Bitrate (Kbps): Max Auto: ☑ - 0 +
Channel Type: Dual
Network SID: 10101010
Node ID: 37426
Security Key:

At the unit named Slave at step #3 above, go to the Basic Settings section, then to Link Settings and set this unit with:

- Type: Slave.
- Tx Power: e.g., 0 dBm (set the minimum value in the range, as currently, we are in the lab, and we don't need high output power anymore).
- Node Name: e.g., Slave (it is the same as the value set at Device Name if this was saved before).
- Channel Width: e.g., 80 MHz.
- Frequency: e.g., 6020 MHz.

The rest of parameters remain with the default values.



Link Settings

rf6.0

General Settings

Enable Link:	☑
Type:	Slave; MultiBS: ☐
Mode:	Fixed
VBR:	☐
Tx Power (dBm):	0; Auto: ☑ [-] 0 [+]
Node Name:	Slave
Scrambling:	☐
Trap gateway:	☐
Switch Border:	☐
Network Entry SNR (dB):	Low 0 High 4
RX Attenuation (dB):	
Multicast Mode:	Unicast 3
Authentication Mode:	public
ODR:	Disabled
OTA:	Passive
Log Level:	normal

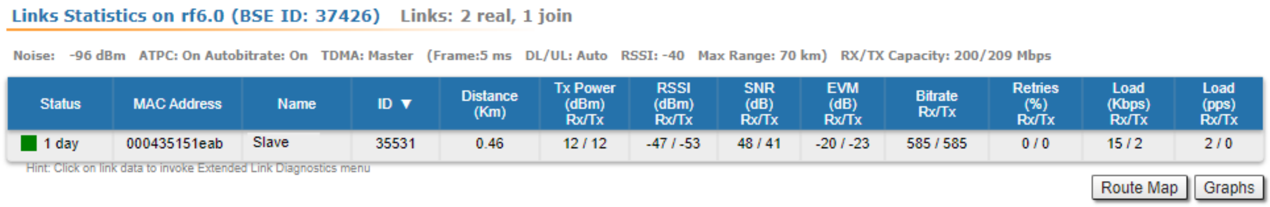
1

Disable profile:	☐
Channel Width (MHz):	80
Frequency (MHz):	6020
Frequency Range List:	
Tx Bitrate (Kbps):	Max; Auto: ☑ [-] 0 [+]
Channel Type:	Dual
Network SID:	10101010
Node ID:	35531
Security Key:	

Step 6: Check the wireless link status

Let's apply all settings described above for each unit and after login let's go to the Device Status section, and check the link establishment at Link Statistics.

Master Link Statistics:



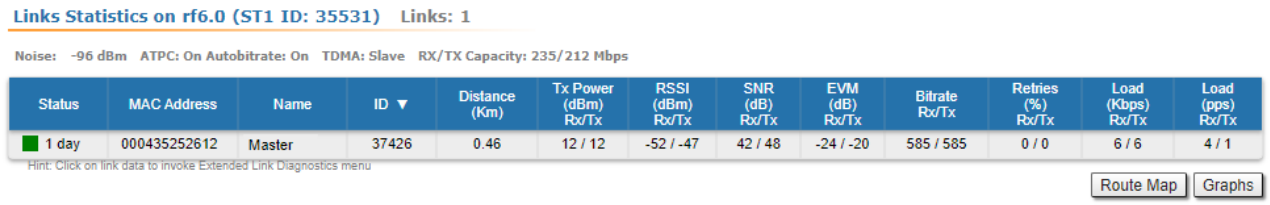
Links Statistics on rf6.0 (BSE ID: 37426) Links: 2 real, 1 join

Noise: -96 dBm ATPC: On Autobitrate: On TDMA: Master (Frame:5 ms DL/UL: Auto RSSI: -40 Max Range: 70 km) RX/TX Capacity: 200/209 Mbps

Status	MAC Address	Name	ID ▼	Distance (Km)	Tx Power (dBm) Rx/Tx	RSSI (dBm) Rx/Tx	SNR (dB) Rx/Tx	EVM (dB) Rx/Tx	Bitrate Rx/Tx	Retries (%) Rx/Tx	Load (Kbps) Rx/Tx	Load (pps) Rx/Tx
🟩 1 day	000435151eab	Slave	35531	0.46	12 / 12	-47 / -53	48 / 41	-20 / -23	585 / 585	0 / 0	15 / 2	2 / 0

Hint: Click on link data to invoke Extended Link Diagnostics menu

Slave Link Statistics:



Links Statistics on rf6.0 (ST1 ID: 35531) Links: 1

Noise: -96 dBm ATPC: On Autobitrate: On TDMA: Slave RX/TX Capacity: 235/212 Mbps

Status	MAC Address	Name	ID ▼	Distance (Km)	Tx Power (dBm) Rx/Tx	RSSI (dBm) Rx/Tx	SNR (dB) Rx/Tx	EVM (dB) Rx/Tx	Bitrate Rx/Tx	Retries (%) Rx/Tx	Load (Kbps) Rx/Tx	Load (pps) Rx/Tx
🟩 1 day	000435252612	Master	37426	0.46	12 / 12	-52 / -47	42 / 48	-24 / -20	585 / 585	0 / 0	6 / 6	4 / 1

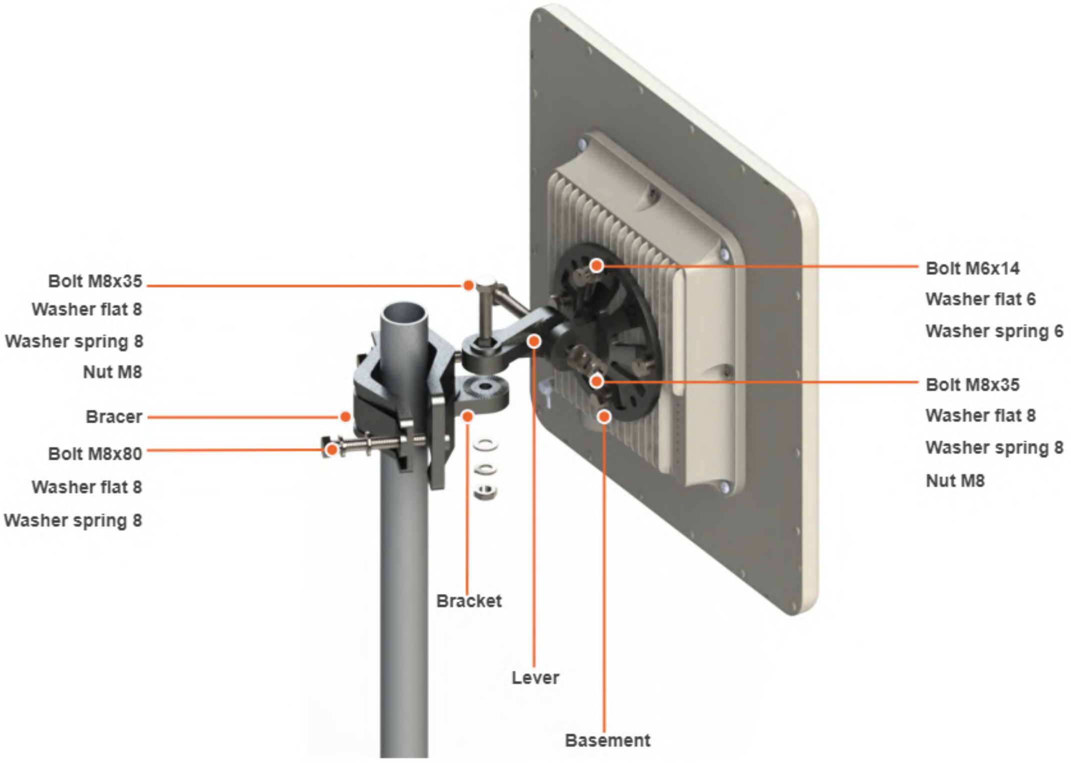
Hint: Click on link data to invoke Extended Link Diagnostics menu

6 Installation

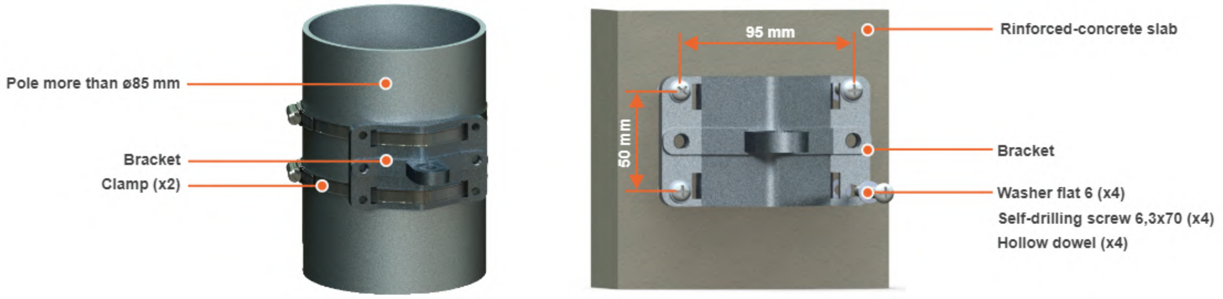
6.1 Mounting kit

6.1.1 MONT-KIT-85 Mounting kit

MONT-KIT-85 | MONT-KIT-85S is supplied with all models by default except E5-ST18 and E6-ST18. It allows to make reliable and easy installation of the unit with two-axis adjustment. Assemble the Mounting kit according to the scheme below. The nut must be tightened until the spring washer clicks, without over-tightening.



Mounting is carried out on a pole with a diameter 30-85 mm. There are also possible options for mounting on a wall or pole with a diameter more than 85 mm.



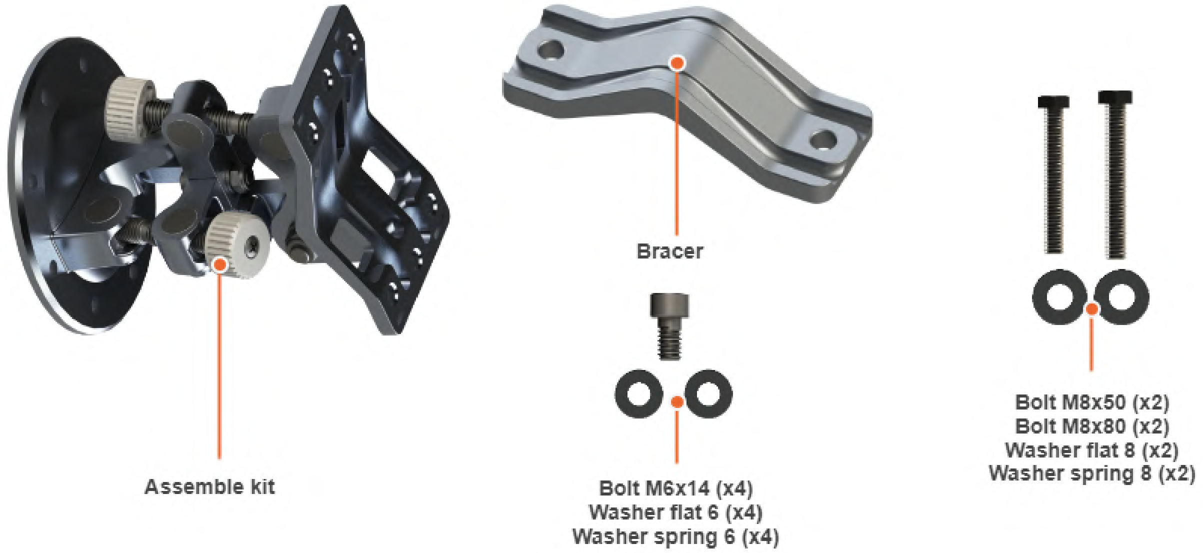
NOTE

Clamps and other optional fasteners are not included in the Mounting kit MONT-KIT-85.

6.1.2 MONT-KIT-85P Mounting kit

High precision mounting kit MONT-KIT-85P allows to make reliable and easy installation and enables extremely accurate adjustment on azimuth and elevation for optimal wireless link performance. Compatible for Quanta 5, Quanta 6, InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution, InfiLINK XG, InfiLINK XG 1000 families units. Especially suitable for installing high-gain antenna models that have a narrow beam.

Packing List



Assemble Procedure

Step 1: Insert and tighten the Assembled kit on the back side of the device using bolts M6x14, washers flat 6 and washers spring 6.

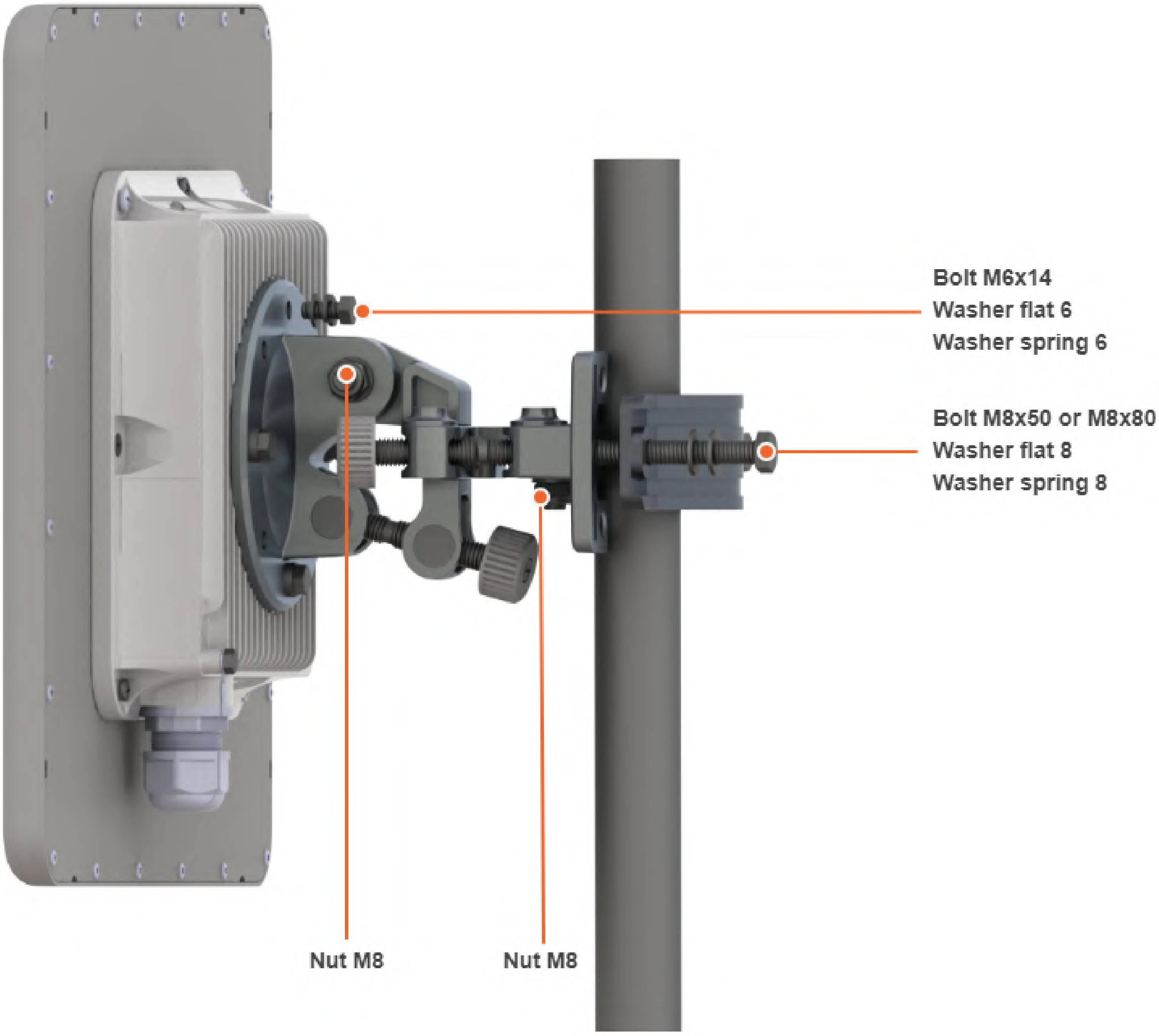
Step 2: Tighten the Assembled kit and Bracer to the pole using bolt M8, washer flat 8 and washer spring 8.

- Bolt M8x50 - used for installation on a pole with Ø 30 ... Ø 55 mm.
- Bolt M8x80 - used for installation on a pole with Ø 55 ... Ø 85 mm.

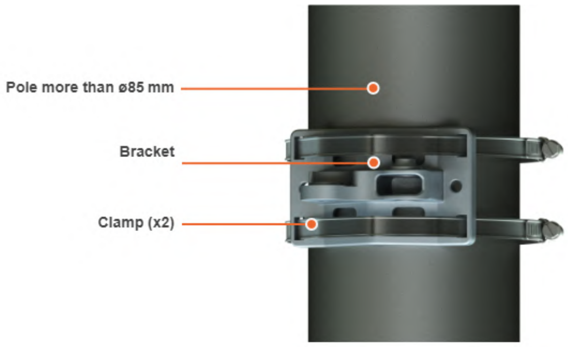
Step 3: Perform required antenna alignment using adjustment knobs and then tighten nuts M8.

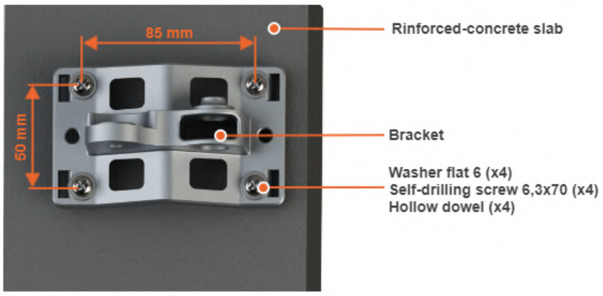
> ⚠ **NOTE**
>
> M8 nuts are pre-tightened at the manufacturing facility in a position that allows the device to be adjusted using the adjustment knobs and ensures that the wireless device does not shift during the final nuts tighten.

> ⚠ **NOTE**
>
> If further adjustment is required, weaken the nuts M8 on about 15 degrees. Do not adjust the knobs without weaken the nuts first.



Mounting is carried out on a pole with a diameter 30 ... 85 mm. There are also possible options for mounting on a wall or pole with a diameter more than 85 mm.



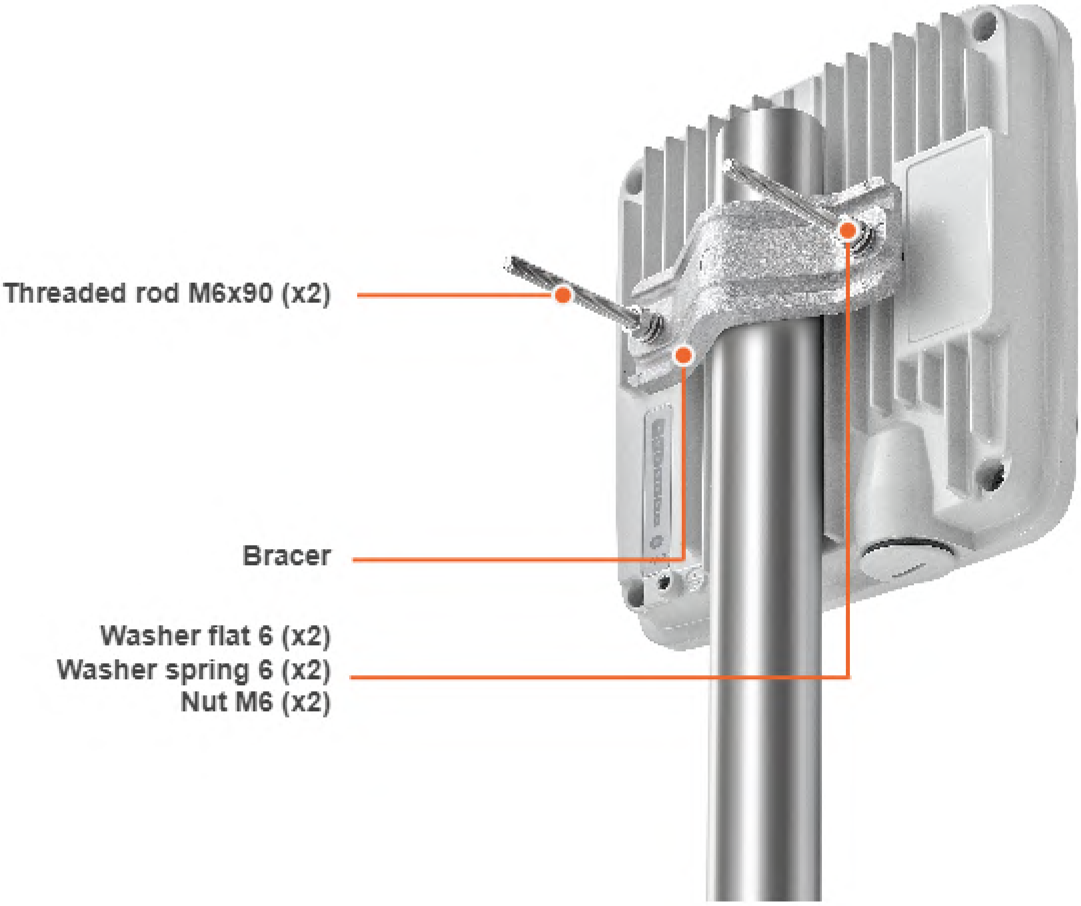


NOTE

Clamps and other optional fasteners are not included in the mounting kit MONT-KIT-85P.

6.1.3 Mounting kit for E5-ST18/E6-ST18

E5-ST18 and E6-ST18 models installation is performed using bracer and threaded rod M6x90 that is supplied by default. Install the device according to the scheme below. The nut must be tightened until the spring washer clicks, without over-tightening.



6.2 Cable Gland Assembly

6.2.1 Cable Gland Assembly for RJ-45 connector

Required components are listed below.

1. Unshielded RJ-45 connector.
2. Shielded RJ-45 connector.
3. FTP Cat5e cable.
4. Cable gland:
    - Cable gland nut.
    - Split sealing grommet (with inner diameter 7 mm).
    - Cable gland threaded coupling.
5. Crimping tool for RJ-45 connector.

NOTE

The outside diameter value of the FTP Cat5e cable should not exceed 7 mm.

NOTE

Cable gland can be assembled on pre-crimped cable.

Assemble procedure

In order to ensure that the device case remains sealed under any environmental conditions follow the assemble procedure:

- **Step 1**: Crimp the standard RJ-45 connector onto the cable using crimping tool. Pin-out scheme: T568B wiring standard.

NOTE

Do not use the shielded RJ-45 connector on this end of the cable as it should be attached on the power supply unit end.

CAUTION

Make sure that the RJ-45 connector is well-crimped. A loose connector can damage the device. Please note that such damage is not covered by the warranty.

- **Step 2**: Assemble cable gland nut, the split sealing grommet and the cable gland threaded coupling onto the pre-terminated cable as shown on the figure below.
- **Step 3**: Insert the split sealing grommet into the cable gland threaded coupling.
- **Step 4**: Insert the RJ-45 connector into the device socket until you hear a click.
- **Step 5**: Screw the cable gland threaded coupling into the port and tighten it. Do not apply excessive force.
- **Step 6**: Tighten the cable gland nut (4). Do not apply excessive force.

6.2.2 Cable Gland Assembly for Optical Cable

Required components are listed below.

1. Optical cable.
2. Optical connector.
3. SFP module.
4. Cable gland:
    - Cable gland nut.
    - Split sealing grommet (with inner diameter 3.2 mm).
    - Cable gland threaded coupling.

Assemble procedure

- **Step 1**: Put the cable gland nut, the split sealing grommet and cable gland threaded coupling onto the pre-terminated optical cable as shown on the figure below.
- **Step 2**: Insert the split sealing grommet into the cable gland threaded coupling.
- **Step 3**: Set the SFP module into the socket until you hear a click.
- **Step 4**: Insert the optical connector into the SFP module.
- **Step 5**: Screw the cable gland threaded coupling into the port and tighten it.
- **Step 6**: Tighten the cable gland nut. Do not apply excessive force.

⚠ **NOTE**

In order to disassemble SFP, please disconnect the optical cable, pull the clip of the SFP module and withdraw the SFP module from the slot.

⚠ **NOTE**

SFP module is not included into the packing list.

6.3 Mounting

6.3.1 Pre-installation

Reqiered tools

- Screwdriwer set.
- Pliers / pipe wrench.
- Wrench set.

Additional equipment

- GPS receiver.
- High magnification binoculars.

❗ **CAUTION**

Before mounting the equipment in an outdoor environment, please make sure that:

- You acknowledge the regulations imposed by the Regulatory Authority for Communications in your country for the radio spectrum to be used.
- You chose known locations for the installation of the links; although InfiNet Wireless devices can also operate in Near-LoS or Non-LoS conditions, to achieve the best performance, it's highly recommended to install the link in locations where Clear-Line-of-Site and clear channels are available.
- You performed link planning using the InfiPLANNER tool (https://infiplanner.infinetwireless.com[9]) to determine the link path profiles, radio equipment placement requirements, etc.
- You met requirements described in the section "Planning considerations" - > "Wireless device placement".

