User Manual

WISE-6610 Series

Indsutrial LoRaWAN Gateway

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (3 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for three years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on screen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Part No. XXXXXXXXXX　　Edition 1
Printed in Taiwan　　December 2018

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

Caution! *Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.*

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Packing List

Before setting up the system, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- 1 x Indsutrial LoRa private gateway
- 1 x DIN-Rail mounting bracket and screws
- 1 x Wall-mounting bracket

Safety Instructions

- Read these safety instructions carefully.
- Keep this User Manual for later reference.
- Disconnect this equipment from any DC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- Keep this equipment away from humidity.
- Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
- The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
- Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- Position the power cord so that people cannot step on it. Do not place anything over the power cord.
- All cautions and warnings on the equipment should be noted.
- If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
- Never pour any liquid into an opening. This may cause fire or electrical shock.
- Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- If one of the following situations arises, get the equipment checked by service personnel:
  - The power cord or plug is damaged.
  - Liquid has penetrated into the equipment.
  - The equipment has been exposed to moisture.
  - The equipment does not work well, or you cannot get it to work according to the user's manual.
  - The equipment has been dropped and damaged.
  - The equipment has obvious signs of breakage.
- DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO -40°C (-40°F) ~ 85°C (185°F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
- The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

  DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.
- The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Wichtige Sicherheishinweise

- Bitte lesen sie Sich diese Hinweise sorgfältig durch.
- Heben Sie diese Anleitung für den späteren Gebrauch auf.
- Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie Keine Flüssig-oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
- Die NetzanschluBsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
- Das Gerät ist vor Feuchtigkeit zu schützen.
- Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen.
- Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor überhitzung schützt. Sorgen Sie dafür, daB diese Öffnungen nicht abgedeckt werden.
- Beachten Sie beim. AnschluB an das Stromnetz die AnschluBwerte.
- Verlegen Sie die NetzanschluBleitung so, daB niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
- Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
- Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
- Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
- Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
- Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
  - Netzkabel oder Netzstecker sind beschädigt.
  - Flüssigkeit ist in das Gerät eingedrungen.
  - Das Gerät war Feuchtigkeit ausgesetzt.
  - Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
  - Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
  - Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
- Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weiger.

  Haftungsausschluss: Die Bedienungsanleitungen wurden entsprechend der IEC-704-1 erstellt. Advantech lehnt jegliche Verantwortung für die Richtigkeit der in diesem Zusammenhang getätigten Aussagen ab.

Safety Precaution - Static Electricity

Static electricity can cause bodily harm or damage electronic devices. To avoid damage, keep static-sensitive devices in the static-protective packaging until the installation period. The following guidelines are also recommended:

- Wear a grounded wrist or ankle strap and use gloves to prevent direct contact to the device before servicing the device. Avoid nylon gloves or work clothes, which tend to build up a charge.
- Always disconnect the power from the device before servicing it.
- Before plugging a cable into any port, discharge the voltage stored on the cable by touching the electrical contacts to the ground surface.

Contents

List of Figures

Chapter 1

Product Overview

1.1 Specifications

Specifications	Description	
WSN Support	Standard	LoRaWAN
	Frequency	868/915 MHz
	ANT Connector	RP-SMA Female connector x 1
LAN Interface	Ethernet	10/100 Mbps, auto MDI/MDIX
	Connector	RJ45 x 1
	Protection	1.5-kV built-in magnetic isolation protection
Digital I/O	Port Type	Digital input on voltage: 2.7 ~ 36 V_{DC}
	Port Connector	4-way Molex moni-fit connector
General	LED Indicators	PWR, DAT, WAN, ETH
	Reboot Trigger	Reset button
Physical	Protection Class	IP30
	Installation	DIN rail, wall
	Dimensions (W x H x D)	150 x 37.5 x 83 mm (5.9" x 1.48" x 3.27")
	Weight	500 g (17.63 oz)
Environment	Operating Temperature	-40 ~ 75°C (-40 ~ 167°F)
	Storage Temperature	-40 ~ 85°C (-40 ~ 185°F)
	Ambient Relative Humidity	10 ~ 95% (non-condensing)
Power	Power Input	9 ~ 36 V_{DC}
	Power Connector	4-way Molex moni-fit connector
	Power Consumption	3.1/6.6/40 mW (average/peak/sleep mode)
Certifications	EMC	■ EN61000-4-2, Level 3 ■ EN61000-4-3, Level 3 ■ EN61000-4-4, Level 3 ■ EN61000-4-5, Level 3 ■ EN61000-4-6, Level 3 ■ EN61000-4-12, Level 3 ■ EN61000-4-11, voltage dip: 70%
	Shock	IEC60068-2-27
	Free Fall	IEC60068-2-32
	Vibration	IEC60068-2-6

1.2 Hardware Views

1.2.1 Front View

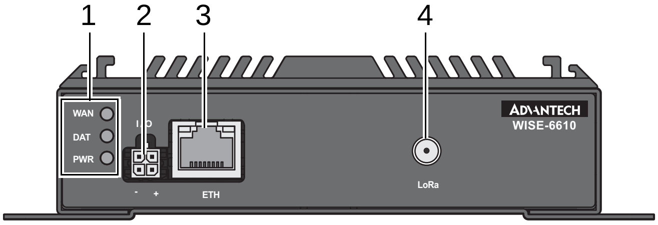


Figure 1.1 Front View

No.	Item	Description
1	System LED panel	See “System LED Panel” on page 4 for further details.
2	I/O (Power socket)	Connect cabling for power.
3	ETH port	RJ45 x 1
4	Antenna connector	Connector for antenna.