6.3.2 Installation Procedure

1. In case of device with external antenna, to mount and connect an external antenna to the InfiMAN Evolution/ InfiLINK Evolution E5-BSE ODU and E5-STE ODU, proceed as follows:
   a. Mount the antenna(s) according to manufacturer’s instructions;
   b. Connect the ODU V and H N-type interfaces to the antenna(s) with RF coaxial cables and with appropriate connectors. Use cables not longer than 3 m (9.8ft). Tighten the N-type connectors to a torque setting of 1.7 Nm (1.3 lb ft);
   c. Form drip loops near the cable ends at the ODU’s side so that water doesn’t creep towards the ODU connectors;
   d. Weatherproof the N-type connectors (when antenna alignment is complete) using PVC tape and self-amalgamating rubber tape;
   e. Weatherproof the antenna connectors in the same way (unless the antenna manufacturer specifies a different method);
   f. Fix the antenna cables to the supporting structure using site approved methods. Ensure that no undue strain is placed on the ODU or antenna connectors. Ensure that the cables do not flap in the wind, as flapping cables are prone to damage and induce unwanted vibrations in the supporting structure.

NOTE

Any external antenna of the same type and with a maximum gain not greater than those listed below can be used with the InfiMAN Evolution / InfiLINK Evolution E5-BSE in the countries abiding by the FCC rules.

Directivity	Type	Manufacturer	Reference	Stated Gain
Sectorized	Flat-panel, dual orthogonal polarization array	MTI Wireless Edge Ltd.	MT-464047/SVH	16 dBi

If other antenna types than above with Gain +16 dBi or LESS are used with this device these antenna types must be approved by FCC with C2PC application by device manufacturer.
External antenna must be professionally installed pursuant to the section 15.203 of the FCC Rules.

NOTE

Any external antenna of the same type and of gain not greater than the one approved by the FCC can be used with the InfiMAN Evolution/InfiLINK Evolution E5-STE in the countries abiding by the FCC Rules.

[9] https://infiplanner.infinetwireless.com/

Directivity	Type	Manufacturer	Reference	Stated Gain
Directional	Flat-panel, dual orthogonal polarization array	MARS Antennas and RF Systems, Ltd.	MA-WA56-DP28N	28 dBi

External antenna must be professionally installed pursuant to the section 15.203 of the FCC Rules.

CAUTION

In order to prevent device damage make sure that antenna is connected to both N-type connectors with serviceable RF cables before switching on.

1. Install ODU connector facing down using the mounting kit. Do not tighten the fasteners to the end until the alignment is completed.
2. Connect the Cat5e FTP cable with the cable gland to ODU.
3. Perform ODU grounding.
4. Lay the Cat5e FTP cable from ODU to the power supply.
5. Connect the Cat5e FTP cable with a shielded connector covered by a cap to the "OUT" port of the power supply, having previously touched the power supply connector case with FTP cable connector case.

   CAUTION

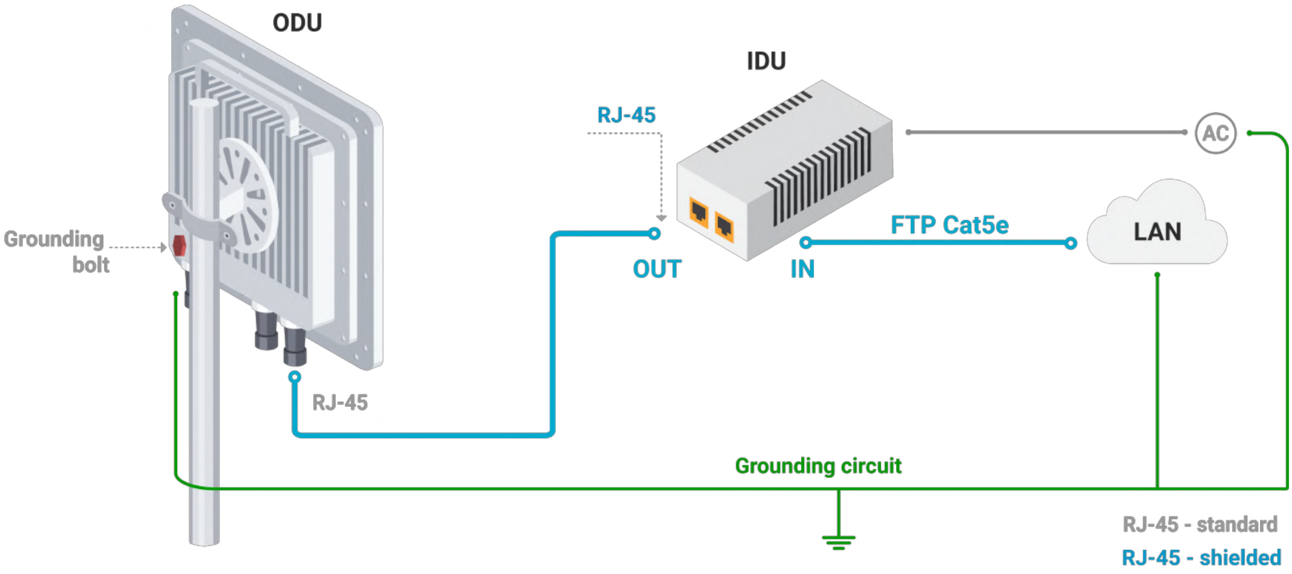
   The power supply must not operate near a direct heat source, near water or in an environment with high humidity. The cables must be connected in such a way to prevent water flow to the power supply connectors.

6. Perform the power supply grounding.
7. Connect the laptop using Cat5e FTP cable to the power supply "IN" port.
8. Connect the power cord to the power supply and then to the power circuit.

   CAUTION

   Use mains supply cords that adhere to safety regulations of the country where the equipment is getting deployed.

Make sure a small loop (at least 10 cable diameters) is provided before the Cat5e FTP cable enter into the building.



CAUTION

Please note that the pressure equalization system in Infinet devices is performed via gas exchange through a cable gland and Ethernet cable jacket with a dry room where the power supply is installed. In order to avoid ODU failure due to moisture entering the device, for example, during the pressure drop during the rain, the cable gland assembly requirements should be met and there are should be no cracks in the Ethernet cable jacket.
In addition, you should avoid the Ethernet cable bending near the ODU and pinching with clamps, that can bring to the pressure equalization system fault between the internal volume of the sealed ODU and the external environment during a sudden air temperature change. This may lead to the leakage and device failures.

6.4 Grounding and Lightning Protection

This section describes factors to be considered when planning the proposed link end sites, including grounding, lightning protection and equipment location for the wireless device, power supply, AUX-ODU-LPU-L and AUX-ODU-LPU-G unit (if installed).

CAUTION

Electro-magnetic discharge (lightning) damage is not covered under warranty. The recommendations in this document, when followed correctly, give the user the best protection from the harmful effects of EMD. However 100% protection is neither implied nor possible.

6.4.1 Grounding and lightning protection recommendations

- The wireless device should be placed on the pole at a height that is at least 1 meter below the top of the pole. In this case, there is a significant probability that the lightning strikes the pole and not the wireless device. The pole should be properly grounded: connected to the building lightning protection circuit according to your local regulations.
- All equipment must be connected at stabilized and surge protected power sources which must be properly grounded.

- The end of the FTP service cable that is connected to the power supply should be assembled with a shielded RJ-45 connector. The other end of the FTP service cable (connected to the wireless device) should be assembled with unshielded (standard) RJ-45 connector.
- The power supply is grounded via a three-conductor power cord and a grounded socket.
- AUX-ODU-LPU-L, AUX-ODU-LPU-G and wireless device grounding is performed using grounding bolt.
- Antenna pole and wireless device should be connected to the common ground ring. Grounding cables should be no less than 10AWG thick and must use corrosion-resistant connectors.

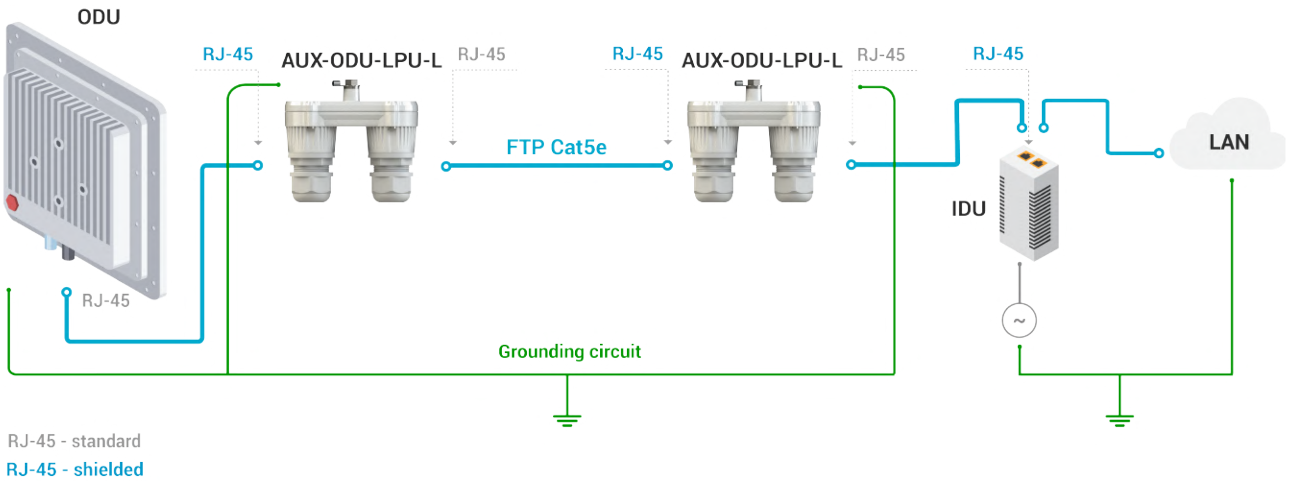
6.4.2 Requirements to the lightning protection unit AUX-ODU-LPU-L location

AUX-ODU-LPU-L is an optional accessory which may be used to serve as a line protection unit for the ODU and for the indoor network equipment connected to the Ethernet port of the IDU. AUX-ODU-LPU-L should be properly assembled, mounted and grounded.

General recommendations for installations of lightning protection units:

- Install the lightning protection unit on both ends of the cable to protect both the outdoor and the indoor unit. The purpose of the LPU at the top is to protect the ODU from a surge of lightning strike which can hit the long FTP cable run along the height of the pole or on the roof of the building. The purpose of the LPU at the bottom is to protect the IDU and customer equipment.
- Use the lightning protection unit to protect all circuits for signal transmission and power supply (video, audio, management signals, Ethernet, etc.)
- Regularly (especially before the periods with high thunderstorm activity) check the integrity of lightning protection units, grounding elements and bonding conductors.
- The ports of the AUX-ODU-LPU-L device are symmetrical, i.e. the correspondence of ports position to the external unit and the power supply does not matter.

Make sure to install the two LPU devices as shown in the scheme below.



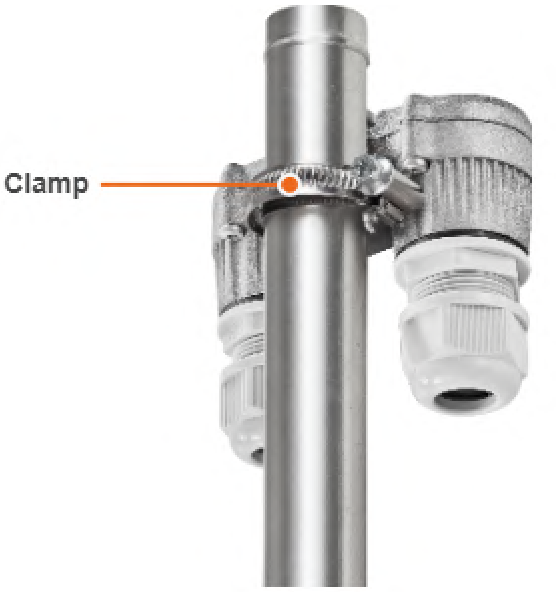
11 Figure - Connection scheme

CAUTION

Please note grounding cables should not be connected to the mast. All devices must use separate grounding cable that should be connected to the grounding circuit. The best scenario is when grounding cables are lined parallel to the Ethernet cable.

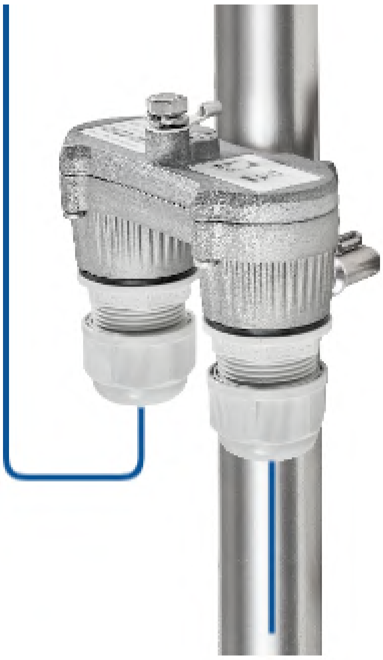
AUX-ODU-LPU-L Mounting

AUX-ODU-LPU-L is installed on a mast, using clamp. Attach the grounding cable (min cross-section 2.5 mm^2) to the case, using grounding bolt.



12 Figure - AUX-ODU-LPU-L Mounting

During AUX-ODU-LPU-L mounting it is necessary to provide a small loop of the FTP cable that should be below the cable gland. This ensures that water is not constantly channeled towards the connector. It will also serve as a cable compensation for the cable linear expansion as the temperature difference result.



13 Figure - Cable loop

CAUTION

Missing or bad grounding may leave the unit vulnerable to lightning damage.

AUX-ODU-LPU-L Cable Ggland Assembly

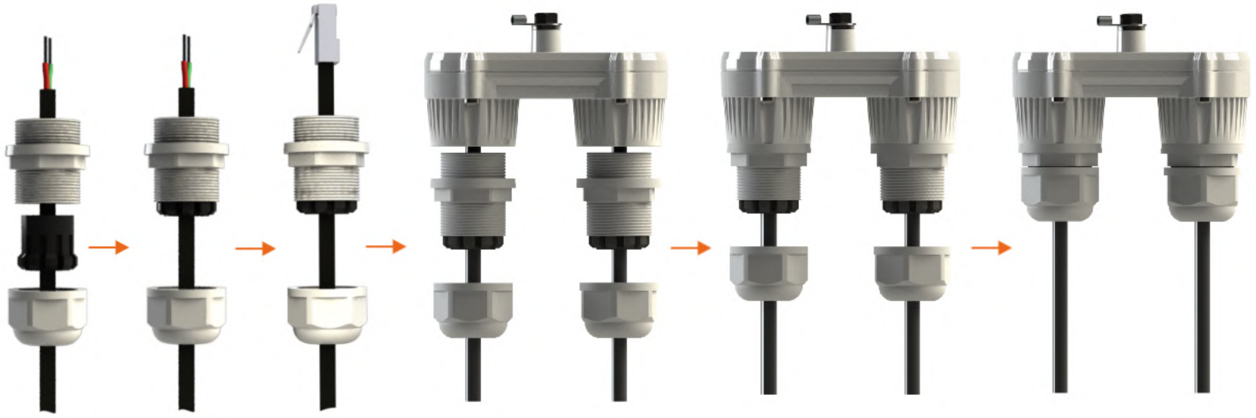
In order to ensure that the cable gland remains sealed under any environmental conditions, please, follow the assembly sequence according to the procedure below:

- **Step 1**: Insert the sealing insert into the clamping claw.
- **Step 2**: Assemble the cable gland by putting the thread-lock sealing nut, clamping claw with sealing insert and body onto the cable as shown on the figure.
- **Step 3**: Insert the clamping claw with sealing insert into the body as shown on the figure.
- **Step 4**: Crimp the standard RJ-45 connector onto the cable using crimping tool. Pin-out scheme: T568B wiring standards.

CAUTION

Make sure that the RJ-45 connector is well-crimped. A loose connector can damage the device. Please note that such damage is not covered by the warranty.

- **Step 5**: Insert the RJ-45 connector into the corresponding socket until you hear a click.
- **Step 6**: Screw the cable gland body into the port and tighten it. Do not apply excessive force.
- **Step 7**: Tighten the thread-lock sealing nut. Do not apply excessive force.



14 Figure - Cable gland assembly

6.4.3 Requirements to the lightning protection unit AUX-ODU-LPU-G location

AUX-ODU-LPU-G is an optional accessory which may be used to serve as a line protection unit for the ODU and for the indoor network equipment connected to the Ethernet port of the IDU.

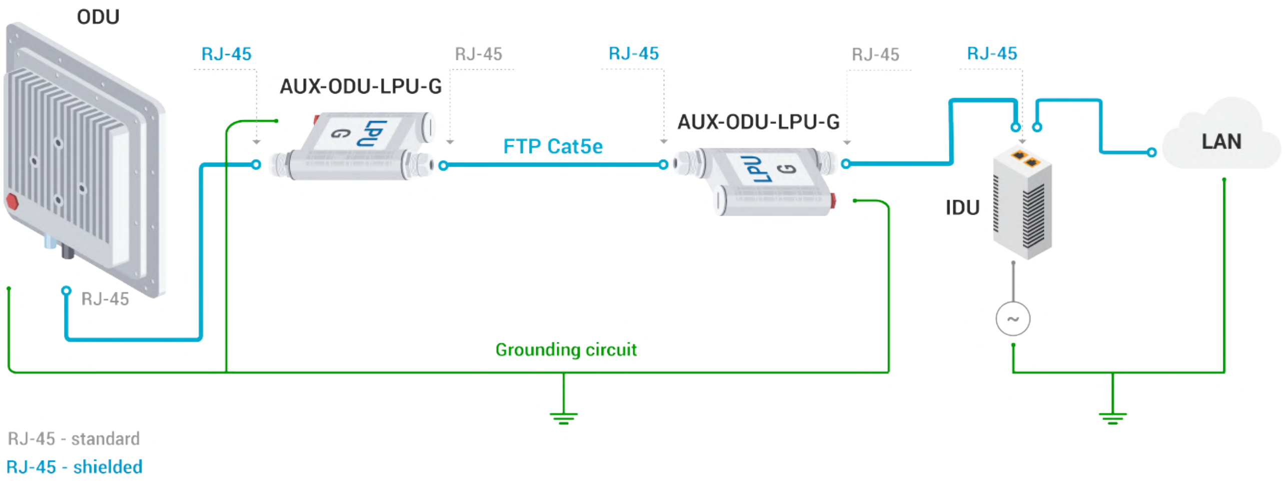
AUX-ODU-LPU-G should be properly assembled, mounted and grounded.

General recommendations for installations of lightning protection units:

- Install the lightning protection unit on both ends of the cable to protect both the outdoor and the indoor unit. The purpose of the LPU at the top is to protect the ODU from a surge of lightning strike which can hit the long FTP cable run along the height of the pole or on the roof of the building. The purpose of the LPU at the bottom is to protect the IDU and customer equipment.
- Use the lightning protection unit to protect all circuits for signal transmission and power supply (video, audio, management signals, Ethernet, etc.)
- Regularly (especially before the periods with high thunderstorm activity) check the integrity of lightning protection units, grounding elements and bonding conductors.

Make sure to install the two LPU devices in the correct polarity, as shown in the diagram:

- Top LPU with "ETH OUT" facing the ODU.
- Bottom LPU with "ETH OUT" facing the IDU.
- LPU units connected to each other via "ETH IN".



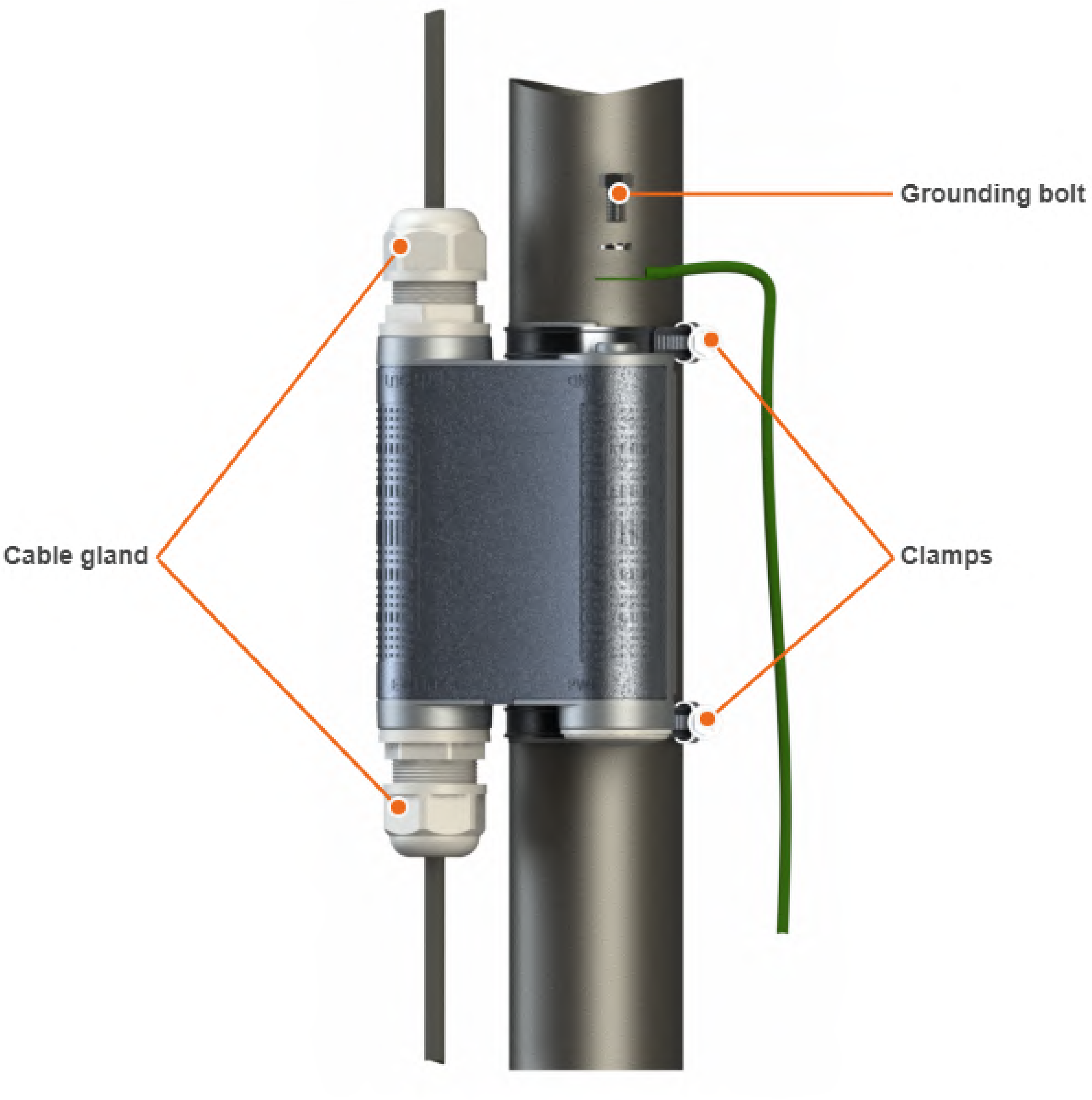
15 Figure - AUX-ODU-LPU-G Assembly Scheme

CAUTION

Please note grounding cables should not be connected to the mast. All devices must use separate grounding cable that should be connected to the grounding circuit. The best scenario is when grounding cables are lined parallel to the Ethernet cable.

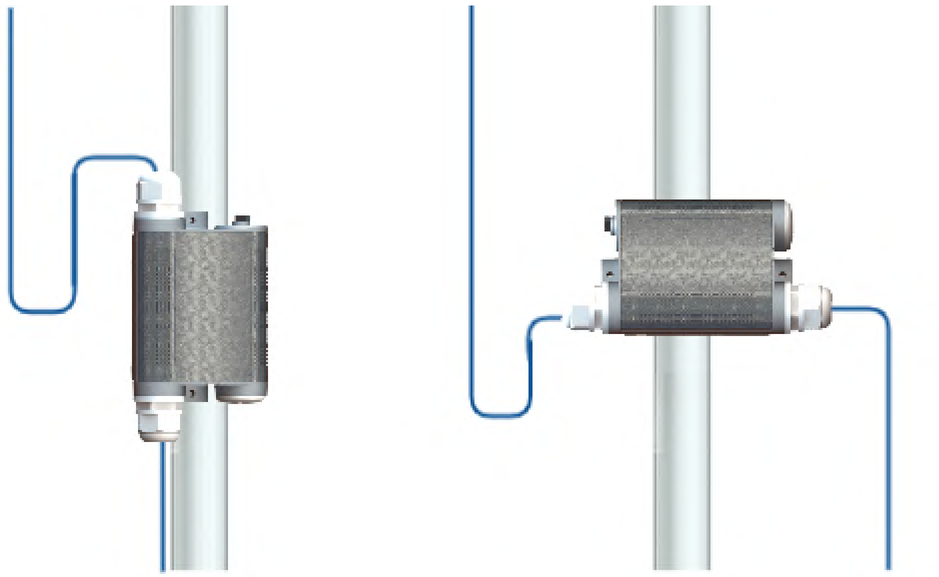
AUX-ODU-LPU-G Mounting

AUX-ODU-LPU-G can be installed on a pole, using hose clamps. Attach the grounding cable (min cross-section 2.5 mm^2) to the case, using grounding bolt.



16 Figure - AUX-ODU-LPU-G Mounting

During AUX-ODU-LPU-G mounting it is necessary to provide a small loop of the FTP Cat5e cable that should be below the cable gland. These ensure that water is not constantly channeled towards the connectors. It will also serve as a cable compensator for the cable linear expansion as the temperature difference result.



17 Figure - Cable loop

CAUTION

Missing or bad grounding may leave the unit vulnerable to lightning damage.

AUX-ODU-LPU-G Cable Gland Assembly

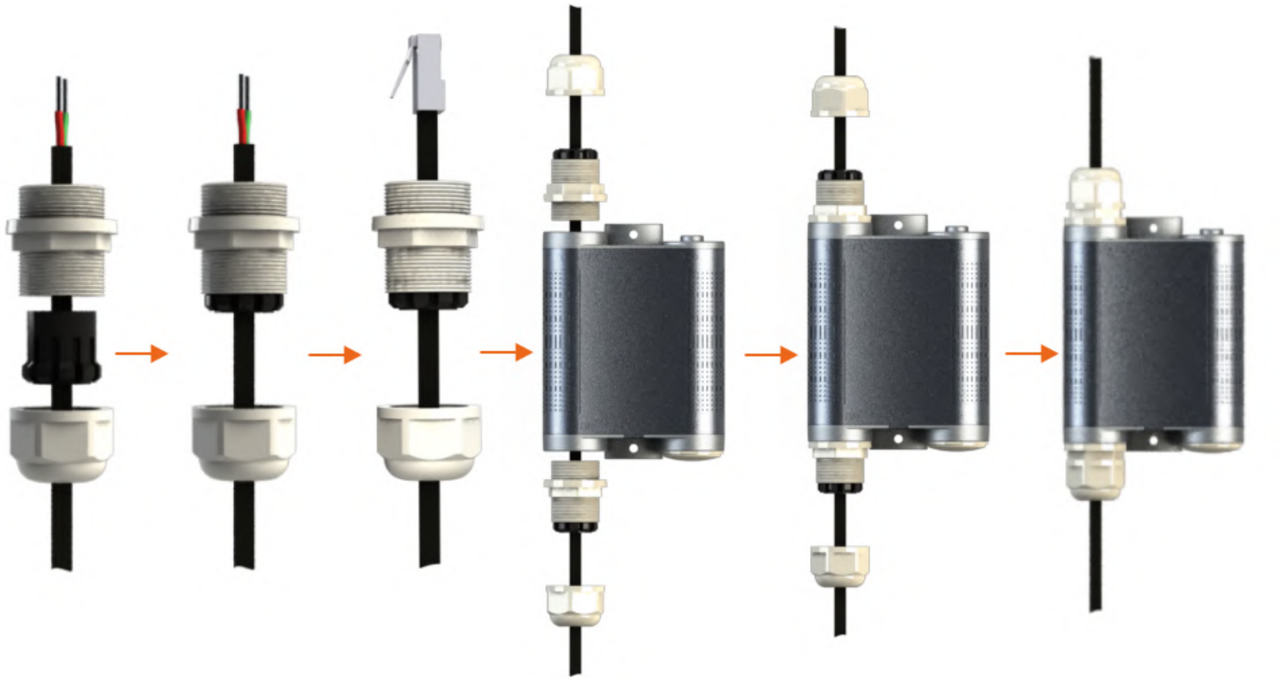
In order to ensure that the cable gland remains sealed under any environmental conditions, please, follow the assembly sequence according to the procedure below:

- **Step 1**: Insert the sealing insert into the clamping claw.
- **Step 2**: Assemble the cable gland by putting the thread-lock sealing nut, clamping claw with sealing insert and body onto the cable as shown on the figure.
- **Step 3**: Insert the clamping claw with sealing insert into the body as shown on the figure.
- **Step 4**: Crimp the standard RJ-45 connector onto the cable using crimping tool. Pin-out scheme: T568B wiring standards.

CAUTION

Make sure that the RJ-45 connector is well-crimped. A loose connector can damage the device. Please note that such damage is not covered by the warranty.

- **Step 5**: Insert the Rj-45 connector into the corresponding socket until you hear a click.
- **Step 6**: Screw the cable gland body into the port and tighten it. Do not apply excessive force.
- **Step 7**: Tighten the thread-lock sealing nut. Do not apply excessive force.



18 Figure - AUX-ODU-LPU-G Cable Gland Assembly Scheme

6.5 Antenna Alignment

6.5.1 Rough alignment

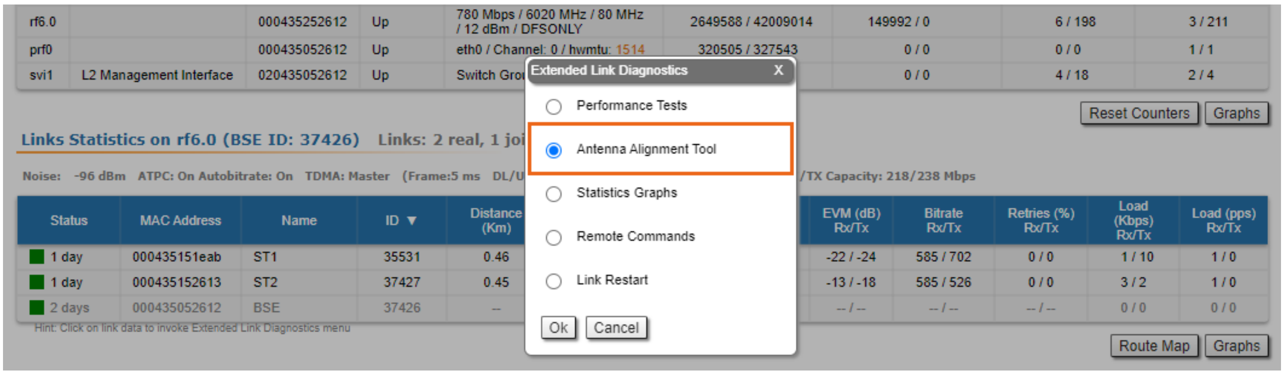
Using the azimuth and elevation values computed by the link planning tool[10] roughly position the antenna (in each location) to detect the opposite system signal. Directly before installing the devices we recommend to set up the maximum output power value. If the link cannot be established, try to switch the bitrate to the minimum value and narrowing the channel width. Assess the link establishment and its quality using the LED indicator on the device case. LED indication are detaily described in the Hardware Platform (see page 6) section. For more accurate alignment, use the alignment tool built into the device web interface.

6.5.2 Precise alignment

It is recommended to have two teams prepared for alignment procedure, each team with at least two installers: one should notisy the signal values and communicate with the remote side, the other should make the adjustments with the device. After the initial approximate alignment (link up), the antenna with the lowest gain should be locked into position.

Both teams should use the Antenna Alignment Tool in the Device Status section of the web GUI.

[10] https://infiplanner.infinetwireless.com/



rf6.0		000435252612	Up	780 Mbps / 6020 MHz / 80 MHz / 12 dBm / DFSONLY	2649588 / 42009014	149992 / 0	6 / 198	3 / 211
prf0		000435052612	Up	eth0 / Channel: 0 / hwmtu: 1514	320505 / 327543	0 / 0	0 / 0	1 / 1
svi1	L2 Management Interface	020435052612	Up	Switch Gro		0 / 0	4 / 18	2 / 4

Links Statistics on rf6.0 (BSE ID: 37426) Links: 2 real, 1 joi

Noise: -96 dBm ATPC: On Autobitrate: On TDMA: Master (Frame:5 ms DL/U /TX Capacity: 218/238 Mbps

Status	MAC Address	Name	ID ▼	Distance (Km)	EVM (dB) Rx/Tx	Bitrate Rx/Tx	Retries (%) Rx/Tx	Load (Kbps) Rx/Tx	Load (pps) Rx/Tx
🟩 1 day	000435151eab	ST1	35531	0.46	-22 / -24	585 / 702	0 / 0	1 / 10	1 / 0
🟩 1 day	000435152613	ST2	37427	0.45	-13 / -18	585 / 526	0 / 0	3 / 2	1 / 0
🟩 2 days	000435052612	BSE	37426	--	-- / --	-- / --	-- / --	0 / 0	0 / 0

Hint: Click on link data to invoke Extended Link Diagnostics menu

Extended Link Diagnostics

○ Performance Tests
● Antenna Alignment Tool
○ Statistics Graphs
○ Remote Commands
○ Link Restart

The team at the antenna which has the highest gain will click on the "Start Test" button and start to change the azimuth slowly while watching the signal indicators

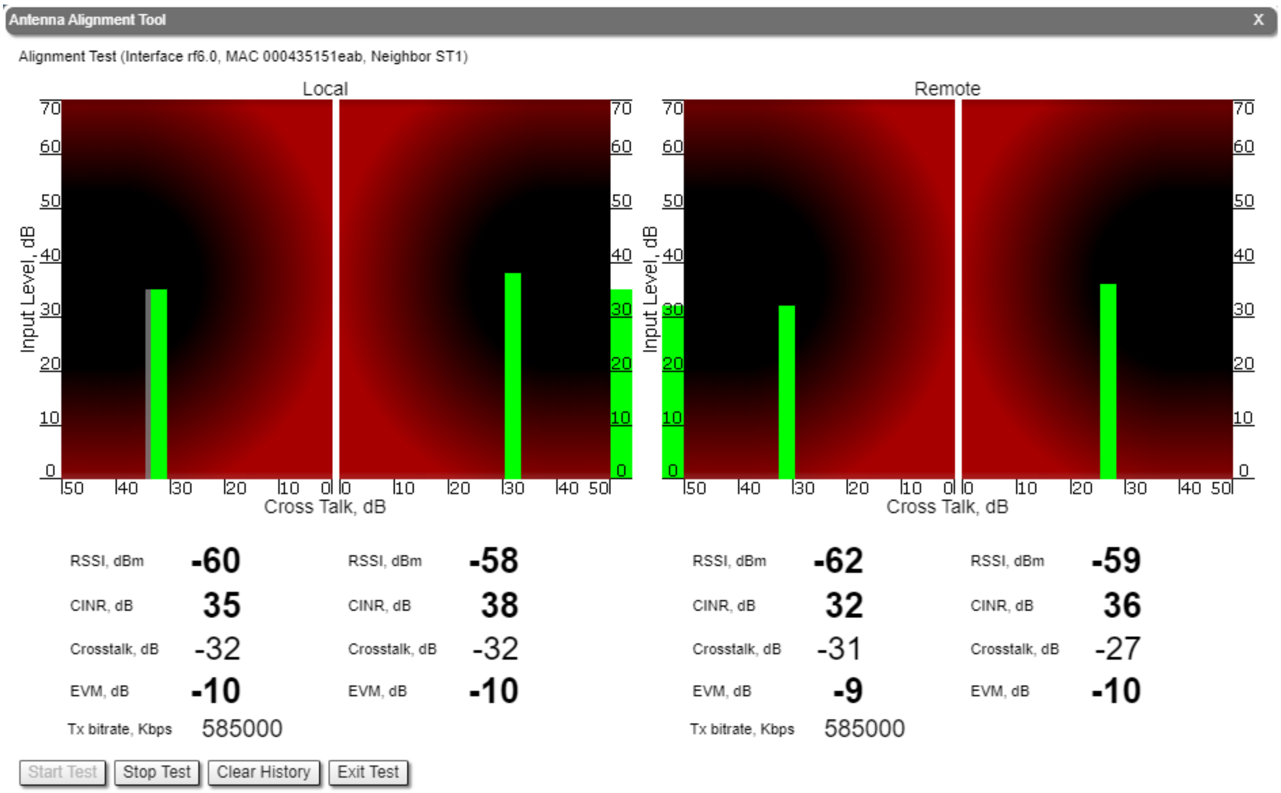
- As soon as the best signal has been found (Input Signal stripes must be located in the black area, closer to its center), the antenna must be locked into that position
- The same action will be performed for the elevation, and the antenna must be locked into the final position where both elevation and azimuth provide the best signal, according to the indicators provided by the antenna alignment tool:
  - EVM: higher than 21 in absolute value.
  - Signal level to interference and noise: higher than 28 dB.
  - Retries: lower than 5 %.

CAUTION

No contact should be made with the antennas during signal reading because the human body can affect the radiation pattern of the antenna and signal readings.

The main parameters displayed in the alignment tool:

- RSSI - indicates the power level of the received radio signal, optimal parameter value -60 ... -40 dBm.
- CINR - input signal level to noise + interference indicator, >=28 dB.
- Crosstalk - indicates how much vertically and horizontally polarized signals influence each other, >20 dB in absolute value.
- 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 in absolute value. Some old firmware had EVM value positive, but most the firmware has negative value, so for the troubleshooting, evaluate the absolute EVM value).
- Tx bitrate - displays the current bitrate for the remote and local units (measured in Kbps).



Antenna Alignment Tool

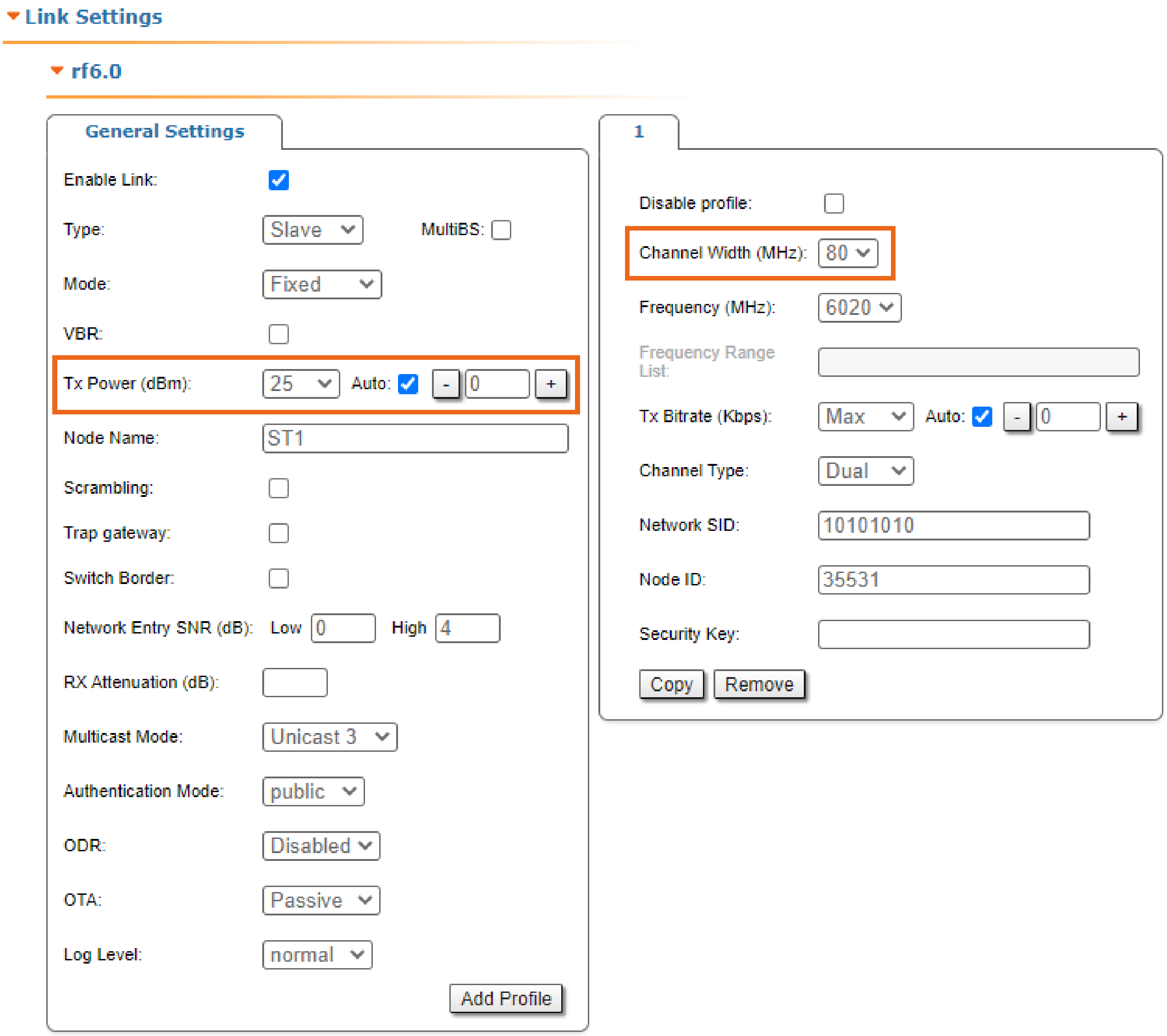
Alignment Test (Interface rf6.0, MAC 000435151eab, Neighbor ST1)

RSSI, dBm	-60	RSSI, dBm	-58	RSSI, dBm	-62	RSSI, dBm	-59
CINR, dB	35	CINR, dB	38	CINR, dB	32	CINR, dB	36
Crosstalk, dB	-32	Crosstalk, dB	-32	Crosstalk, dB	-31	Crosstalk, dB	-27
EVM, dB	-10	EVM, dB	-10	EVM, dB	-9	EVM, dB	-10
Tx bitrate, Kbps	585000			Tx bitrate, Kbps	585000		

As soon as the antennas have been precisely alignment, set the "auto" option for Tx power and bitrate at both units and select values in accordance with the EIRP limitations.

Depending on the values for SNR, RSSI, retries and current bitrate, change the following parameters:

- Decrease/increase the Tx power level (keeping the auto option checked) to have the SNR at around 25 dB and the RSSI at around -55 dBm.
- Decrease the bandwidth to lower the noise and to increase the SNR to above 20 dB.



Link Settings

rf6.0

General Settings

Enable Link:	☑
Type:	Slave MultiBS: □
Mode:	Fixed
VBR:	□
Tx Power (dBm):	25 Auto: ☑ - 0 +
Node Name:	ST1
Scrambling:	□
Trap gateway:	□
Switch Border:	□
Network Entry SNR (dB):	Low 0 High 4
RX Attenuation (dB):	
Multicast Mode:	Unicast 3
Authentication Mode:	public
ODR:	Disabled
OTA:	Passive
Log Level:	normal

Add Profile

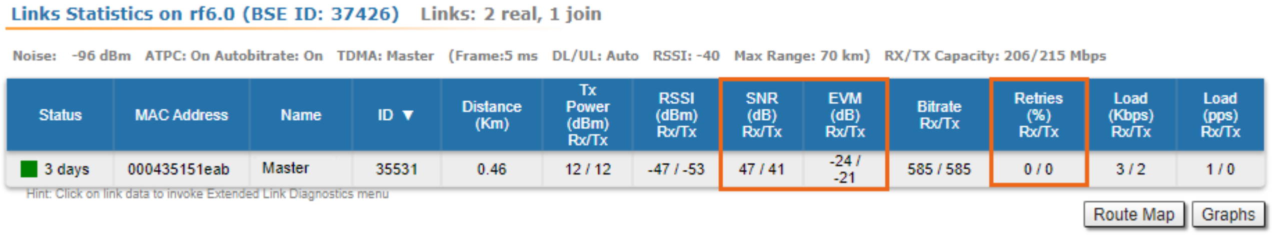
1

Disable profile:	□
Channel Width (MHz):	80
Frequency (MHz):	6020
Frequency Range List:	
Tx Bitrate (Kbps):	Max Auto: ☑ - 0 +
Channel Type:	Dual
Network SID:	10101010
Node ID:	35531
Security Key:	

Copy Remove

Wireless link statistics

- Let's check the link parameters. Go to the Device Status section and in the Link Statistics, check the following parameters:
  - Retries Rx/Tx: maximum 5 %.
  - EVM Rx/Tx: not less than 21 dB in absolute value.
  - SNR Rx/Tx: not less than 27 dB.



Links Statistics on rf6.0 (BSE ID: 37426) Links: 2 real, 1 join

Noise: -96 dBm ATPC: On Autobitrate: On TDMA: Master (Frame:5 ms DL/UL: Auto RSSI: -40 Max Range: 70 km) RX/TX Capacity: 206/215 Mbps

Status	MAC Address	Name	ID ▼	Distance (Km)	Tx Power (dBm) Rx/Tx	RSSI (dBm) Rx/Tx	SNR (dB) Rx/Tx	EVM (dB) Rx/Tx	Bitrate Rx/Tx	Retries (%) Rx/Tx	Load (Kbps) Rx/Tx	Load (pps) Rx/Tx
🟩 3 days	000435151eab	Master	35531	0.46	12 / 12	-47 / -53	47 / 41	-24 / -21	585 / 585	0 / 0	3 / 2	1 / 0

Hint: Click on link data to invoke Extended Link Diagnostics menu

Route Map Graphs

If these conditions are met and the maximum bitrate is reached, the wireless connection quality is good. Otherwise, use the diagnostic tools described in the Device Status(see page 64) article.

7 Operation & Administration

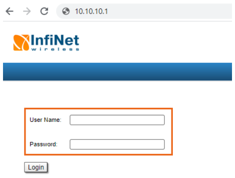
7.1 Web GUI Access

> **NOTE**
>
> Connecting third-party equipment via Ethernet (switches, PCs), make sure the PoE, Energy Efficient Ethernet and Green Ethernet functions are disabled on the network interfaces connected to Infinet devices.

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 the default address: 10.10.10.1/24.

> **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:

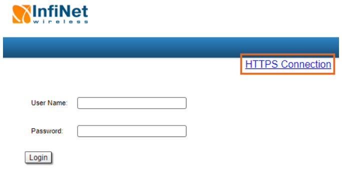


19 Figure - GUI login

> **NOTE**
>
> Please change the credentials you have just inserted with a permanent username and password for it after the first log in. In order to change the credentials proceed to the "Basic Settings" - "System Settings (see page 85)" section.

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 (see page 129) of Web interface). The «HTTPS Connection» link is available in the right side of the login form:

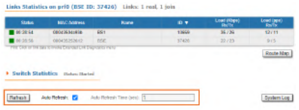


20 Figure - HTTPS connection

7.2 Device Status

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



Links Statistics on prf0 (BSE ID: 37426) Links: 1 real, 1 join

Status	MAC Address	Name	ID ▼	Load (Kbps) Rx/Tx	Load (pps) Rx/Tx
🟩 00:20:54	00043594a898	BS1	13659	36 / 36	12 / 11
🟩 00:20:56	000435252612	BSE	37426	22 / 23	9 / 5

21 Figure - Refresh option

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

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 or dropped.

7.2.1 Interface Statistics

The software version is displayed in the right side of Interface Statistics section (for example: TDMAv2.1.26).

In case of connection to the AUX-ODU-SYNC synchronization unit, the number of visible GPS/GLONASS satellites will be displayed as well as the current device synchronization status:

- "*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
- "*Lost Sync*": the connecting to the AUX-ODU-SYNC was lost
- "*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)

Following parameters are displayed in the "Interface Statistics" section:

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. • Ethernet interface: • 10,100 or 1000 Mbps; • Half or full duplex mode - red value of this parameter informs that transmission is performed in a half-duplex mode. • Radio interface: • Bitrate; • Operating frequency - red value of this parameter indicates an absence of data transmission due to the spectrum scanning by the DFS tool; • Channel width; • TX Power - red value for this parameter may indicate a problem with the transceiver's hardware.; • DFS tool state; • Greenfield mode. • SVI: • Switch group number. • PRF interface: • Parent; • Channel number; • Frame size - red value of this parameter means impossibility to set the optimal size due to external limitation (MTU value on the switch port). • Vlan interface: • Parent; • Vlan ID; • Selected vlan interface operation standard.
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

Parameter	Description
Load	• Displays the packet flow through each interface in real-time (for the system and the data traffic)

7 Table - Interface Statistics

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

22 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. If you are not sure you want to permanently delete all statistics of the device for previous periods without the possibility to recover, click the «**Cancel**» button.

7.2.2 Links Statistics on rf6.0

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)
- Operational mode of the unit (Master/Slave)
- For Master - current TDMA parameters:
    - Time slot duration (in microseconds)
    - Downlink percentage of the time slot
    - Maximum RSSI level (in dBm)
    - Maximum operational distance (in kilometers)
    - RX/TX Capacity

Parameter	Description
Status	• Gives a color indication for the wireless connection quality with the neighbor unit: ◦ Red: poor connection ◦ Yellow: good connection ◦ Green: excellent connection • Link Uptime. Displays the link uptime • F – relevance of remote unit firmware (optional). Idicates that the remote unit has the older firmware than the local one • ? – system password of the remote unit (optional). Idicates that the remote unit has not the system password • E – Ethernet port status on the remote device (optional). Indicates that the remote device Ethernet port is flapping
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) • Deflection angle from the main antenna direction towards the subscriber terminal, in the column "Distance" (only for sector base station with "Q" index, which have antanna with beamforming technology support).
Tx Power	• Displays the power level of the Tx and Rx signals of the neighbor unit (in dBm)
RSSI	• Displays the received signal level in dBm, the optimal value is in the range from -60 to -40. "*" – indicates the difference in the signals power of the vertical and horizontal polarizations
SNR	• Displays the ratio of the useful signal power to the noise power for the input and output signals at the neighbor unit (in dB). For radio link stable operation, the SNR value must in the range of 12-50 dB, higher modulation are available at values of 27-50 dB
EVM	• Displays the input signal quality in dB. For stable operation, its absolute value should be as high as possible - not less than 21 dB
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

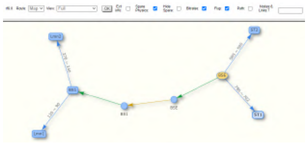
Parameter	Description
Errors	• Displays the percentage of Tx and Rx errors of the neighbor unit
Load	• Displays the number of kbps and packets that are going inbound and outbound the radio interface of the neighbor unit (main data)

8 Table - Wireless Links Statistics

By clicking the "**Route Map**" button in the right corner under the Link Statistics table you can get the MINT topology schematic map with the visualization of the active and alternative routes to each node.

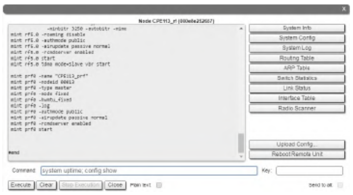
23 Figure - Route map

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



24 Figure - Schematic map

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



Node CPE113_rf (000e8e252607)

```
              -minbitr 3250 -autobitr -mimo
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
mint rf5.0 tdma mode=slave vbr start

mint prf0 -name "CPE113_prf"
mint prf0 -nodeid 00013
mint prf0 -type master
mint prf0 -mode fixed
mint prf0 -hwmtu_fixed
mint prf0 -log
mint prf0 -authmode public
mint prf0 -airupdate passive normal
mint prf0 -rcmdserver enabled
mint prf0 start

#end
```

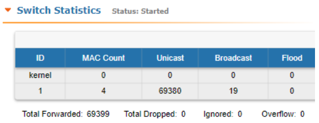
Command: system uptime; config show

25 Figure - Remote commands

Detailed information about options in this tool is described in the "Command Line(see page 137)" section.

7.2.3 Switch Statistics

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



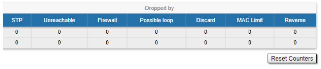
Switch Statistics Status: Started

ID	MAC Count	Unicast	Broadcast	Flood
kernel	0	0	0	0
1	4	69380	19	0

Total Forwarded: 69399 Total Dropped: 0 Ignored: 0 Overflow: 0

26 Figure - Switch Statistics

In addition, this section displays in real time statistics on dropped packets from the last configuration update.



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

27 Figure - Switch Statistics

Total forwarded, dropped, ignored and buffer overflow packets are displayed in real-time below the table.

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

Switch Statistics parameters:

Parameter	Description
ID	• The ID of a switch group or Kernel
MAC Count	• The MAC addresses number involved in data transmission within this switch group
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
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

Parameter	Description
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
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)

9 Table - Switch statistics parameters

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

28 Figure - System log

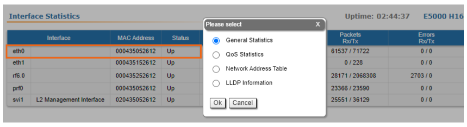
The "System Log" section allows browsing the unit's system log. It is possible to minimize/enlarge the system log window by clicking the buttons:

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.

7.2.4 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:



Interface Statistics

Uptime: 02:44:37 E5000 H16

Interface		MAC Address	Status	Packets Rx/Tx	Errors Rx/Tx
eth0		000435052612	Up	61537 / 71722	0 / 0
eth1		000435152612	Up	0 / 228	0 / 0
rf6.0		000435252612	Up	28171 / 2068308	2703 / 0
prf0		000435052612	Up	23366 / 23590	0 / 0
svi1	L2 Management Interface	020435052612	Up	25551 / 36129	0 / 0

Please select

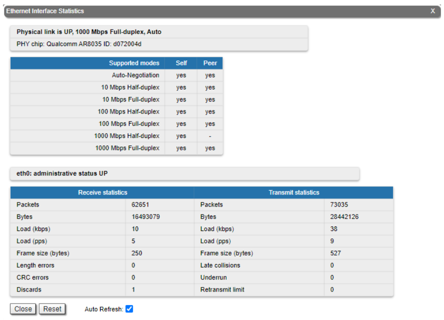
- ● General Statistics
- ○ QoS Statistics
- ○ Network Address Table
- ○ LLDP Information

29 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.

For Ethernet interfaces information about current status, operational mode and load statistics is available.



Ethernet Interface Statistics

Physical link is UP, 1000 Mbps Full-duplex, Auto

PHY chip: Qualcomm AR8035 ID: d072004d

Supported modes	Self	Peer
Auto-Negotiation	yes	yes
10 Mbps Half-duplex	yes	yes
10 Mbps Full-duplex	yes	yes
100 Mbps Half-duplex	yes	yes
100 Mbps Full-duplex	yes	yes
1000 Mbps Half-duplex	yes	-
1000 Mbps Full-duplex	yes	yes

eth0: administrative status UP

Receive statistics		Transmit statistics	
Packets	62651	Packets	73035
Bytes	16493079	Bytes	28442126
Load (kbps)	10	Load (kbps)	38
Load (pps)	5	Load (pps)	9
Frame size (bytes)	250	Frame size (bytes)	527
Length errors	0	Late collisions	0
CRC errors	0	Underrun	0
Discards	1	Retransmit limit	0

Auto Refresh: ☑

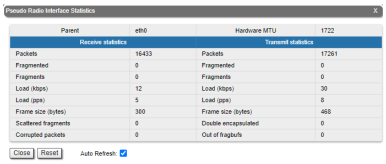
30 Figure - General Statistics Ethernet

Rx and Tx statistics parameters:

Parameter	Description
Receive statistics	
Packets	The total number of received packets
Bytes	The sum of lengths of all good Ethernet frames received
Load (kbps)	The link load, Kbit/s
Load (pps)	The link load, packets per second
Frame size (bytes)	The frame size in bytes
CRC errors	Total frames received with a CRC error
Length errors	Total abnormal length frames received
Discards	Number of dropped frames
Transmit statistics	

Parameter	Description
Packets	The total number of transmitted packets
Bytes	The sum of lengths of all good Ethernet frames sent
Load (kbps)	The link load, Kbit/s
Load (pps)	The link load, packets per second
Frame size (bytes)	The frame size in bytes
Late collisions	The number of times a collision is detected later than 512 bits-times into the transmission of a frame
Underrun	The number of times the transmitter's packet processing rate exceeded the switch capabilities
Retransmit limit	Packets dropped due to queue overflow

For the pseudo-radio interface information about parent interface, MTU value and load statistics is available.



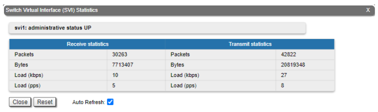
Parent	eth0	Hardware MTU	1722
Receive statistics		Transmit statistics	
Packets	16433	Packets	17261
Fragmented	0	Fragmented	0
Fragments	0	Fragments	0
Load (kbps)	12	Load (kbps)	30
Load (pps)	5	Load (pps)	8
Frame size (bytes)	300	Frame size (bytes)	468
Scattered fragments	0	Double encapsulated	0
Corrupted packets	0	Out of fragbufs	0

31 Figure - General Statistics PRF

Parameter	Description
Receive statistics	
Packets	Number of correctly received packets
Fragmented	Number of fragmented packets
Fragments	Number of fragments
Load (kbps)	The link load, Kbit/s
Load (pps)	The link load, packets per second
Frame size (bytes)	The frame size in bytes
Scattered fragments	Number of frames where one or several fragments were lost, the frame cannot be restored

Parameter	Description
Corrupted packets	Number of frames with the wrong length or structure
Transmit statistics	
Packets	Number of correctly transmitted packets
Fragmented	Number of fragmented packets
Fragments	Number of fragments
Load (kbps)	The link load, Kbit/s
Load (pps)	The link load, packets per second
Frame size (bytes)	The frame size in bytes
Double encapsulated packets	Number of frames with double encapsulation
Out of fragbufs	Number of errors as a result of frame assembly buffer overflow due to too many fragments (neighbors) sources

For the SVI interface information about current status, RX and TX staistics is available.



Switch Virtual Interface (SVI) Statistics

svi1: administrative status UP

Receive statistics		Transmit statistics	
Packets	30263	Packets	42822
Bytes	7713407	Bytes	20819348
Load (kbps)	10	Load (kbps)	27
Load (pps)	5	Load (pps)	8

32 Figure - General Statistics SVI

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.

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 (see page 125)" section.

Channal	Priority
BACKGROUND	16
REGULAR Best Effort	15
BUSINESS6	14
BUSINESS5	13
BUSINESS4	12
BUSINESS3	11
BUSINESS2	10
BUSINESS1	9
QOS4	8
QOS3	7
QOS2	6
QOS1	5
VIDEO2	4
VIDEO	3
VOICE	2
CONTROL	1
NETCRIT	0

10 Table - MINT priorities

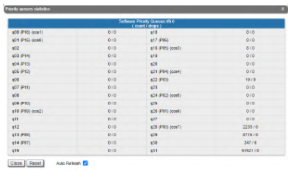
Transparent packet prioritization is a **WANFleX** feature which allows QM manager to transparently map 802.1p/TOS/DSCP priority to MINT priority for the ease of deployment.

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

MINT Priority	Traffic Types (802.1p)	dot1p	TOS	DSCP Name	DS Field Value
16 BACKGROUND	Background	1			
15 REGULAR Best Effort	Best Effort	0	0	CS0	0
14 BUSINESS6			1	CS1, AF11-13	8, 10
13 BUSINESS5					12, 14
12 BUSINESS4			2	CS2, AF21-23	16, 18
11 BUSINESS3					20, 22
10 BUSINESS2			3	CS3, AF31-33	24, 26
9 BUSINESS1	Excellent Effort	2			28, 30
8 QOS4			4	CS4, AF41-43	32
7 QOS3					34
6 QOS2					36
5 QOS1	Critical Applications	3			38
4 VIDEO2	Video	4	5	CS5, EF	40, 42
3 VIDEO					44, 46
2 VOICE	Voice	5	6	CS6	48, 50
1 CONTROL	Internetwork Control	6			52, 54
0 NETCRIT	Network Control	7	7	CS7	56, 58, 60, 62

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

This section displays the number of inbound packets to each priority queue and the number of dropped packets. Of the 32 priority queues 17 are available for user configuration (from P00 to P16), where 0 is the highest priority. The rest are reserved for the system. Packets with 802.1p priority are distributed to queues with "cosX" values.



Priority queues statistics

Software Priority Queues rf5.0 (count / drops)			
q00 (P16) (cos1)	0 / 0	q16	0 / 0
q01 (P15) (cos0)	0 / 0	q17 (P06)	0 / 0
q02	0 / 0	q18 (P05) (cos3)	8 / 0
q03 (P14)	0 / 0	q19	0 / 0
q04 (P13)	0 / 0	q20	0 / 0
q05 (P12)	0 / 0	q21 (P04) (cos4)	0 / 0
q06	0 / 0	q22 (P03)	19 / 9
q07 (P11)	0 / 0	q23	0 / 0
q08	0 / 0	q24 (P02) (cos5)	0 / 0
q09 (P10)	0 / 0	q25	0 / 0
q10 (P09) (cos2)	0 / 0	q26 (P01) (cos6)	0 / 0
q11	0 / 0	q27	0 / 0
q12	0 / 0	q28 (P00) (cos7)	2233 / 0
q13 (P08)	0 / 0	q29	8719 / 0
q14 (P07)	0 / 0	q30	247 / 8
q15	0 / 0	q31	67621 / 0

33 Figure - QoS Statistics

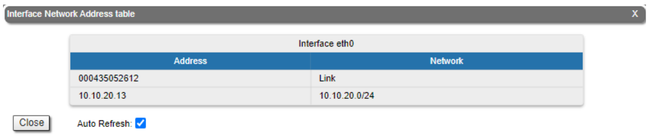
By clicking the «**Close**» button, you return to the "Device Status" page.

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.



Interface eth0

Address	Network
000435052612	Link
10.10.20.13	10.10.20.0/24

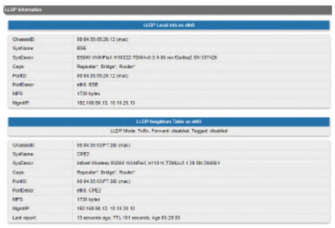
34 Figure - The Network Address Table for the local unit

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.



LLDP Local info on eth0

ChassisID:	00:04:35:05:28:12 (mac)
SysName:	BSE
SysDescr:	E5000 WANFleX H16S22-TDMAv0.3.9-80 rev:f2a4ba2 SN:337428
Caps:	Repeater*, Bridge*, Router*
PortID:	00:04:35:05:28:12 (mac)
PortDescr:	eth0, BSE
MFS:	1728 bytes
MgmtIP:	192.168.98.13, 10.10.20.13

LLDP Neighbors Table on eth0

LLDP Mode: TxRx, Forward: disabled, Tagged: disabled

ChassisID:	00:04:35:03:F7:DD (mac)
SysName:	CPE2
SysDescr:	Infinet Wireless R5000 WANFleX H11S11.TDMAv0.1.38 SN:268061
Caps:	Repeater*, Bridge*, Router*
PortID:	00:04:35:03:F7:DD (mac)
PortDescr:	eth0, CPE2
MFS:	1728 bytes
MgmtIP:	192.168.98.12, 10.10.20.12
Last report:	13 seconds ago, TTL 181 seconds, Age 05:29:33

35 Figure - LLDP Information

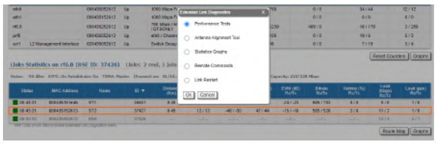
By clicking the «**Close**» button, you return to the "Device Status" page.

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

7.2.5 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 rf6.0" section:



36 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.

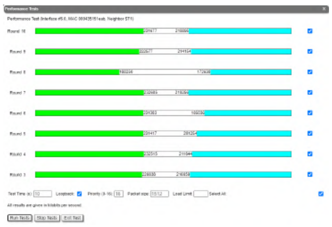
The "Performance tests" tool generates traffic between the devices and displays the channel throughput for the traffic with chosen priority. For the full throughput tests of the channel, you must set the highest priority “0” for the test traffic. In this case, the transmission of any other traffic is 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 current bitrate.

NOTE

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

Performance tests contains of 8 tests performed on established bitrate, test can be performed in one direction or bidirectionally.



37 Figure - Performance test

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:

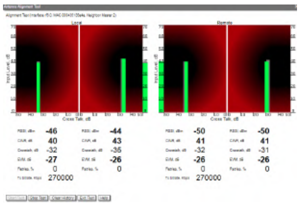
- “*Test time*” parameter - allows setting the duration (in seconds) of the test for each bitrate (5s by default).
- “*Bidirectional*” check-box - allows choosing between bi-directional (when checked) and unidirectional (when unchecked) performance test.
- "*Priority (0-16)"* - by default, it is 16, which is lower than the data traffic that has priority 15. You can increase the test priority by setting a lower value.
- "*Packet size*" - allows to set the desired packet size in bytes.

- "*Load limit*" - sets a limit on the data rate at which the test runs, in Mbps.

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.



38 Figure - Alignment test

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

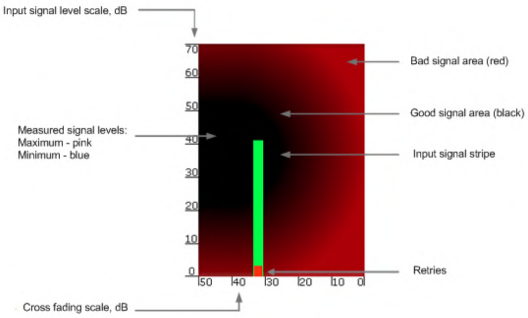
By clicking the «**Clear History**» button, you delete all data stored from the moment you clicked the «**Start Test**» button.

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.

Graphical indicator:



39 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.

The text indicators are:

- "*RSSI*" - indicates the power level of the received radio signal (measured in dBm), optimal parameter value -60 ... -40.
- "*CINR*" - input signal level to noise + interference (measured in dB) indicator, >=28.
- "*Crosstalk*" - indicates how much vertically and horizontally polarized signals influence each other, >20.
- "*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), > 21 in absolute value.
- "*Tx bitrate*" - displays the current bitrate for the remote and local units (measured in Kbps).

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 (CINR) should be between 12 dB and 50 dB.
- If signal level is more than 50 dB, 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 20 MHz to 10 MHz).
- 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 0 dB).

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

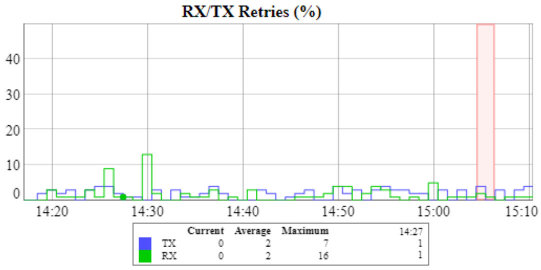
Statistics Graphs

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:

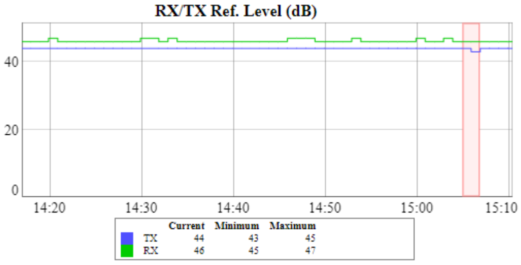


40 Figure - Statistics graphs - balloon indicators

Working with the charts:

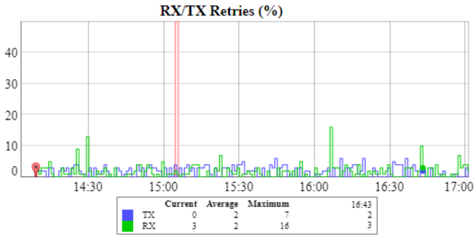
- Select a chart region to zoom in
- Hold the «**Shift**» button and drag the graphs to the pan
- Double-click on any chart to reset the zoom.

The parameters that can be monitored are:



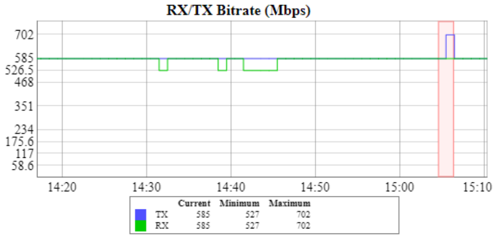
41 Figure - Statistics Graphs - RX/TX Ref. Level

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.



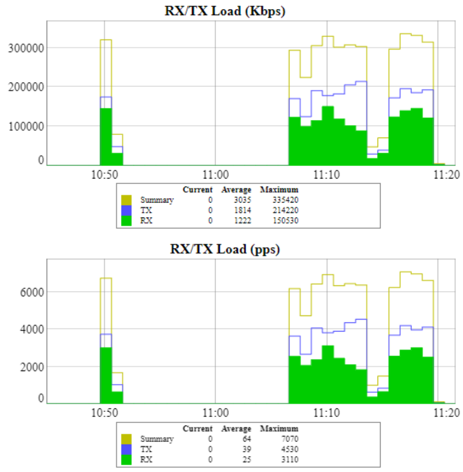
42 Figure - Statistics Graphs - RX/TX Retries

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.



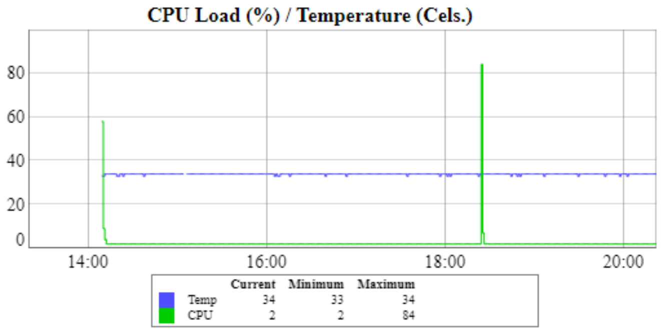
43 Figure - Statistics Graphs - RX/TX Bitrate

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



44 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.



45 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[11].

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[12]).

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.

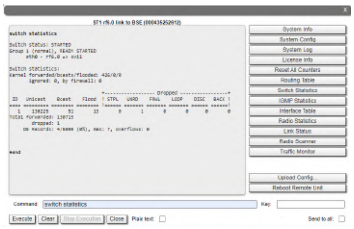
By clicking the «**Close**» button, you return to the "Device Status" page.

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:



```
switch statistics

Switch status: STARTED
Group 1 (normal), READY STARTED
      eth0 - rf6.0 => svi1

Switch statistics:
Kernel forwarded/bcasts/flooded: 436/0/0
       ignored: 0, by firewall: 0

                              +------------------ Dropped -----------------+
 ID   Unicast    Bcast    Flood  ! STPL   UNRD    FRWL    LOOP    DISC   BACK !
---- --------- -------- -------- !------ ------- ------- ------- ------ ------!
   1    138225       51       15       0       1       0       0      0      0
Total forwarded: 138715
        dropped: 1
     DB Records: 4/8000 (0%), max: 7, overflows: 0

#end
```

Command: switch statistics Key:

Plain text: □ Send to all: □

46 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.

[11] https://wiki.infinetwireless.com/display/DR/WANFleX+-+Technical+User+Manual
[12] https://wiki.infinetwireless.com/display/DR/WANFleX+-+Technical+User+Manual

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 rf6.0 -t5 -p mac3*" command.

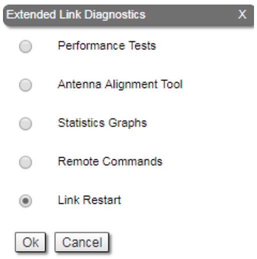
All commands are executed automatically after clicking one of the buttons mentioned above.

> **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.



Extended Link Diagnostics X

○ Performance Tests

○ Antenna Alignment Tool

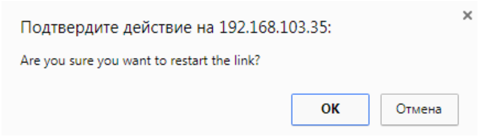
○ Statistics Graphs

○ Remote Commands

● Link Restart

Ok Cancel

47 Figure - Link restart



Подтвердите действие на 192.168.103.35:

Are you sure you want to restart the link?

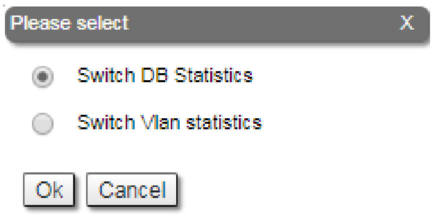
OK Отмена

48 Figure - Link restart - warning message

7.2.6 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:



Please select X

● Switch DB Statistics

○ Switch Vlan statistics

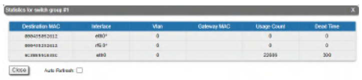
Ok Cancel

49 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:



Statistics for switch group #1 X

Destination MAC	Interface	Vlan	Gateway MAC	Usage Count	Dead Time
000435852012	eth0*	0		0	0
000435252012	rf5.0*	0		0	0
[illegible]	eth0	0		23686	300

Close   Auto Refresh: □

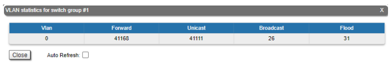
50 Figure - Switch DB Statistics

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:



VLAN statistics for switch group #1 X

Vlan	Forward	Unicast	Broadcast	Flood
0	41168	41111	26	31

Close   Auto Refresh: □

51 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.

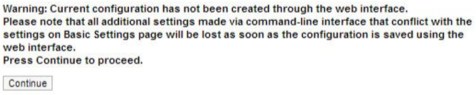
7.3 Basic Settings

Devices 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 (see page 128) 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:



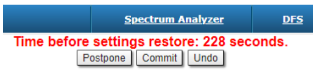
Warning: Current configuration has not been created through the web interface.
Please note that all additional settings made via command-line interface that conflict with the settings on Basic Settings page will be lost as soon as the configuration is saved using the web interface.
Press Continue to proceed.

Continue

52 Figure - Basic settings warning message

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

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.



Time before settings restore: 228 seconds.

53 Figure - Settings restore

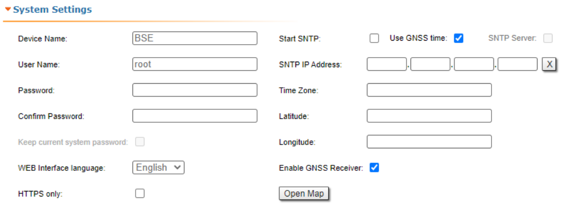
By clicking the «**Preview Configuration**» button, you can view the configuration results in CLI-style format.

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.

The "Basic Settings" page has the following sections:

7.3.1 System Settings

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



System Settings

Device Name:	BSE	Start SNTP:	☐ Use GNSS time: ☑ SNTP Server: ☐
User Name:	root	SNTP IP Address:	. . .
Password:		Time Zone:	
Confirm Password:		Latitude:	
Keep current system password:	☐	Longitude:	
WEB Interface language:	English	Enable GNSS Receiver:	☑
HTTPS only:	☐		

54 Figure - System Settings default configuration

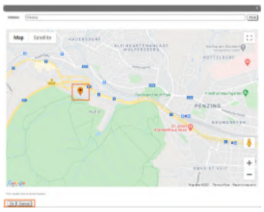
General System Parameter	Description
Device Name	• You can set the device name • This parameter is displayed in the web-page header
User Name	• Displays the username (Login) used to access the unit management interfaces • You can change the current username

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
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)

General System Parameter	Description
Use GNSS Position	• Enable/disable GNSS position • Disabled by default

12 Table - System Settings

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



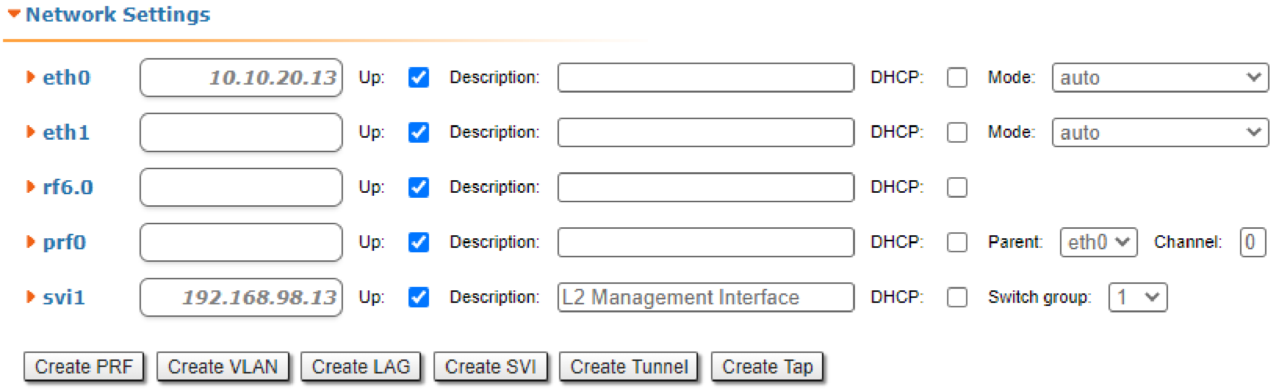
55 Figure - Google Map

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.

7.3.2 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 rf6.0) are set by default and they cannot be removed. For these two interfaces, you are allowed to change the parameters only.

> **NOTE**
>
> Before making the configurations in the "Network Settings" section, please read the information presented in the "MAC Switch (see page 103)" section.



▾ Network Settings

▸ eth0	10.10.20.13	Up: ☑	Description:	DHCP: □	Mode: auto
▸ eth1		Up: ☑	Description:	DHCP: □	Mode: auto
▸ rf6.0		Up: ☑	Description:	DHCP: □	
▸ prf0		Up: ☑	Description:	DHCP: □	Parent: eth0 Channel: 0
▸ svi1	192.168.98.13	Up: ☑	Description: L2 Management Interface	DHCP: □	Switch group: 1

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:

- "**PRF**" - Pseudo Radio Interface 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**" 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***" 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;
- "**SVI**", Switch Virtual Interface 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**" 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**" interface simulates a link layer (L2) device and operates with Ethernet frames. TAP interface is used for creating a network bridge.

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: 1000Base-TX-fullduplex) - the default value is "*Auto*" (recommended)
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)

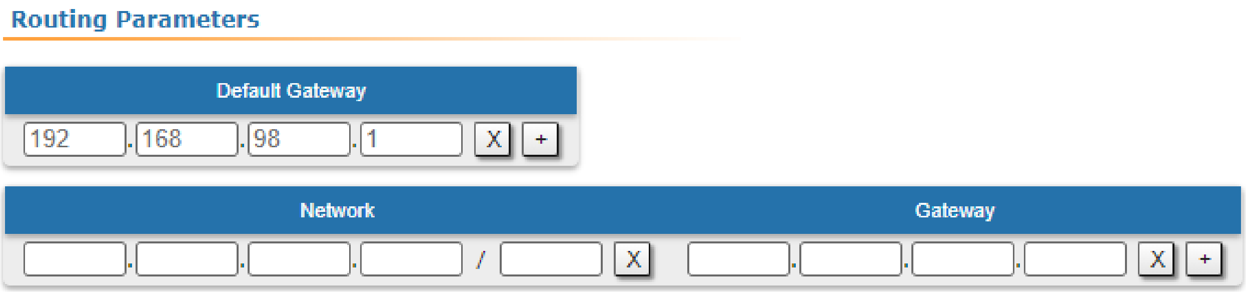
Interface type	Operations
sviX	• SVI interface is a logical L3 interface of the switch (solely used for the management of the unit) • Configure the IP address(es) and the mask of the interface (as the management IP address(es) of the unit) • Enable/disable the interface • Enable/disable DHCP - obtain 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)
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[13]) • 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 (not recommended way) • 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) • In the drop-down window, you can select the vlan interface operation mode: • 802.1q - vlan tag operations are performed according to this standard; • 802.1ad - double tagging "QinQ"; • 802.1ah - backbone bridge using mac-in-mac technology described by the IEEE 802.1ah-2008 standard.

[13] https://wiki.infinetwireless.com/display/DR/WANFleX+-+Technical+User+Manual

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

13 Table - Network Settings

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



- 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.

7.3.3 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:

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

"rf6.0" subsection

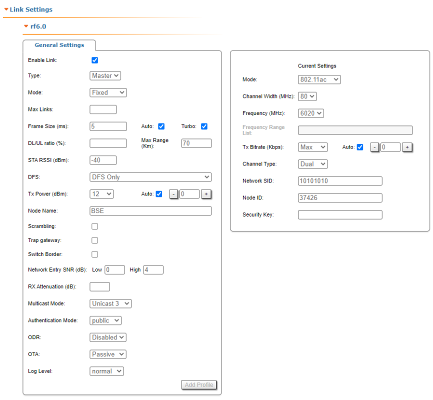
This subsection is used for:

- Radio link settings(see page 91).
- Frequency limitation(see page 99).
- Setting channel type mode(see page 99).

Radio link settings

"rf6.0" subsection is divided in two zones:

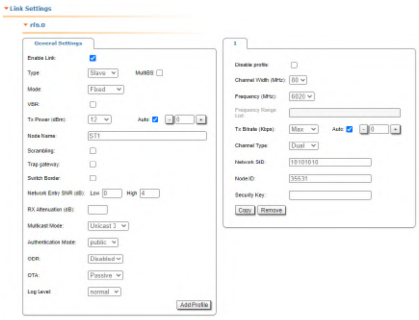
- The panel that describes global link settings, in the left side of the page
- The panel that describes the radio channel settings which are currently in use, in the right side of the page.



Enable Link: ☑
Type: Master
Mode: Fixed
Max Links:
Frame Size (ms): 5 Auto: ☑ Turbo: ☑
DL/UL ratio (%): Max Range (Km): 70
STA RSSI (dBm): -40
DFS: DFS Only
Tx Power (dBm): 12 Auto: ☑ - 0 +
Node Name: BSE
Scrambling: ☐
Trap gateway: ☐
Switch Border: ☐
Network Entry SNR (dB): Low 0 High 4
RX Attenuation (dB):
Multicast Mode: Unicast 3
Authentication Mode: public
ODR: Disabled
OTA: Passive
Log Level: normal

Current Settings
Mode: 802.11ac
Channel Width (MHz): 80
Frequency (MHz): 6020
Frequency Range List:
Tx Bitrate (Kbps): Max Auto: ☑ - 0 +
Channel Type: Dual
Network SID: 10101010
Node ID: 37426
Security Key:

56 Figure - Master node configuration



Enable Link: ☑
Type: Slave MultiBS ☐
Mode: Fixed
VBR: ☐
Tx Power (dBm): 12 Auto: ☑ - 0 +
Node Name: ST1
Scrambling: ☐
Trap gateway: ☐
Switch Border: ☐
Network Entry SNR (dB): Low 0 High 4
RX Attenuation (dB):
Multicast Mode: Unicast 3
Authentication Mode: public
ODR: Disabled
OTA: Passive
Log Level: normal

Disable profile: ☐
Channel Width (MHz): 80
Frequency (MHz): 6020
Frequency Range List:
Tx Bitrate (Kbps): Max Auto: ☑ - 0 +
Channel Type: Dual
Network SID: 10101010
Node ID: 35531
Security Key:

57 Figure - Slave node configuration

In a point-to-multipoint topology, several profiles can be configured on the Slave device (with parameters for connecting to each base station sector). A subscriber terminal can connect to more than one base station, both in nomadic or mobile mode and in a fixed mode for redundancy purposes (a separate profile for each base station). When trying to establish a wireless connection, the subscriber terminal selects a base station with parameters that provide the best connection quality (RSSI, signal-to-noise ratio, bitrate, errors number, retries, etc.) If connection with the base station is lost, the subscriber terminal will not try to reconnect to it, but will evaluate the signal parameters of all available base stations sectors.

The "Frequency roaming" function is enabled by default (the "auto" option of the Frequency parameter), and allows the subscriber terminal with automatic frequency selection (if it has appropriate radio profiles):

- Automatically switch from the main base station (roamingleader) to the backup.
- Automatically switch between different base stations while moving.
- Automatically switch to a new base station frequency if the current base station frequency has changed.

During frequency roaming process the traffic transmission does not stop.The radio link parameters are described in the table:

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.
MultiBS (Slave)	• Enabled: when the link parameters deteriorate, the CPE will disconnect from the current base station and try to find the sector with the best parameters values • Disabled: the CPE will keep the connection with a current base station until the signal is completely lost • 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
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)	• Increase the throughput in case of link degradation due to errors in the radio. The sliding window of the ARQ algorithm are extended from three to five frames, which increases its efficiency.
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

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.
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.)
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

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[14]".
Authentication Mode	• Set the mode: • *"static"* - the unit can establish connections only with units, which MAC-addresses are listed in the "Static Links[15]" 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)

[14] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=10780854
[15] https://wiki.infinetwireless.com/display/DR/Static+Links

ODR	Activate routing using the ODR protocol. The following modes are available: • "Disable" - routing using ODR is not performed. • "Hub" - the device acts as a central node. • "Spoke" - the device acts as a peripheral node. The main advantage of ODR protocol is a network throughput efficient use. Part of the link throughput is usually used by the routing protocol to transmit service information, this part can be released by ODR using. The ODR protocol transmits the hosts IP prefixes using the MINT protocol at the data link layer. The ODR protocol can only be used in networks with star topology, where all nodes are connected to the central node only. An example of such a network is a point-to-multipoint topology, where each subscriber is connected only to a base station.
OTA	Automatic updates in the MINT domain may be configured in the following modes: • “Disabled” - the device does not check if other devices in the MINT domain have a newer software versions. • "Passive" - in case a newer software version is detected on one of the neighboring nodes, the device requests and updates the software. The device does not announce own software version. • "Active" - the device announces its software version in the MINT domain, making it available to download by other nodes.
Log Level	• Set the log level: • *off* • *normal* • *detailed*
Current Settings	
Mode (Master)	There are two modes for access to the radio medium available: • 802.11ac - compatibility mode with InfiLINK Evolution / InfiMAN Evolution family device • 802.11nHT - compatibility mode with InfiLINK 2x2 / InfiMAN 2x2 family device ⚠ **NOTE** To establish a wireless connection in 802.11nHT mode, the "greenfield" option on InfiLINK 2x2 / InfiMAN 2x2 families devices must be disabled.

Channel Width	• Set the bandwidth of the radio interface in MHz • It must be the same at both ends of the link • For 802.11ac mode the values 20, 40 and 80 MHz are available, for 802.11nHT mode - 20 and 40 MHz, for models E5-BSE-L and E5-BSI-L - 20 and 40 MHz
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
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 780000 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
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

14 Table - Radio settings parameters in the time division networks

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

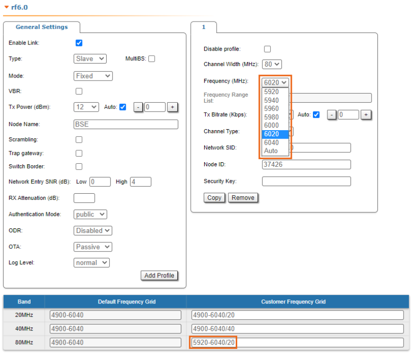
- "**Disable profile**" check box disable a radio profile
- Add a new radio profile by clicking the «**Add Profile**» button
- Copy the radio profile values to a new radio profile by clicking the «**Copy**» button
- Remove the radio profile by clicking the «**Remove**» button.

Frequency limitation

The licensed frequencies range per each bandwidth is displayed in the "rf6.0" 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: 5920-6040/20 means that the step between the center frequencies from 5920 GHz and 6040 GHz is 20 MHz).

The changes performed in “*Customer Frequency Grid*” will be available in the “*Frequency*” drop down list from the radio profiles and in DFS(see page 137) page in “*Frequency grid*” field.



rf6.0

General Settings

Enable Link: ☑
Type: Slave
MultiBS: □
Mode: Fixed
VBR: □
Tx Power (dBm): 12 Auto: ☑ - 0 +
Node Name: BSE
Scrambling: □
Trap gateway: □
Switch Border: □
Network Entry SNR (dB): Low 0 High 4
RX Attenuation (dB):
Authentication Mode: public
ODR: Disabled
OTA: Passive
Log Level: normal
Add Profile

1

Disable profile: □
Channel Width (MHz): 80
Frequency (MHz): 6020
5920
5940
5960
5980
6000
6020
6040
Auto
Frequency Range List:
Tx Bitrate (Kbps): Auto: ☑ - 0 +
Channel Type:
Network SID:
Node ID: 37426
Security Key:
Copy Remove

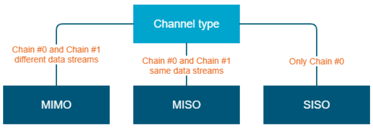
Band	Default Frequency Grid	Customer Frequency Grid
20MHz	4900-6040	4900-6040/20
40MHz	4900-6040	4900-6040/40
80MHz	4900-6040	5920-6040/20

58 Figure - Customer frequency grid

Setting channel type mode

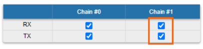
When Channel Type is set to “*Single*”, then *Tx* and/or *Rx of Chain #1* (for horizontal polarization antenna) can be deactivated:

- "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


Channel type
Chain #0 and Chain #1 different data streams
Chain #0 and Chain #1 same data streams
Only Chain #0
MIMO
MISO
SISO

59 Figure - Configuration options

If the "Single" mode is selected when, then "Chain #1" column (horizontal polarization) can be disabled for transmission (TX) and / or reception (RX):



	Chain #0	Chain #1
RX	☑	☑
TX	☑	☑

60 Figure - Chain #

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**

15 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**

16 Table - Settings for MISO mode

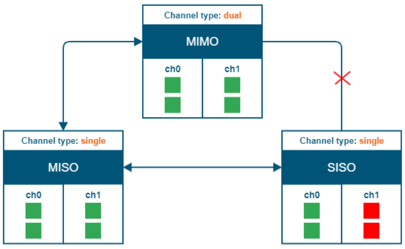
Settings for "SISO" mode

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**

17 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[16] – SISO[17] is not functional.

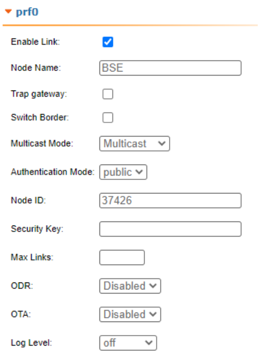


61 Figure - Radio link establishment

"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(see page 87)" 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 "rf6.0" subsection(see page 91) above:

[16] https://wiki.infinetwireless.com/display/DR/MIMO
[17] https://wiki.infinetwireless.com/display/DR/SISO



prf0

Enable Link: ☑

Node Name: BSE

Trap gateway: □

Switch Border: □

Multicast Mode: Multicast

Authentication Mode: public

Node ID: 37426

Security Key:

Max Links:

ODR: Disabled

OTA: Disabled

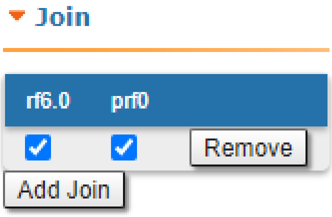
Log Level: off

62 Figure - PRF settings

"Join" subsection

In the "Join" subsection, you can link two or more radio/pseudo-RF[18] interfaces of one unit into one MINT[19] domain. Each of these interfaces may act as an independent MINT[20] network node. The "Join" subsection is available for configurations only after at least one pseudo-RF[21] interface has been created in "Network Settings[22]" section.

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



Join

rf6.0	prf0	
☑	☑	Remove

63 Figure - «Remove» and «Add Join» buttons

7.3.4 Static Links

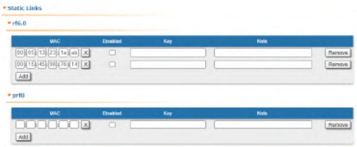
In the "Static Links" section, you can set up fixed links to the unit. Although the radio parameters and security key match with other nodes, the node that has Static Links set up is only linked with the nodes which are configured in this section. The parameters are:

- "*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

[18] https://wiki.infinetwireless.com/display/DR/RF
[19] https://wiki.infinetwireless.com/display/DR/MINT
[20] https://wiki.infinetwireless.com/display/DR/MINT
[21] https://wiki.infinetwireless.com/display/DR/RF
[22] https://wiki.infinetwireless.com/display/DR/Network+Settings



Static Links

rf6.0

MAC	Disabled	Key	Note	
00:05:13:23:1e:ab X	□			Remove
00:15:45:98:78:14 X	□			Remove

Add

prf0

MAC	Disabled	Key	Note	
: : : : : X	□			Remove

Add

64 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.

7.3.5 MAC Switch

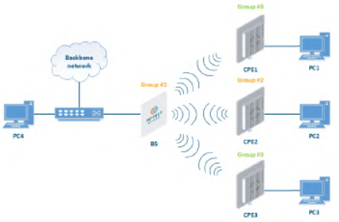
Switch configuration

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

- An unique numeric identifier (1-4999) 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.



65 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.

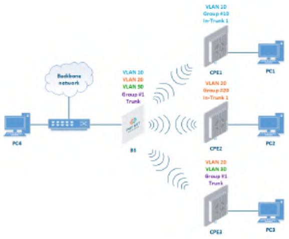
Trunk groups

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.



66 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[23]).

Management connection to the unit

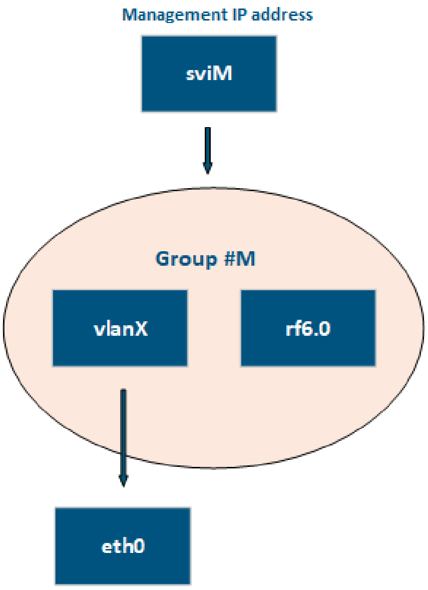
For the management purposes, you can create a dedicated Switch Group for all units in the MINT network, attached to the Switch Virtual Interface (SVI). Assign the IP addresses directly on the SVI interface for native management. All packets sent via SVI interface will be distributed only within the assigned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

The universal way to configure Management VLAN via dedicated switch group is presented in the figure below (for more information see section "Remote management of the InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution and InfiMAN Evolution units[24]").

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 "*rf6.0"* interface:

[23] https://wiki.infinetwireless.com/display/DR/WANFleX+-+Technical+User+Manual

[24] https://wiki.infinetwireless.com/display/DR/Remote+management+of+the+InfiLINK+2x2%2C+InfiMAN+2x2%2C+InfiLINK+Evolution+and+InfiMAN+Evolution+units



67 Figure - Management configuration

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”

18 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
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"*

Primitives	Description
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*"
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*"
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*”

Primitives	Description
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
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

Primitives	Description
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
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*
clnp, **esis**, **isis**	• Abbreviations for: “iso proto p”, where “*p*” is one of the above protocols

Primitives	Description
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) • 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

19 Table - Primitives

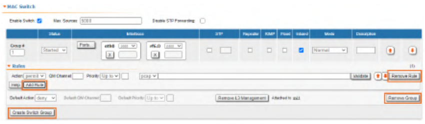
Primitives may be combined using:

- 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.



68 Figure - MAC Switch 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 L3 Management*» - by clicking this button you can delete the "*sviX*" interface, which is available in the default configuration, for the unit management
- «*Create L3 Management*» - by clicking this button you can add an "*sviX*" interface for the unit management via Web interface.

«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)
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

Switch parameter	Description
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
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 (see page 125)" 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

20 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 (see page 125)" 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), PCAP expressions cannot be used in "trunk/in-trunk mode" • Validate rule by clicking the «**Validate**» button

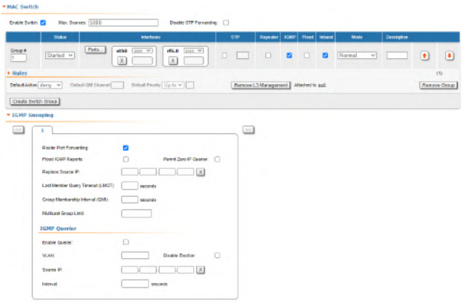
21 Table - Switch Groups Rules

⚠ **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).



MAC Switch

Enable Switch: ☑ Max. Sources: 5000 Disable STP Forwarding: ☐

	Status	Interfaces			STP		Repeater	IGMP	Flood	Inband	Mode	Description		
Group # 1	Started	Ports...	eth0	rf6.0	☐		☐	☑	☐	☑	Normal			

Rules

Default Action: deny Default QM Channel: Default Priority: Up to

Remove L3 Management Attached to null Remove Group

Create Switch Group

IGMP Snooping

1

Router Port Forwarding: ☑

Flood IGMP Reports: ☐ Permit Zero IP Querier: ☐

Replace Source IP:

Last Member Query Timeout (LMQT): seconds

Group Membership Interval (GMI): seconds

Multicast Group Limit:

IGMP Querier

Enable Querier: ☐

VLAN: Disable Election: ☐

Source IP:

Interval: seconds

69 Figure - IGMP snooping configuration

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
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

IGMP Snooping parameter	Description
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)

22 Table - IGMP Snooping

7.3.6 IP Firewall menu

IP Firewall is a mechanism of filtering packets crossing an IP[25] 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:

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.

[25] https://wiki.infinetwireless.com/display/DR/IP

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
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 (see page 125)" 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

23 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.

7.3.7 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

SNMP access parameter	Description
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
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
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

SNMP access parameter	Description
Privacy Password	• Set the privacy password • It is necessary when privacy is enabled for the required security level

24 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)

25 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
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%
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

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

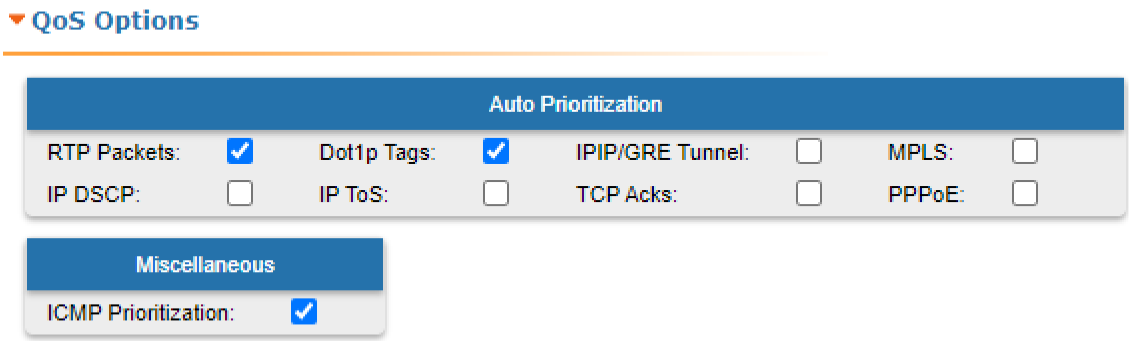
26 Table - SNMP Trap Types

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.

7.3.8 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.



QoS Options

Auto Prioritization

RTP Packets: ☑ Dot1p Tags: ☑ IPIP/GRE Tunnel: □ MPLS: □
IP DSCP: □ IP ToS: □ TCP Acks: □ PPPoE: □

Miscellaneous

ICMP Prioritization: ☑

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

QoS Parameter	Description
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
MPLS	• Enable/disable automatic prioritization for the packets tagged with MPLS priority tags
IP DSCP	• Enable/disable automatic prioritization for the packets tagged with DiffServ priority tags
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
PPPoE	• Enable/disable automatic prioritization for the PPPoE tunnels traffic
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)

27 Table - QoS

7.3.9 Traffic Shaping

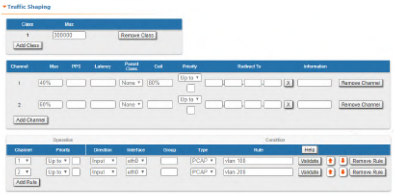
The "Traffic Shaping" section allows to manipulate the data streams flowing through the device. Up to 200 logical channels can be created, characterized by different properties (such as priority levels and data transfer rates), and then the data streams can be assigned to these logical channels according to the special rules, previously created. In order to configure distribution of the transmit rate between several channels, can be created the class.

In the default configuration, there is no channel or class created.

Create the class by clicking the "**Add Class**" button, to set the transmit rate redistribution for one or more channels.

Parameter	Description
Class	Service class number in the range 1-200
Max	Maximal available transmit rate in Kbps

You can delete an existed class by clicking the corresponding "**Remove Class**" button.



Traffic Shaping

Class	Max	
1	300000	Remove Class

Add Class

Channel	Max	PPS	Latency	Parent Class	Ceil	Priority	Redirect To	Information	
1	40%			None	80%	Up to			Remove Channel
2	60%			None		Up to			Remove Channel

Add Channel

Operation		Condition								
Channel	Priority	Direction	Interface	Group	Type	Rule	Help			
1	Up to	Input	eth0		PCAP	vlan 100	Validate	↑	↓	Remove Rule
2	Up to	Input	eth0		PCAP	vlan 200	Validate	↑	↓	Remove Rule

Add Rule

70 Figure - Traffic Shaping options

In order to prioritize the data flows and/or to set the data transfer rates, create the logical channels by clicking the "**Add Channel**" button.

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 • The value can also be set in percentage of the class.
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
Parent Class	• Establish affiliation to a class.
Ceil	• Available only if the parent class is specified. • Set the maximum non-guaranteed transmit rate in a percentage of the higher-class band or in Kbps. • If no value is specified, the free transmit rate of the class is distributed evenly between the channels, depending on the load.

Logical channel parameter	Description
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

28 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
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

Traffic shaping rule parameter	Description
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 • 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

29 Table - Traffic shaping rules

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

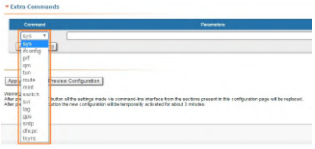
7.3.10 Extra commands

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[26] **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*:



Warning
After p... button all the settings made via command-line interface from the sections present in this configuration page will be replaced.
After p... button the new configuration will be temporarily activated for about 3 minutes.

71 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[27] for the full explanation of all command parameters and options

[26] https://wiki.infinetwireless.com/display/DR/CLI
[27] https://wiki.infinetwireless.com/display/DR/WANFleX+-+Technical+User+Manual

Parameter	Description
Disabled	• Check this option in order to disable the command temporarily

30 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

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.

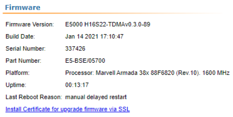
7.4 Maintenance menu

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:

- Firmware(see page 129)
  - SSL certificate installation(see page 130)
  - Firmware update(see page 131)
  - Mass firmware upgrade(see page 133)
- Upload(see page 134)
- Download(see page 134)
- Bottom section of the page(see page 134)

7.4.1 Firmware



Firmware

Firmware Version:	E5000 H16S22-TDMAv0.3.0-89
Build Date:	Jan 14 2021 17:10:47
Serial Number:	337426
Part Number:	E5-BSE/05700
Platform:	Processor: Marvell Armada 38x 88F6820 (Rev.10). 1600 MHz
Uptime:	00:13:17
Last Reboot Reason:	manual delayed restart

Install Certificate for upgrade firmware via SSL

72 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

Parameter	Description
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

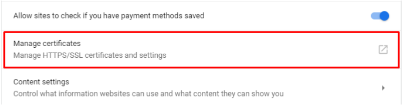
31 Table - Firmware parameters

SSL certificate installation

> **NOTE**
>
> To configure a wireless device via Web GUI using secure protocol HTTPS, a SSL certificate must be installed as trusted into your web browser. Otherwise, the automatic update function will not be available.

The following description shows an installation process for Google Chrome web browser. Configuration of other web browsers is described in the relevant product user guide and is similar to following.

1. Download SSL certificate by clicking the "Install Certificate for upgrade firmware via SSL" link. Please note, this link is available if you connect to the Web GUI via HTTPS only.
2. Open the "Chrome Settings" section and click on the "Manage certificates" button.



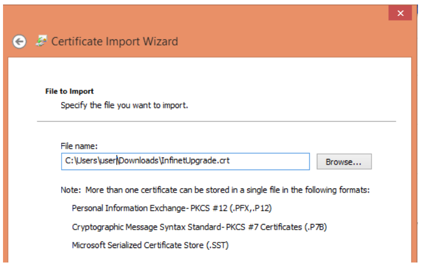
Allow sites to check if you have payment methods saved

Manage certificates
Manage HTTPS/SSL certificates and settings

Content settings
Control what information websites can use and what content they can show you

73 Figure – Google Chrome Settings

3. Click the "Import..." button to launch Certificate Import Wizard.
4. Follow the wizard's instructions and choose the file to be imported. Click the "Browse..." button and choose the SSL certificate that you have downloaded before. Click the "Next" button to proceed.



File to Import

Specify the file you want to import.

File name: C:\Users\user\Downloads\InfinetUpgrade.crt

Note: More than one certificate can be stored in a single file in the following formats:

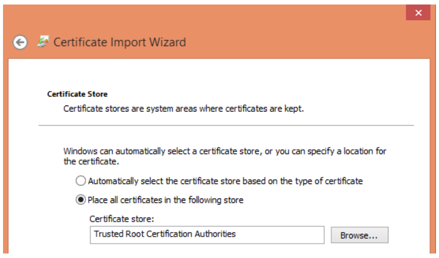
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

74 Figure – Certificate Import Wizard

5. In the next step it is necessary to select the repository where certificate will be placed. All new certificates are installed into the personal repository by default, click on the "Browse..." button and select "Trusted Root Certification Authorities". Click the "Next" button to proceed.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

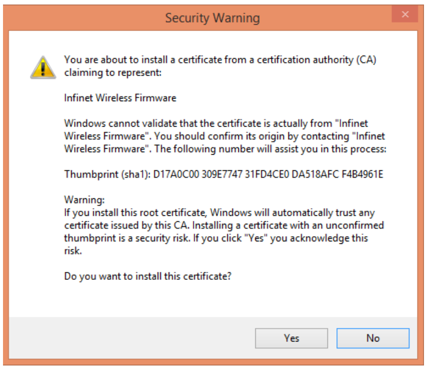
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

75 Figure – Certificates store selection

6. Final step is to check all the provided information. Click the "Finish" button if it's correct. The security warning will appear, click the "Yes" button to confirm you really want to install the certificate.



You are about to install a certificate from a certification authority (CA) claiming to represent:

Infinet Wireless Firmware

Windows cannot validate that the certificate is actually from "Infinet Wireless Firmware". You should confirm its origin by contacting "Infinet Wireless Firmware". The following number will assist you in this process:

Thumbprint (sha1): D17A0C00 309E7747 31FD4CE0 DA518AFC F4B4961E

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

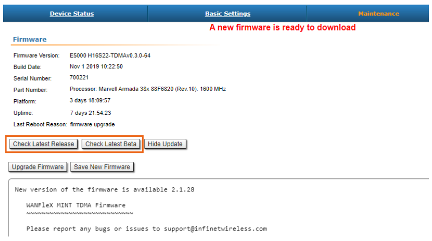
76 Figure – Installation confirmation

Firmware update

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:

> **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:



A new firmware is ready to download

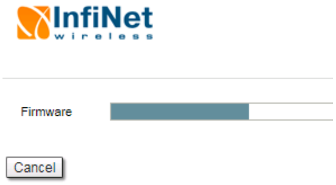
Firmware

Firmware Version: E5000 H16S22-TDMAv0.3.0-64
Build Date: Nov 1 2019 10:22:50
Serial Number: 700221
Part Number: Processor: Marvell Armada 38x 88F6820 (Rev.10). 1600 MHz
Platform: 3 days 18:09:57
Uptime: 7 days 21:54:23
Last Reboot Reason: firmware upgrade

```
New version of the firmware is available 2.1.28

   WANFleX MINT TDMA Firmware
   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~

   Please report any bugs or issues to support@infinetwireless.com
```

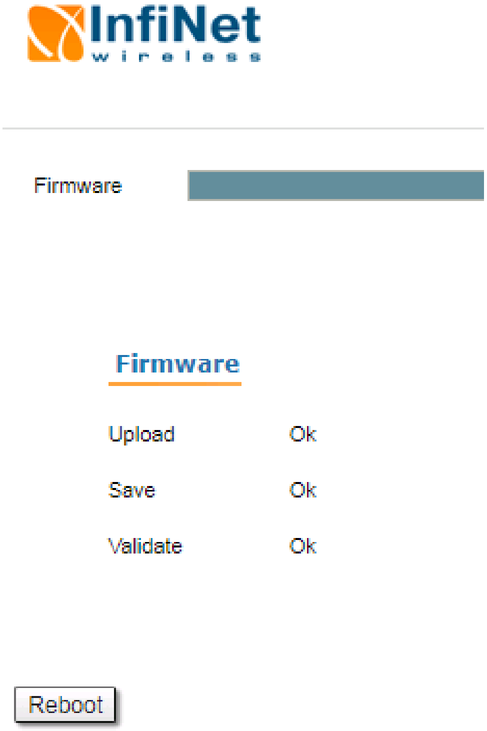
77 Figure - New firmware availability

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



78 Figure - Firmware upgrade

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



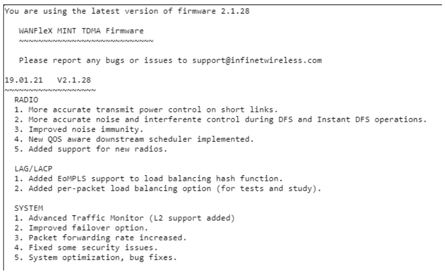
Firmware

Upload Ok
Save Ok
Validate Ok

79 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:



```
You are using the latest version of firmware 2.1.28

   WANFleX MINT TDMA Firmware
   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~

   Please report any bugs or issues to support@infinetwireless.com

19.01.21   V2.1.28
~~~~~~~~~~~~~~~~~~~
  RADIO
  1. More accurate transmit power control on short links.
  2. More accurate noise and interferente control during DFS and Instant DFS operations.
  3. Improved noise immunity.
  4. New QOS aware downstream scheduler implemented.
  5. Added support for new radios.

  LAG/LACP
  1. Added EoMPLS support to load balancing hash function.
  2. Added per-packet load balancing option (for tests and study).

  SYSTEM
  1. Advanced Traffic Monitor (L2 support added)
  2. Improved failover option.
  3. Packet forwarding rate increased.
  4. Fixed some security issues.
  5. System optimization, bug fixes.
```

80 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.

Mass firmware upgrade

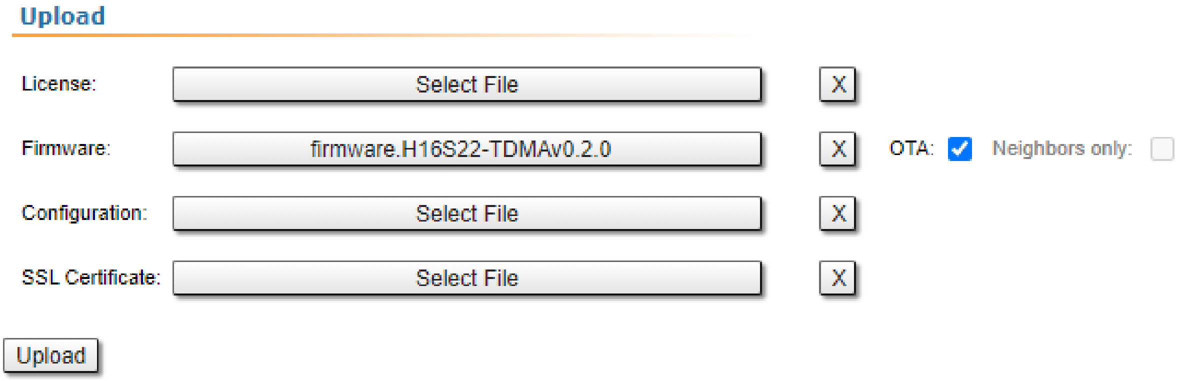
Each device has the ability to mass firmware upgrade using OTA (Over the Air) function. The firmware can be distributed to:

- All devices within a single MINT domain. The firmware will be applied even to the not directly connected devices.
- Neighbor devices, directly connected to the current.

> **NOTE**
>
> Only one firmware version can be applied during one mass upgrade cycle. The uploaded firmware version will be applied only to those devices that are built on the same platform. Thus if the upgraded network includes devices on different platforms, the mass upgrade cycle should be performed for each platform. In case the OTA function is enabled the uploaded firmware will not be applied to the device from which the upgrade is performed. It will be uploaded only to the other network devices.

Mass upgrade cycle includes the following steps:

1. Download the required firmware version from the official FTP server (ftp://ftp.infinetwireless.com).[28]
2. Choose the downloaded firmware file in the "Upload" section. Enable OTA function. Enable "Neighbors only" in case you want to upgrade only the neighbor devices.



Upload

License: Select File X

Firmware: firmware.H16S22-TDMAv0.2.0 X OTA: ☑ Neighbors only: □

Configuration: Select File X

SSL Certificate: Select File X

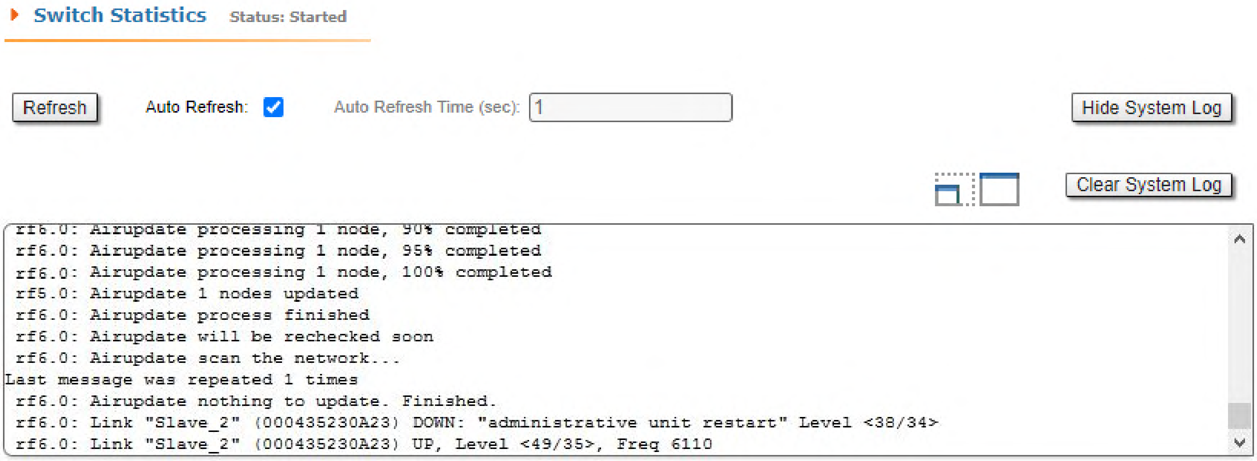
3. Click the "Upload" button. The mass upgrade process will be started.

[28] ftp://ftp.infinetwireless.com%29./

Mass upgrade monitoring

The mass upgrade progress can be seen in the System Log (Device Status section): the number of upgraded devices and progress.

The remote devices will be rebooted after upgrade completion. The connection failure duration is approximately 35-40 seconds per device.



```
 rf6.0: Airupdate processing 1 node, 90% completed
 rf6.0: Airupdate processing 1 node, 95% completed
 rf6.0: Airupdate processing 1 node, 100% completed
 rf5.0: Airupdate 1 nodes updated
 rf6.0: Airupdate process finished
 rf6.0: Airupdate will be rechecked soon
 rf6.0: Airupdate scan the network...
Last message was repeated 1 times
 rf6.0: Airupdate nothing to update. Finished.
 rf6.0: Link "Slave_2" (000435230A23) DOWN: "administrative unit restart" Level <38/34>
 rf6.0: Link "Slave_2" (000435230A23) UP, Level <49/35>, Freq 6110
```

7.4.2 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.

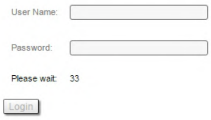
7.4.3 Download

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».

7.4.4 Bottom section of the page

The following buttons are available:

- «Reboot» - 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:



User Name:

Password:

Please wait: 33

81 Figure - Unit reboot

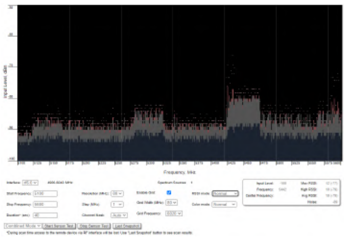
- «Restore Factory Settings» - restores the factory default configuration. A warning message pops up, asking for the permission before the operation to start. During the reset to factory process, you are redirected to the login page and the timeout period of 30 seconds counts down before the new login:
- «View Current License» - shows the current device license parameters in a new window
- «View Current Configuration» - shows the current device configuration in text format in a new window
- «Create Diagnostic Card» - 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.

7.5 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.



82 Figure - Spectrum analyzer

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

Parameter	Description
Interface	• rf6.0 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
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 – holds the maximum signal values at a given point • Peak Hold – holds the peak signal values at a given point
Scan mode	• "*Local mode*" – scanning is performed only on the local device. • "*Combined mode*" – Scanning is performed simultaneously on all devices in the sector. The "**Last Snapshot**" button will display the blended result

32 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.

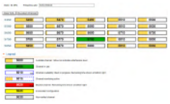
You can get detailed information about the scanned radio signals on a specific frequency. Just point a cursor on the needed frequency and you will see a hint with exact Signal level (dBm), Frequency (MHz), Noise Floor (dBm), indicators of RSSI (dBm), High RSSI (dBm), Max RSSI (dBm) and their values in dB. High RSSI allows you to estimate the signal sources number, if the value is significantly different from the average RSSI, then there are several sources of interference.

7.6 DFS menu

The "DFS[29]" 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.

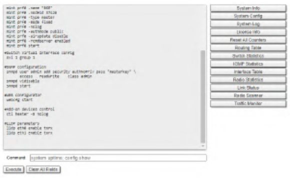


83 Figure - DFS

7.7 Command Line menu

The "Command Line" page emulates CLI[30] (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:



```
mint prf0 -name "[illegible]"
mint prf0 -nodeid [illegible]
mint prf0 -type master
mint prf0 -mode fixed
mint prf0 -nolog
mint prf0 -authmode public
mint prf0 -airupdate disable
mint prf0 -roamserver enabled
mint prf0 start

#switch virtual interface config
svi 1 group 1

#snmp configuration
snmpd user admin add security authnopriv pass "masterkey" \
      access   readwrite    class admin
snmpd v1disable
snmpd start

#web configurator
webcfg start

#add-on devices control
ctl heater -s nolog

#LLDP parameters
lldp eth0 enable txrx
lldp eth1 enable txrx
```

Command: system uptime; config show

84 Figure - Command line

[29] https://wiki.infinetwireless.com/display/DR/DFS
[30] https://wiki.infinetwireless.com/display/DR/CLI

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.

8 Troubleshooting

8.1 No access to the local unit

Make sure that the connectivity is provided between the control center and the device's installation point. If the access is missing only for the InfiNet device, further actions must be performed at the device's installation site.

8.1.1 Indicators

Pay attention to the LED indicators on the device's enclosure.

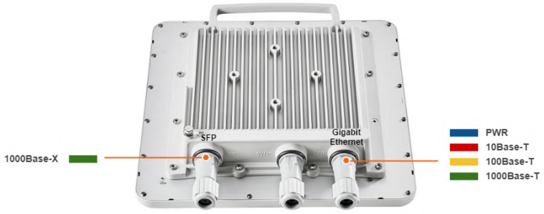
> **NOTE**
>
> The LED indication on the device can be disabled administratively. Make sure there is no "system no indicator[31]" command in the last saved device configuration. We recommend to save backup configurations to the internal memory of the device and to a folder on your PC. The device can store 8 configuration backups. When saving the current configuration, its previous version is automatically added to the backup list with record number 0. All operations with the device configurations are performed using the "config[32]" command.

If the power and Ethernet indicators are off, check the integrity of the power supply, the Ethernet cables and the RJ-45 connectors. Replace the power supply and the cables if necessary.

InfiMAN Evolution Base Station Sectors

LED indicators on the InfiMAN Evolution family base station sectors are located in the the cable glands ports. These indicators help to monitor the device's status during the installation. The correspondence between the state of the indicators and the current device state is shown in the table below.

[31] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-system
[32] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-config



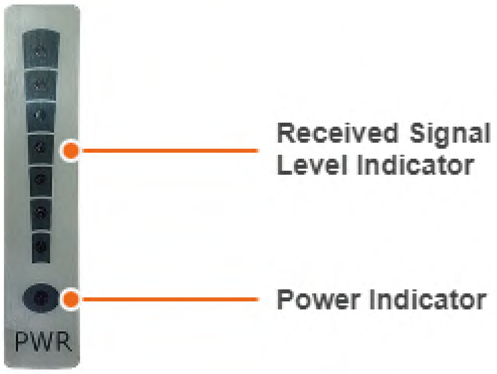
85 Figure - LED indication of InfiMAN Evolution BS

LED	State	Status	Description
Gigabit Ethernet **SFP**	Flash	Initialization	The LEDs on both ports light up with white on second. Then LEDs check is performed: red, blue, green are lightened up sequentially.
	Flash	Loading	Only for Gigabit Ethernet port: at the beginning green is lightened a few seconds, on the second loading stage switches to blue.
	ON/ Blue	Power	Only for Gigabit Ethernet port.
	ON/ Red	Speed 10 Mbps	Only for Gigabit Ethernet port.
	ON/ Yellow	Speed 100 Mbps	Only for Gigabit Ethernet port.
	ON/ Green	Speed 1000 Mbps	
	ON/ Green	ERConsole stage	Port with the established link lights up with green, the second port remains blue.

33 Table - LEDs modes and device status of InfiMAN Evoluton BS

InfiMAN Evolution Su**bscriber Terminals and** InfiLINK Evolution **devices**

InfiMAN Evolution ST and InfiLINK Evolution devices have a LED indicator set located at the back of each device, displaying the current device state.



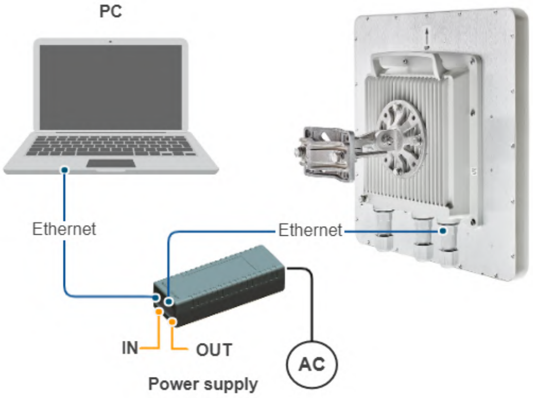
86 Figure - LED indication of InfiMAN Evoluton ST, InfiLINK Evolution

PWR - power indicators will light red when the device is connected to a power source, yellow when 10/100 Mbps wired connection appears and green when 1000 Mbps wired connection appears. Other indicators are used to perform coarse antenna alignment. The more indicators are on, the better wireless connection is established. The blinking indicator means an intermediate state. The more often the indicator blinks the higher level connection is established.

8.1.2 Access recovery

If the power indicator is on and there is connection via the Ethernet interface, connect to the device directly as it is shown in the scheme below. Make sure that the IP address of the PC is in the same subnet as the IP address of the device. You can restore the IP address and reset the device to the factory settings using the ERConsole utility.

The factory reset process using the ERConsole is described in the "Emergence Repair Console(see page 156)" article.



87 Figure - The recommended connection scheme

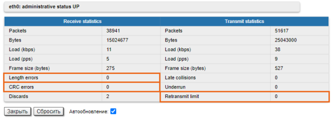
8.1.3 Checking the status of the Ethernet interface

Wired interface statistics

Web interface

If you were able to access the device by connecting directly, try to determine the possible reason for the unavailability through the network. Pay attention to the wired interface statistics. In order to do this, go to the

"Device status" section of the web interface and open the "General statistics" window for the Ethernet interface in the "Interface statistics" section. Pay attention to the CRC errors number, as they indicate a violation of the data integrity during the transmission over the wired segment. Also, the problem can be caused by a queue overflow (Retransmit limit) or an inappropriate frame size (Length errors).



eth0: administrative status UP

Receive statistics		Transmit statistics	
Packets	38941	Packets	51617
Bytes	15024677	Bytes	25043000
Load (kbps)	11	Load (kbps)	38
Load (pps)	5	Load (pps)	9
Frame size (bytes)	275	Frame size (bytes)	527
Length errors	0	Late collisions	0
CRC errors	0	Underrun	0
Discards	2	Retransmit limit	0

88 Figure - Interface statistics

The description of the parameters for a complete diagnostic is available in the "Device status(see page 64)" article.

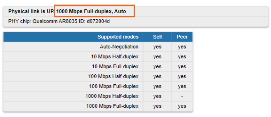
Command line interface

If there is no access to the device's web interface, run the "*ifconfig eth0*" command to get statistics via CLI.

The description of the parameters for a complete diagnostic is available in the "Ifconfig command (interfaces configuration)[33]" article.[34]

Duplex mode

Pay attention to the duplex mode on the network devices connected to the wireless router. This information is available in the the web interface. Proceed to the "Device status" section - "Interface statistics" and open the "General statistic" for the Ethernet interface, or run the "*ifconfig eth0*" command in the command line interface.



Physical link is UP 1000 Mbps Full-duplex, Auto

PHY chip: Qualcomm AR8035 ID: d072004d

Supported modes	Self	Peer
Auto-Negotiation	yes	yes
10 Mbps Half-duplex	yes	yes
10 Mbps Full-duplex	yes	yes
100 Mbps Half-duplex	yes	yes
100 Mbps Full-duplex	yes	yes
1000 Mbps Half-duplex	yes	-
1000 Mbps Full-duplex	yes	yes

89 Figure - Duplex mode

We recommend to set the auto-negotiation mode provided by the Ethernet standard. The problem can occur due to the connection between two devices with different duplex settings. For example, if one device is in auto-negotiation mode and the other is in fixed full duplex mode.

Red value of this parameter in the interface statistics "Mode" column informs that transmission is performed in a half-duplex mode.

8.2 The wireless link cannot be established

[33] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=10781004
[34] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=17605871

8.2.1 Checking the radio settings

Pre-configuration in the lab

Before installing the devices on site, we recommend to configure the basic parameters in the lab and to make sure that the link is establishing.

⚠ **NOTE**

During the configuration of the devices in a lab, take into account the following requirements:

- Make sure that the devices are not directed at each other in order to prevent the damage of the radio modules. It is recommended to place the devices at a distance from each other, with the antennas directed to the floor.
- The minimum transmit output power must be set on the devices.
- In case of using two devices with "E" index, it is recommended to connect them directly using RF cables and RF attenuators with an attenuation of at least 40 dB for each polarization (the installation\deinstallation of the RF attenuators and of the RF cables should only be performed when the devices are switched off).
- The failure or damage of the device's radio module in case of disregarding these requirements is not covered by warranty.

Checking the radio parameters

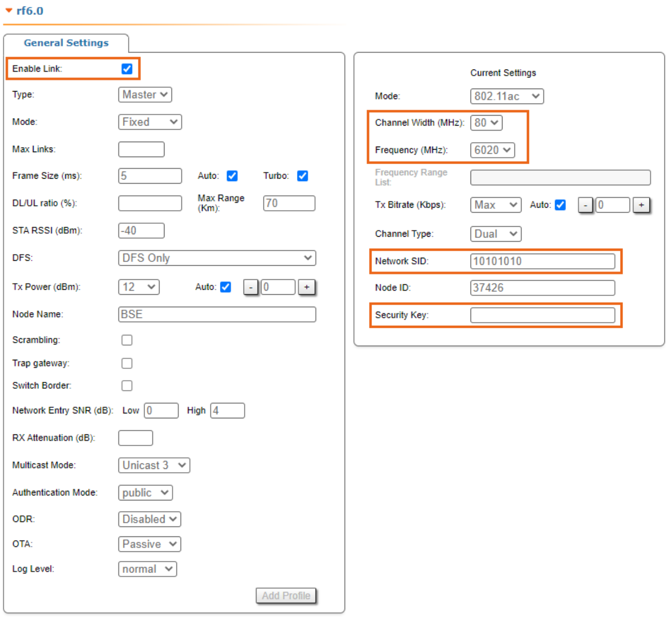
If the wireless link is not establishing in lab conditions, make sure that the radio parameters are set to the values determined during the planning stage. The correct configuration of the device can be obtained using the Configuration Generator tool found on the IW Academy[35] website. To establish a wireless link, one device must be configured as Master, the second (or all subscribers of the base station in the point-to-multipoint topology) as Slave. The following parameters must be identical on both devices:

- Channel Width.
- Frequency ("auto" settings are possible).
- Network SID.
- Security Key.

Web interface

To check the wireless link parameters go to the "Basic settings" - Link settings" section. Make sure that the "Enable Link" checkbox is on.

[35] https://academy.infinetwireless.com/en/configuration_generator



rf6.0

General Settings

Enable Link: ☑

Type: Master

Mode: Fixed

Max Links:

Frame Size (ms): 5 Auto: ☑ Turbo: ☑

DL/UL ratio (%): Max Range (Km): 70

STA RSSI (dBm): -40

DFS: DFS Only

Tx Power (dBm): 12 Auto: ☑ 0

Node Name: BSE

Scrambling: □

Trap gateway: □

Switch Border: □

Network Entry SNR (dB): Low 0 High 4

RX Attenuation (dB):

Multicast Mode: Unicast 3

Authentication Mode: public

ODR: Disabled

OTA: Passive

Log Level: normal

Current Settings

Mode: 802.11ac

Channel Width (MHz): 80

Frequency (MHz): 6020

Frequency Range List:

Tx Bitrate (Kbps): Max Auto: ☑ 0

Channel Type: Dual

Network SID: 10101010

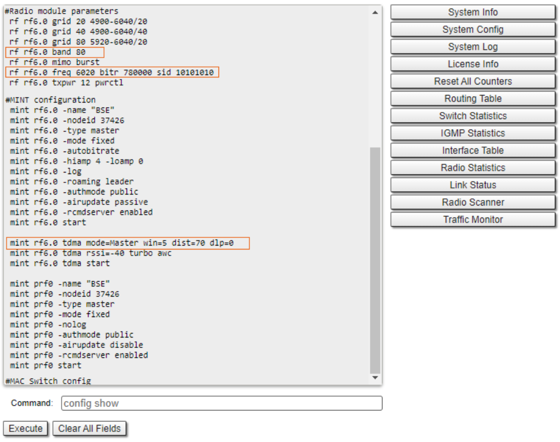
Node ID: 37426

Security Key:

90 Figure - Checking radio parameters in the web interface

Command line interface

Use the "*config show*" command to check the configuration via the CLI.



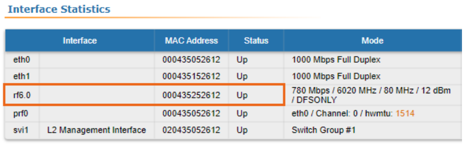
```
#Radio module parameters
 rf rf6.0 grid 20 4900-6040/20
 rf rf6.0 grid 40 4900-6040/40
 rf rf6.0 grid 80 5920-6040/20
 rf rf6.0 band 80
 rf rf6.0 mimo burst
 rf rf6.0 freq 6020 bitr 780000 sid 10101010
 rf rf6.0 txpwr 12 pwrctl

#MINT configuration
 mint rf6.0 -name "BSE"
 mint rf6.0 -nodeid 37426
 mint rf6.0 -type master
 mint rf6.0 -mode fixed
 mint rf6.0 -autobitrate
 mint rf6.0 -hiamp 4 -loamp 0
 mint rf6.0 -log
 mint rf6.0 -roaming leader
 mint rf6.0 -authmode public
 mint rf6.0 -airupdate passive
 mint rf6.0 -rcmdserver enabled
 mint rf6.0 start

 mint rf6.0 tdma mode=Master win=5 dist=70 dlp=0
 mint rf6.0 tdma rssi=-40 turbo awc
 mint rf6.0 tdma start

 mint prf0 -name "BSE"
 mint prf0 -nodeid 37426
 mint prf0 -type master
 mint prf0 -mode fixed
 mint prf0 -nolog
 mint prf0 -authmode public
 mint prf0 -airupdate disable
 mint prf0 -rcmdserver enabled
 mint prf0 start

#MAC Switch config
```

Command: config show

91 Figure - Checking radio parameters via the CLI

Checking the status of the radio interface

Make sure that the radio interfaces of both devices are in the "Up" state.

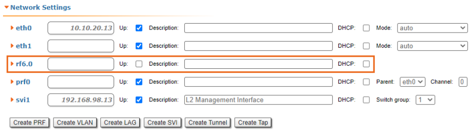


Interface Statistics

Interface		MAC Address	Status	Mode
eth0		000435052612	Up	1000 Mbps Full Duplex
eth1		000435152612	Up	1000 Mbps Full Duplex
rf6.0		000435252612	Up	780 Mbps / 6020 MHz / 80 MHz / 12 dBm / DFSONLY
prf0		000435052612	Up	eth0 / Channel: 0 / hwmtu: 1514
svi1	L2 Management Interface	020435052612	Up	Switch Group #1

92 Figure - Checking the interface status

If the status of the interface is "Down", enable the radio interface in the "Network settings" section by clicking the checkbox.



Network Settings

- eth0 10.10.20.13 Up: ☑ Description: DHCP: □ Mode: auto
- eth1 Up: ☑ Description: DHCP: □ Mode: auto
- rf6.0 Up: □ Description: DHCP: □
- prf0 Up: ☑ Description: DHCP: □ Parent: eth0 Channel: 0
- svi1 192.168.98.13 Up: ☑ Description: L2 Management Interface DHCP: □ Switch group: 1

93 Figure - Changing the interface status

If the device does not have a radio interface, the reason for such behavior can be the recovery mode present during the reset of the device using the ERConsole(see page 156). Complete the recovery process by returning the device to the factory settings from the Maintenance section.

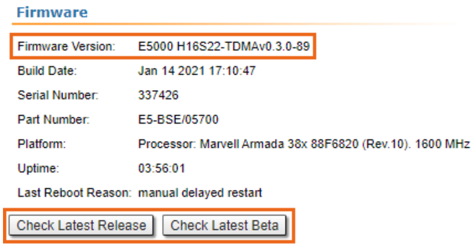
Pay attention to the red values of the parameters in the interface statistics "Mode" column:

- Operating frequency - red value of this parameter indicates an absence of data transmission due to the spectrum scanning by the DFS tool;
- TX Power - red value for this parameter may indicate a problem with the transceiver's hardware.

Checking the firmware version

Web interface

In the "Maintenance(see page 129)" section, make sure that the same software version is installed on both device. We recommend to update the devices to the latest beta software version.



Firmware

Firmware Version: E5000 H16S22-TDMAv0.3.0-89
Build Date: Jan 14 2021 17:10:47
Serial Number: 337426
Part Number: E5-BSE/05700
Platform: Processor: Marvell Armada 38x 88F6820 (Rev.10). 1600 MHz
Uptime: 03:56:01
Last Reboot Reason: manual delayed restart

94 Figure - Checking the firmware version

The latest software versions can be downloaded from the official Infinet FTP server[36].

Command line interface

To upload the software via the command line, use the "*flashnet*" command described in the "General Purpose Command Set[37]" article.

8.2.2 Checking the installation requirements

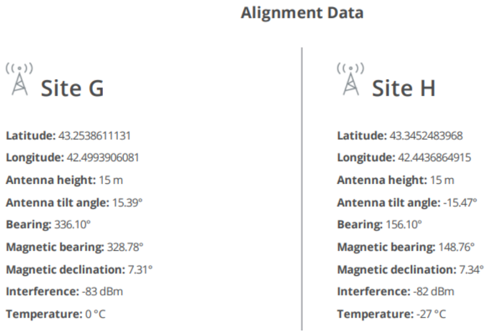
Checking the network infrastructure

If the link is not established after the installation on site, make sure that the devices were not damaged during shipping, check the integrity of the network infrastructure, the cables and the power supplies.

[36] ftp://ftp.infinetwireless.com/pub/Firmware
[37] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-flashnet

Checking the installation requirements

Check if the suspension height, azimuth and elevation of the antenna match with the values obtained from InfiPLANNER[38]. Make sure that the obstacles on the path profile are not higher than those specified during the planning phase.



Alignment Data

Site G

Latitude: 43.2538611131
Longitude: 42.4993906081
Antenna height: 15 m
Antenna tilt angle: 15.39°
Bearing: 336.10°
Magnetic bearing: 328.78°
Magnetic declination: 7.31°
Interference: -83 dBm
Temperature: 0 °C

Site H

Latitude: 43.3452483968
Longitude: 42.4436864915
Antenna height: 15 m
Antenna tilt angle: -15.47°
Bearing: 156.10°
Magnetic bearing: 148.76°
Magnetic declination: 7.34°
Interference: -82 dBm
Temperature: -27 °C

95 Figure - InfiPLANNER report with installation data

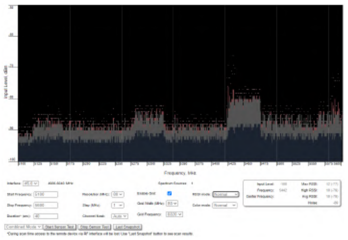
Interference detection

Web interface

Using the built-in Spectrum Analyzer tool, scan the air on both sides of the link to make sure there is no interference that could corrupt the signal on the device's operating frequency and on the adjacent frequencies. The current modulation (bit rate) will be selected by the device depending on the carrier to interference and noise ratio (CINR). To operate at higher modulations, the CINR parameter must be greater or equal to 28 dB. To get accurate information about the frequency, hover the mouse cursor over it. The pop-up window below provides information about frequency, noise level (in dBm), maximum signal level (Max RSSI), average signal level (Average RSSI). The "High RSSI" indicator allows to estimate the number of signal sources. If the value differs significantly from the average RSSI, then there are several interference sources. The indicators show the signal level in dB, while the signal in dBm is indicated in parentheses.

NOTE

It is recommended to run the spectrum scanning simultaneously on both devices to avoid a misrepresentation due to the signal received from the remote device.



96 Figure - Spectrum analyzer

Command line interface

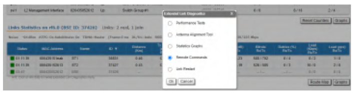
[38] https://infiplanner.infinetwireless.com/

The radio environment analysis is also available via the command line using the "*muffer sensor*[39]" command.

8.3 The wireless link is established, but there is no access to the remote device

8.3.1 Configuration analysis

In the web interface go to the section "Device status" → "Link statistics on rf6.0 interface", then left-click on the device to which the access is missing. Select "Remote commands".



97 Figure - Remote commands

In the pop-up window enter "config show". If the devices are configured via telnet, access to the remote device can be obtained with the "*mint rf6.0 rcmd*[40]" command.

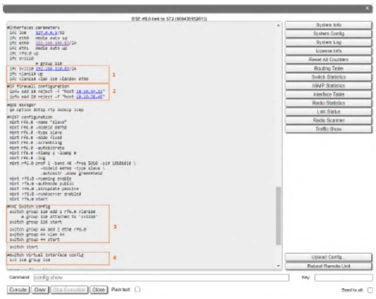
"Vlan" interfaces

Make sure that the "vlan" interfaces are configured in accordance with the company's security policy (see point 1 in the figure below). The VLAN configuration process using the command line is described in the "VLAN configuration[41]" article.

Filtering rules

Pay attention to the traffic filtering rules in the switch group and in the "IP Firewall menu (see page 118)" subsection (point 2).

[39] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=10780956
[40] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=42274923#mintcommand(TDMAversion)-RemoteCommandManagement
[41] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=17597370


BSE rf6.0 link to ST2 (000435652615)

```
#Interfaces parameters
 ifc lo0    127.0.0.1/32
 ifc eth0   media auto up
 ifc eth0   192.168.100.63/24
 ifc eth1   media auto up
 ifc rf6.0 up
 ifc svi110
            # group 110
 ifc svi110 192.168.110.85/24
 ifc vlan110 up
 ifc vlan110 vlan 110 vlandev eth0
#IP firewall configuration
 ipfw add 10 reject -f "host 10.10.34.31"
 ipfw add 20 reject -f "host 10.10.38.45"
#QoS manager
 qm option dotip rtp msdcp icmp
#MINT configuration
 mint rf6.0 -name "slave"
 mint rf6.0 -nodeid 60758
 mint rf6.0 -type slave
 mint rf6.0 -mode fixed
 mint rf6.0 -scrambling
 mint rf6.0 -autobitrate
 mint rf6.0 -hlamp 2 -lcamp 0
 mint rf6.0 -log
 mint rf6.0 prof 1 -band 40 -freq 5050 -sid 10101010 \
             -nodeid 60758 -type slave \
             -autobitr -mimo greenfield
 mint rf6.0 -roaming enable
 mint rf6.0 -authmode public
 mint rf6.0 -airupdate passive
 mint rf6.0 -roamserver enabled
 mint rf6.0 start
#MAC Switch config
 switch group 110 add 1 rf6.0 vlan110
      # group 110 attached to 'svi110'
 switch group 110 start
 switch group 44 add 2 eth0 rf6.0
 switch group 44 vlan 44
 switch group 44 start
 switch start
#Switch virtual interface config
 svi 110 group 110
```

Command: config show

98 Figure - Display configuration

8.3.2 Checking the switch settings on the remote device

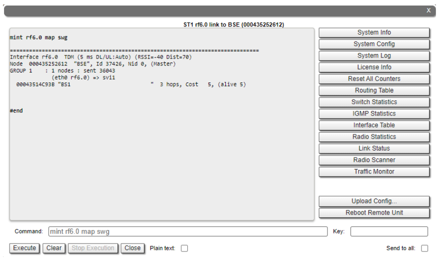
Device management

Make sure that the switch group for the device management is configured correctly (see point 3 in the figure above):

- To access the device via the radio interface, the rf6.0 interface must be added to the management switch group.
- The svi interface must be associated with the switch group. The interface can be associated using the "*svi*[42]" command (point 4).
- The device's management IP address must be assigned to the svi interface using the "ifconfig[43]" command (point 1). The switch groups are configured using the "switch[44]" command.

Checking the members of the switch group

To display information about the devices included in the switch groups, use the "mint rf6.0 map swg[45]" command.


ST1 rf6.0 link to BSE (000435252612)

```
mint rf6.0 map swg

==============================================================================
Interface rf6.0  TDM (5 ms DL/UL:Auto) (RSSI=-40 Dist=70)
Node  000435252612  "BSE", Id 37426, Nid 0, (Master)
GROUP 1    : 1 nodes : sent 36043
             (eth0 rf6.0) => svi1
  00043514C93B "BS1                         "  3 hops, Cost   5, (alive 5)



#end
```

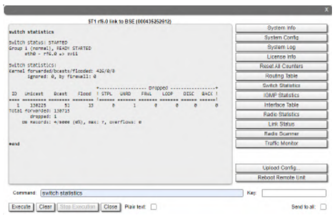
Command: mint rf6.0 map swg

99 Figure - Checking the switch group

Switch statistics

To display statistics about the dropped/blocked MAC addresses for each switch group, use the "switch statistics[46]" command.

[42] https://wiki.infinetwireless.com/display/DR/svi+command
[43] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=10781004
[44] https://wiki.infinetwireless.com/display/DR/switch+command
[45] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=42274923#mintcommand(TDMAversion)-CurrentConnectionsInformation
[46] https://wiki.infinetwireless.com/display/DR/switch+command#switchcommand-Managementcommands



```
switch statistics

Switch status: STARTED
Group 1 (normal), READY STARTED
      eth0 - rf6.0 => svi1

Switch statistics:
Kernel forwarded/bcasts/flooded: 436/0/0
       ignored: 0, by firewall: 0

                                 +------------------ Dropped -----------------+
 ID   Unicast     Bcast     Flood ! STPL    UNRD    FRWL    LOOP    DISC   BACK !
==== ========= ======== ======== !====== ======= ======= ======= ====== ======!
  1    130225       51       15       0       1       0       0      0      0
Total forwarded: 130715
        dropped: 1
     DB Records: 4/8000 (0%), max: 7, overflows: 0


#end
```

Command: switch statistics

100 Figure - Switch statistics

8.3.3 Checking the switch settings on the local device

Device management

Make sure that the switch group ID assigned for management on the local device matches with the switch group ID on the remote device. Make sure that the rf6.0 interface has been added to the switch group. The svi interface must be associated with the switch group and its IP address is used for the management of the device. For detailed information about the device management configuration proceed to the "Remote management of the R5000 units[47]" article.

Filtering rules

Pay attention to the traffic filtering rules in the switch group and in the "*IPFirewall*" subsection. Make sure that the traffic from the remote device is not restricted.

8.4 The wireless link throughput is lower than expected

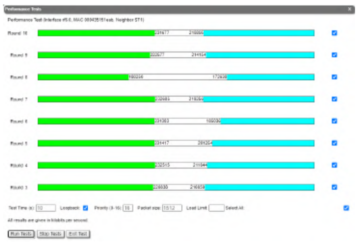
8.4.1 Performance tests

Web interface

The throughput test can be performed with the "Performance Tests" tool built into the web interface, in the section "Device status" → "Link statistics for the rf6.0 interface". This tool generates test traffic between the devices and it allows to obtain data about the real link throughput both in one direction and in a two-way manner. The throughput evaluation is performed using traffic with the specified priority without taking into account the service traffic required to maintain the link operational. To exclude the influence of the data traffic on the test's result, it is recommended to set the highest priority for the test traffic (at least 15). Performance tests are always performed on

[47] https://wiki.infinetwireless.com/display/DR/Remote+management+of+the+R5000+units

the highest modulation,the detailed description of the parameters and the performance test settings are available in the "Device Status menu(see page 64)" article.



Test Time (s): 10 Loopback: ☑ Priority (9-16): 16 Packet size: 1512 Load Limit: Select All: ☑

All results are given in kilobits per second.

101 Figure - Performance tests

Command line interface

When using the command line interface to manage the device, it is possible to test the radio link via the "ltest[48]" command.

8.4.2 Wireless link status

Link statistics on the rf6.0 interface

Web interface

To evaluate the quality of the wireless connection with the neighboring device, use the color indication in the "Status" column of the "Link statistics on rf5.0" subsection:

- Red: bad connection.
- Yellow: good connection.
- Green: perfect connection.

The following symbols indicate problems:

- In the wireless connection uptime column:
  - F - the local device has a newer software version than the remote device.
  - E - the Ethernet port of the remote device is flapping.
- In the TX power column:
  - * - hardware device failure.
- In the RSSI column:
  - * - significant difference in the signal power between the vertical and horizontal polarizations.

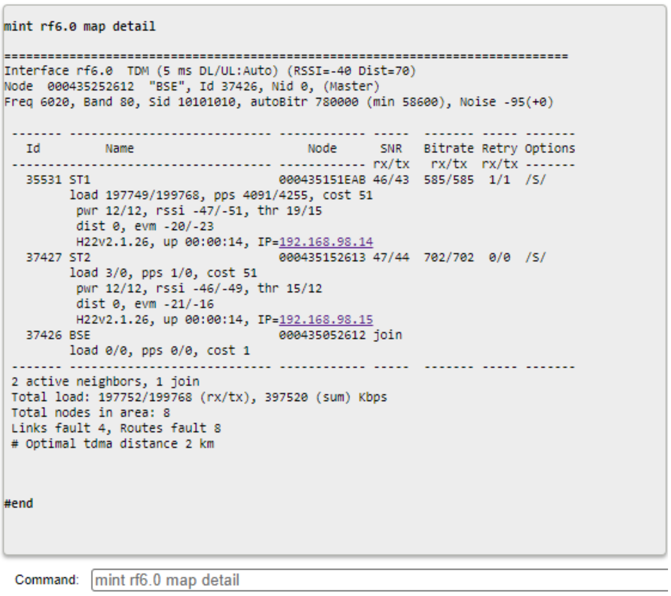
Make sure that the "TX Power" and "Bitrate" parameters match with the values of the planning phase. In the "Link statistics on rf6.0" of the "Device status" section, pay attention to the wireless connection parameters. The main parameters are the retries number and the bitrate. It is not recommended to use the link with a retries number exceeding 5%. The actual bitrate (modulation level) depends on the SNR parameter - the signal-to-noise ratio. The highest modulations are available at SNR values of 27-50 dB.

For detailed description of the link parameters proceed to the "Device Status menu(see page 64)" article.

Command line interface

To display information about the wireless link status via the command line interface, use the "mint rf6.0 map detail[49]" command.

[48] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=10780952
[49] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=42274923#mintcommand(TDMAversion)-CurrentConnectionsInformation



```
mint rf6.0 map detail

=============================================================================
Interface rf6.0  TDM (5 ms DL/UL:Auto) (RSSI=-40 Dist=70)
Node  000435252612  "BSE", Id 37426, Nid 0, (Master)
Freq 6020, Band 80, Sid 10101010, autoBitr 780000 (min 58600), Noise -95(+0)

 ------- ---------------------------- ----------- -----  ------- ----- -------
   Id         Name                        Node     SNR   Bitrate Retry Options
 ------------------------------------ ----------- rx/tx   rx/tx  rx/tx -------
   35531 ST1                          000435151EAB 46/43  585/585  1/1  /S/
         load 197749/199768, pps 4091/4255, cost 51
          pwr 12/12, rssi -47/-51, thr 19/15
          dist 0, evm -20/-23
          H22v2.1.26, up 00:00:14, IP=192.168.98.14
   37427 ST2                          000435152613 47/44  702/702  0/0  /S/
         load 3/0, pps 1/0, cost 51
          pwr 12/12, rssi -46/-49, thr 15/12
          dist 0, evm -21/-16
          H22v2.1.26, up 00:00:14, IP=192.168.98.15
   37426 BSE                          000435052612 join
         load 0/0, pps 0/0, cost 1
 ------- ---------------------------- ----------- -----  ------- ----- -------
 2 active neighbors, 1 join
 Total load: 197752/199768 (rx/tx), 397520 (sum) Kbps
 Total nodes in area: 8
 Links fault 4, Routes fault 8
 # Optimal tdma distance 2 km


#end
```

102 Figure - The "mint rf6.0 map detail" command output

Pay attention to the indicators in the "Options" column. The following values are possible:

- M - Master device;
- S - Slave device;
- TM - Master device with software having support for the TDMA technology;
- L - the throughput is limited by license;
- F - the software version is older than the one on the local device.

A question mark in front of the remote's device name indicates that it has no password.

Pay attention to the "*" symbol, which can represent the following:

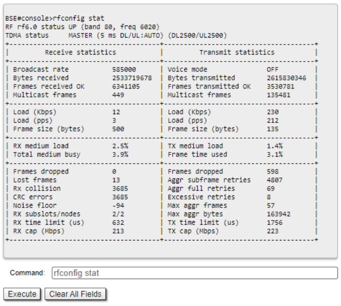
- At the "pwr" column - hardware device failure.
- At the "rssi" column - significant difference between the signal power of the vertical and horizontal polarizations.

Radio statistics

Command line interface

To display statistics via the command line interface, use the ""*rfconfig stat*[50]" command.

[50] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=43827064



```
BSE#console>rfconfig stat
RF rf6.0 status UP (band 80, freq 6020)
TDMA status     MASTER (5 ms DL/UL:AUTO) (DL2500/UL2500)
+---------------------------------------+---------------------------------------+
|         Receive statistics            |         Transmit statistics           |
+---------------------------------------+---------------------------------------+
| Broadcast rate          585000        | Voice mode              OFF           |
| Bytes received          2533719678    | Bytes transmitted       2615830346    |
| Frames received OK      6341105       | Frames transmitted OK   3530781       |
| Multicast frames        449           | Multicast frames        135481        |
+---------------------------------------+---------------------------------------+
| Load (Kbps)             12            | Load (Kbps)             230           |
| Load (pps)              3             | Load (pps)              212           |
| Frame size (bytes)      500           | Frame size (bytes)      135           |
+---------------------------------------+---------------------------------------+
| RX medium load          2.5%          | TX medium load          1.4%          |
| Total medium busy       3.9%          | Frame time used         3.1%          |
+---------------------------------------+---------------------------------------+
| Frames dropped          0             | Frames dropped          598           |
| Lost frames             13            | Aggr subframe retries   4807          |
| Rx collision            3685          | Aggr full retries       69            |
| CRC errors              3685          | Excessive retries       8             |
| Noise floor             -94           | Max aggr frames         57            |
| RX subslots/nodes       2/2           | Max aggr bytes          163942        |
| RX time limit (us)      632           | TX time limit (us)      1756          |
| RX cap (Mbps)           213           | TX cap (Mbps)           223           |
+---------------------------------------+---------------------------------------+
```

Command: rfconfig stat

103 Figure - General statistics

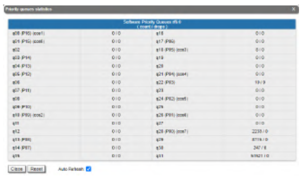
Pay attention to the following indicators:

- "Lost Frames" - the number of frames that were not received by the device, even after retrying.
- "Aggr Subframe Retries" and "Aggr Full Retries" - the number of frames that the device has sent several times because the other side did not acknowledge the receipt.
- "Excessive Retries" - the number of frames that failed to to be sent after all the retry attempts.

QoS statistics

Web interface

The "QoS statistics" section provides information about the transmitted and dropped packets in each priority queue configured on the device. Drops present in the traffic processing queues indicate that the throughput threshold has been exceeded. Losses in queue q00 (P16) are acceptable because this queue contains performance test data.



Software Priority Queues rf6.0 (count / drops)			
q00 (P16) (cos1)	0 / 0	q16	0 / 0
q01 (P15) (cos6)	0 / 0	q17 (P06)	0 / 0
q02	0 / 0	q18 (P05) (cos3)	8 / 0
q03 (P14)	0 / 0	q19	0 / 0
q04 (P13)	0 / 0	q20	0 / 0
q05 (P12)	0 / 0	q21 (P04) (cos4)	0 / 0
q06	0 / 0	q22 (P03)	10 / 0
q07 (P11)	0 / 0	q23	0 / 0
q08	0 / 0	q24 (P02) (cos5)	0 / 0
q09 (P10)	0 / 0	q25	0 / 0
q10 (P09) (cos2)	0 / 0	q26 (P01) (cos6)	0 / 0
q11	0 / 0	q27	0 / 0
q12	0 / 0	q28 (P00) (cos7)	2233 / 0
q13 (P08)	0 / 0	q29	8716 / 0
q14 (P07)	0 / 0	q30	247 / 8
q15	0 / 0	q31	[illegible] / 0

104 Figure - QoS statistics

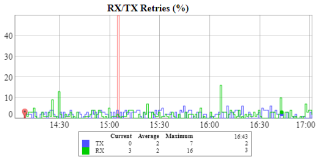
Command line interface

To display statistic via the command line interface, use the "rfconfig rf6.0 stat qos[51]" command. The number of dropped packets for each configured queue can be displayed by the "*qm stat*[52]" command.

8.4.3 Statistics graphs

If the link has deteriorated during its operation, having the initial parameters corresponding to the calculated ones, it is necessary to find out when the problem has occured. Use the "Statistics graphs" tool to determine when or how often the problem occurs by changing the display options.

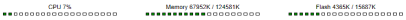
[51] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=43827064
[52] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=10781010



105 Figure - Statistics graphs

8.4.4 Device status

Pay attention to the CPU and memory usage indicators in the "Device status(see page 64)" section. Excessive processes running on a device can overflow the volatile memory and overload the CPU (over 95% usage), leading to a deterioration in the wireless link's quality. The CPU load can be displayed using the "system cpu[53]" command and information about the device's memory state can be shown using the "mem[54]" command.



106 Figure - CPU and memory usage

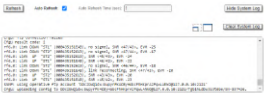
8.4.5 Last reboot reason

Disruptions in the wireless link may be caused by the reboot of the device. In the "Maintenance(see page 129)" section or in the "system uptime[55]" command output pay attention to the last device reboot reason. The following values are possible:

- "*Software fault*".
- "*Unexpected restart*".
- "*Manual restart*".
- "*Manual delayed restart*".
- "*Firmware upgrade*".
- "*SNMP managed restart*".
- "*Test firmware loaded*".
- "*Power-on reset*".

8.4.6 System log

Proceed to the System Log tool in the "Device status" section or by using the "system log[56]" command. Using the log entries, check if the link degradation was caused by a configuration change ("system reconfiguration" message). Restore the previous version of the configuration if necessary. Detailed information about saving and uploading the configuration is available in the "General Purpose Command Set[57]" article.



```
[illegible]
CfgU result code: 1
rf6.0: link DOWN "STL" [illegible], no signal, SNR [illegible], EVM -25
rf6.0: link DOWN "ST2" [illegible], no signal, SNR [illegible], EVM -17
rf6.0: link  UP  "ST2" [illegible], SNR [illegible], EVM -24
rf6.0: link  UP  "STL" [illegible], SNR [illegible], EVM -22
rf6.0: link DOWN "ST2" [illegible], no signal, SNR [illegible], EVM -18
rf6.0: link DOWN "STL" [illegible], link reconnecting, SNR [illegible], EVM -28
rf6.0: link  UP  "ST2" [illegible], SNR [illegible], EVM -28
rf6.0: link  UP  "STL" [illegible], SNR [illegible], EVM -22
[illegible] using operative ftp account [illegible]
CfgU uploading config to [illegible]
```

107 Figure - System log

[53] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-system
[54] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-mem
[55] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-system
[56] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-system
[57] https://wiki.infinetwireless.com/display/DR/General+Purpose+Command+Set#GeneralPurposeCommandSet-config

Pay attention to the following messages:

Messages in the log	Description
Link DOWN	The wireless link has disconnected. The reason for the disconnection is indicated in the same entry.
"too many transmit errors"	The wireless link was interrupted due to transmission errors.
"link reconnecting"	The wireless link is reestablished.
"no signal from the remote side detected"	There is no signal received, check the remote device.
Scrambling engine overflow	The hardware capabilities of the scrambling module are exceeded. To connect more subscribers (more than 62) scrambling should be disabled.
Warning: Abnormal transmit power disbalance!	May indicate a hardware problem.

Frequent changes in the status of the Ethernet interface ("Up" and "Down") may indicate problems with the Ethernet interface, the cable connected to it, with the power supply, or with the switch.

8.4.7 Antenna alignment

Web interface

The link degradation can be caused by antenna misalignment or by the appearance of obstacles along the signal's propagation path. Use the built-in "Antenna Alignment Tool". The recommended parameters are shown in the table below. If the parameters differ significantly from the calculated ones, check the alignment accuracy on both link sides.

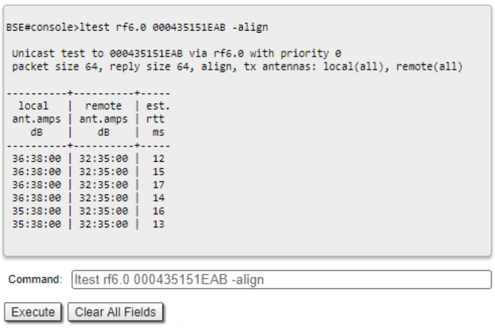
RSSI (dBm)	
-90 ... -80	The value is close to the receiver sensitivity level, only lower modulations are available
-80 ... -60	Low level. Average modulations are available
-60 ... -40	The recommended value for maximum performance
>-40	The received signal level is too high
Absolute value EVM (dB)	

>21	Recommended value
CINR (dB)	
>28	Higher modulations are available
Absolute value Crosstalk (dB)	
>20	Recommended value

If the value of the RSSI parameter remains high while the CINR value decreases, it may indicate high interference levels near one of the devices. The deterioration of both the RSSI and the CINR parameters can indicate a misalignment of the devices. A detailed description of the "Antenna Alignment" tool is available in the "Device status menu(see page 64)" article.

Command line interface

When using the command line to manage the device, fine antenna alignment can be performed using the "ltest rf6.0 MAC ADDRESS -align[58]" command. The command output will show the average CINR for the local and the remote devices.



```
BSE#console>ltest rf6.0 000435151EAB -align

 Unicast test to 000435151EAB via rf6.0 with priority 0
 packet size 64, reply size 64, align, tx antennas: local(all), remote(all)

----------+----------+-----
  local   |  remote  | est.
 ant.amps | ant.amps | rtt
    dB    |    dB    |  ms
----------+----------+-----
 36:38:00 | 32:35:00 |  12
 36:38:00 | 32:35:00 |  15
 36:38:00 | 32:35:00 |  17
 36:38:00 | 32:35:00 |  14
 35:38:00 | 32:35:00 |  16
 35:38:00 | 32:35:00 |  13
```

Command: ltest rf6.0 000435151EAB -align

108 Figure - "ltest - align" command output

8.5 Common errors in configuration

Some device modes and options can significantly affect the link's stability and throughput.

- Autobitrate and ATPC(see page 156)
- Frame size(see page 156)
- Packet retries management(see page 156)

[58] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=10780952

8.5.1 Autobitrate and ATPC

To keep a balance between the wireless link's performance and the retries number, we recommend to always set the "Bitrate" parameter to "Auto" mode. Also enable the automatic transmit power control (ATPC) in order to increase the operational life of the devices.

8.5.2 Frame size

Make sure that the selected frame size ensures the best performance for your wireless system. A short frame will transmit less payload than a long one, however it ensures a smaller delay. A detailed description of the frame sizes in the TDMA technology is available in the "TDMA and Polling: Application features[59]" article.

8.5.3 Packet retries management

The "Turbo" mode is available in the TDMA software version, which allow to increase the wireless link throughput in case that the degradation is caused by a large number of errors in the radio.

Detailed information about the radio parameter configuration via the web interface is available in the "Link Settings (see page 91)" article or via CLI in the articles: "mint command (TDMA version)[60]" and "rfconfig command (TDMA version)[61]".

8.6 Emergence Repair Console

If the management of the unit is completely lost (of the local and/or the remote one), the ERConsole recovery procedure should be used. ERConsole is a software application created to recover or add a new IP address to the InfiNet Wireless units. Additionally, the ERConsole can be used to reset the Infinet Wireless units to the factory default configuration.

8.6.1 ERConsole recovery procedure

Required software

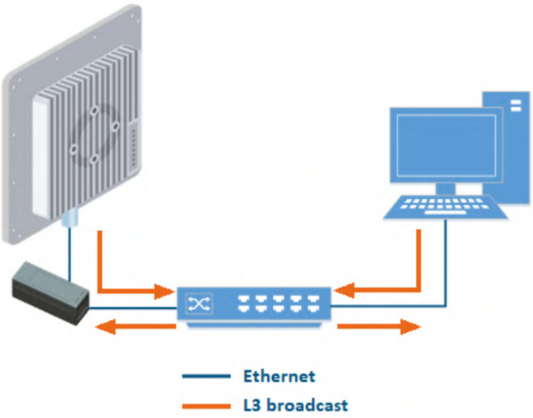
- Java Runtime Environment should be installed. Please download it if it is not installed: http://www.java.com/en/download/
- Download ERConsole from our ftp site: ftp://ftp.infinet.ru/pub/Utils/EmergenceRepairConsole/ERConsole.zip

Network Requirements

- Turn off any anti-virus or firewall running on your computer. If no device can be discovered by ERConsole, turn on the firewall, and add an UDP connection port 10009 as an exception.
- Use a simple unmanaged switch as intermediary device between your PC and the **Infinet** unit. It is essential to reboot the InfiNet unit each time in order to activate the Emergency Repair Protocol on the unit, therefore

[59] https://wiki.infinetwireless.com/display/DR/TDMA+and+Polling%3A+Application+features
[60] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=42274923
[61] https://wiki.infinetwireless.com/pages/viewpage.action?pageId=43827064

the switch would prevent your PC Ethernet interface from flapping up and down. Using Cisco Catalyst switches for unit recovery is not recommended due to a known issue port mode negotiation delay.
- IP address should be configured on the PC for the ERConsole utility work.



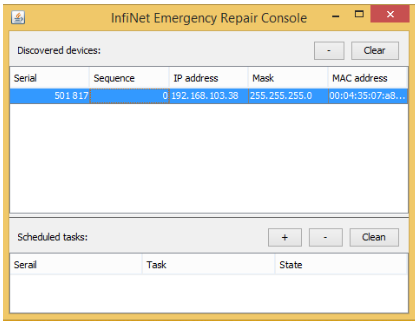
109 Figure - The recommended connection scheme

- Set default gateway address to the same network interface configuration connected to Infinet Wireless unit or to switch connected with Infinet Wireless unit. Turn off all the network interfaces (except Ethernet interface connected to Infinet Wireless unit).

> **NOTE**
>
> ERConsole and InfiNet Wireless units exchange information only during the bootup process, therefore each time you need to read the units IP-address, to add a new IP-address or to restore to the default configuration, the InfiNet Wireless unit should be rebooted.

Step-by-step instruction to obtain or add additional IP-address via ERConsole operation

1. Run the ERConsole.jar application downloaded from our FTP.
2. Connect a network Ethernet cables between the Infinet Wireless unit, unmanaged switch and your PC, as shown in the figure above.
3. Turn off the InfiNet Wireless unit by removing ethernet cable from power supply unit and then turn it on in a few seconds.
4. Wait for 30 seconds and the ERConsole screen should receive update from the unit as shown in the figure below. The Serial number, number of device reset cycles ("*Sequence*" field), IP-address, network mask and MAC-adress will be displayed on the screen.

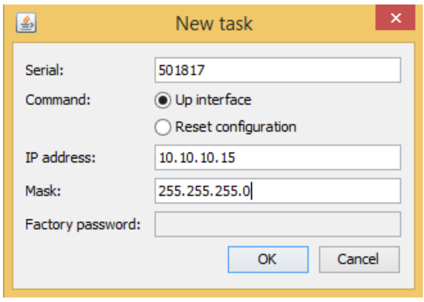


Serial	Sequence	IP address	Mask	MAC address
501 817	0	192.168.103.38	255.255.255.0	00:04:35:07:a8...

Serail	Task	State

110 Figure - ERConsole information

5. If an IP-address is assigned to the unit, configure on your laptop an IP-address belonging to the same network and connect to the unit. If there is no IP-address displayed (0.0.0.0), proceed with the next step.
6. If there is more than one unit on the list, please, select the required unit.
7. Click the «**+**» button in the ERConsole application and a new window will appear.
8. In the new task window, set the additional IP-address and network mask, then click «**OK**».



New task

Serial: 501817

Command: ● Up interface ○ Reset configuration

IP address: 10.10.10.15

Mask: 255.255.255.0

Factory password:

111 Figure - Adding a new IP address

9. Turn off and on the InfiNet unit. Wait for about 30 seconds until the "Complete" sign will appear.
10. Add an IP-address from the same network subnet to your PC and access the unit. ERConsole will not show newly assigned IP-address.
11. Login to the unit using the new IP-address. Do not reboot the unit now because the IP-address added by ERConsole is temporar until the new configuration has been saved.

8.6.2 Restore to factory default settings using ERConsole

If you need to restore your unit to the factory default settings, follow the instructions below:

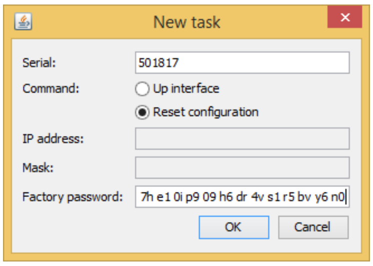
> **NOTE**
>
> If the management of the unit is lost due to unknown user name or password it can be restored using factory password. Put an serial number of device in the "User name" field and factory password in the "Password" field. User's PC and InfiNet unit should belong to the same subnet.

1. Obtain the IP-address of the unit using the ERConsole as described in the section above.
2. Click on the «**+**» button in the ERConsole application and a new window will appear.
3. Obtain the Factory Password. In order to do this, please contact the distributor which the device was purchased from. The request must include the device serial number and the value of "Sequence" field (if it's non-zero).

   > **NOTE**
   >
   > In case of purchasing the unit directly in InfiNet Wireless, you may send a request to the InfiNet Wireless Technical support to support@infinetwireless.com[62]. Please be ready to provide a purchasing confirmation.

4. Select “Reset configuration” option and enter the Factory Password obtained at the previous step in the "Factory password" field, then click «**OK**». The password must be entered the same format as it has been got it from the distributor or IW support (with the gaps).

[62] mailto:support@infinetwireless.com



Serial: 501817

Command: ○ Up interface ● Reset configuration

IP address:

Mask:

Factory password: 7h e1 0i p9 09 h6 dr 4v s1 r5 bv y6 n0

112 Figure - Reset configuration

5. Turn off and on the unit and then wait for about 30 seconds until the "Complete" sign will uppear.
6. The unit will start in special emergency mode with the IP-address 10.10.10.1 and mask 255.255.255.0.
7. Login to the unit and use "Restore Factory Settings" button on the "Maintenance" page if you use Web GUI or by command "*config clear*" by CLI to switch off emergency mode.
8. Set new login and password, then save the configuration and restart the unit.

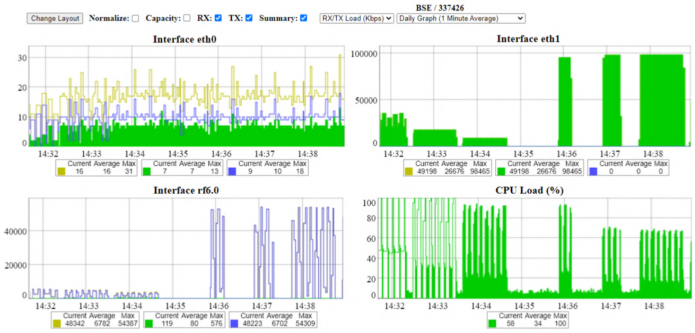
8.7 Unicast-flood detection

Unicast-flood occurs when the unicast frame's destination MAC-address is unknown for the switch (not included in its routing table), it sends this frame to all interfaces of the network, besides the sender interface. The most common reasons of unicast-flood are:

- MAC address table overflow (a common problem in large networks)
- Hosts with ARP timers longer than the ARP cache time on switches
- Incorrect STP settings
- Incorrect switch groups settings (in particular, when the IDs of switch groups for the receiving and sending traffic are different).

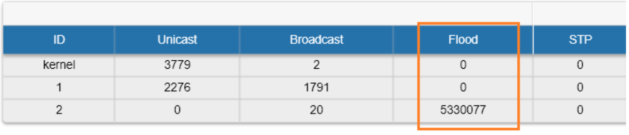
The unicast-flood process on devices is the following: if the frame's destination MAC-address is not included in the unit's MAC switch forwarding table, then this frame is flooded to all interfaces besides the sender interface. The distribution occurs until the unit receives a frame with this MAC-address as the sender (i.e., the interface to which the frame was destinated to respond). After that, the device will learn: it will add this MAC address to the MAC switch forwarding table and map it with the interface from which it was received. If the device does not learn in 4 seconds, and frames still arrive, then traffic to this direction will be blocked for 4 seconds. Then the process repeats.

This process has the following representation in the unit's interfaces and links graphs:



113 Figure - Unicast-flood example in the interfaces graphs

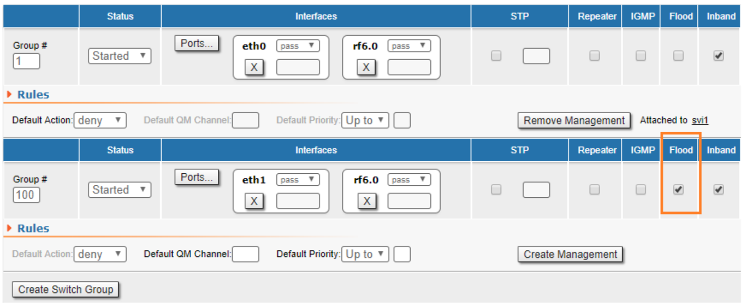
Also, unicast-flooding can be detected in the "Switch Statistics" → "Device Status" tab in "Flood" column:



ID	Unicast	Broadcast	Flood	STP
kernel	3779	2	0	0
1	2276	1791	0	0
2	0	20	5330077	0

114 Figure - Unicast-flood detection in switch statistics

Infinet Wireless units provide unicast-flood protection. If necessary, you can allow unlimited unicast-flood without protection filter through the switch group by setting the check box in "Basic Settings" → "MAC Switch" settings:



	Status	Interfaces	STP	Repeater	IGMP	Flood	Inband
Group # 1	Started	Ports... eth0 pass X; rf6.0 pass X	□	□	□	□	☑

Rules

Default Action: deny Default QM Channel: Default Priority: Up to Remove Management Attached to svi1

	Status	Interfaces	STP	Repeater	IGMP	Flood	Inband
Group # 100	Started	Ports... eth1 pass X; rf6.0 pass X	□	□	□	☑	☑

Rules

Default Action: deny Default QM Channel: Default Priority: Up to Create Management

Create Switch Group

115 Figure - How to allow unicast-flood without protection filter

Devices react to unidirectional traffic (which is not a unicast-flood) in a similar manner. This happens, for example, in case of generating "artificial" traffic (using specialized units or software) or when the real traffic is unidirectional. In these cases, it is recommended to allow unlimited unicast-flood through the switch group without protection filter.

9 Glossary

- AC - Alternating Current
- AMC - Automatic Modulation Control
- ARQ - Automatic Repeat reQuest
- ATPC - Automatic Transmit Power Control
- DHCP - Dynamic Host Configuration Protocol
- DC - Direct Current
- DFS - Dynamic Frequency Selection
- ERC - Emergence Repair Console
- ETH - Ethernet
- EVM - Error Vector Magnitude
- FTP - File Transfer Protocol
- IP - Internet Ptotocol
- LBT - Listen Before Talk
- LOS - Line of Sight
- MAC - Media Access Control
- MCS - Modulation and Coding Scheme
- PHY - Physical layer
- PoE - Power over Ethernet
- QAM - Quadrature Amplitude Modulation
- QoS - Quality of Service
- QPSK - Quadrature Phase Shift Keying
- RF - Radio Frequency
- RSSI - Received Signal Strength Indicator
- SDR - Software-Defined Radio
- SC-FDE - Single-Carrier Frequency Domain Equalization
- STP - Spanning Tree Protocol
- TDD - Time Division Duplexing
- VLAN - Virtual Local Area Network