1.2.2 Rear View

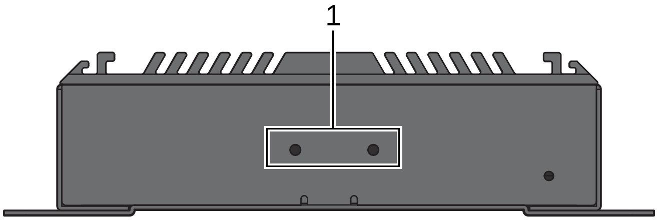


Figure 1.2 Rear View

No.	Item	Description
1	DIN-Rail holes	Screw holes (2) used in the installation of a DIN rail clip.

1.2.3 Top View

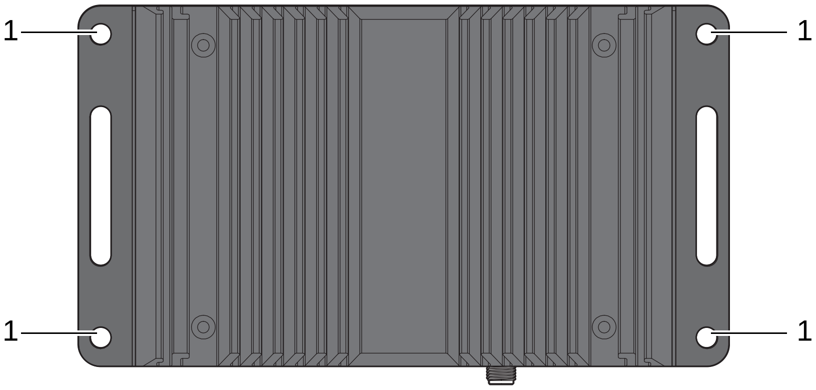


Figure 1.3 Top View

No.	Item	Description
1	Wall mounting holes	Screw holes (4) used in the installation on wall.

1.2.4 System LED Panel

LED Name	LED Color	Description
PWR	Green	
DAT	Green	
WAN	Green	

1.3 Dimensions

mm [inch]

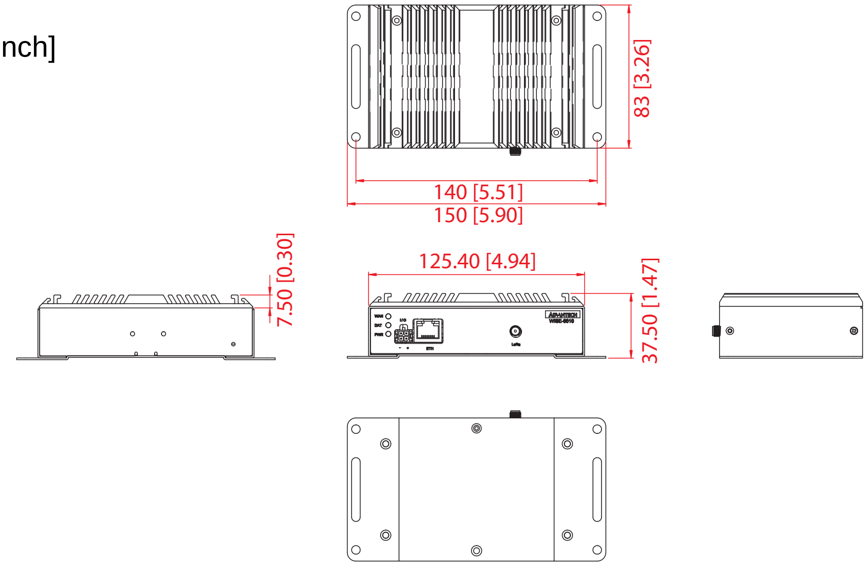


Figure 1.4 System LED Panel

Chapter 2

Gateway Installation

2.1 Warning

Warning: Before working on equipment that is connected to power lines, remove any jewelry (including rings, necklaces, and watches). Metal objects can heat up when connected to power and ground, which can cause serious burns or weld the metal object to the terminals.

Caution! *Exposure to chemicals can degrade the sealing properties of materials used in the sealed relay device.*

Caution! *It is not recommended to work on the system or connect or disconnect cables during periods of lightning activity.*

Caution! *Before performing any of the following procedures, disconnect the power source from the DC circuit.*

Caution! *Read the installation instructions before connecting the system to its power source.*

Caution! *The device must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor.*

Caution! *The installation, replacement, or service of the device must be Only be performed by trained and qualified personnel.*

Caution! *Ultimate disposal of this product should be handled according to local and national regulations*

Caution! *To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 70°C (158°F).*

Caution! *If the switch is to be installed in a hazardous location, ensure that the DC power source is located away from the vicinity of the switch.*

Caution! *The installation of the equipment must comply with all national and local electrical codes.*

Caution! *Explosion Hazard-The area must be known to be nonhazardous before servicing or replacing any components.*

Warning! *Airflow around the switch must be unrestricted. To prevent the switch from overheating, there must be the following minimum clearances:*

- Top and bottom: 2.0 in. (50.8 mm)
- Sides: 2.0 in. (50.8 mm)
- Front: 2.0 in. (50.8 mm)

2.2 Installation Guideline

The following guidelines are provided to optimize the device performance. Review the guidelines before installing the device.

- Make sure cabling is away from sources of electrical noise. Radios, power lines, and fluorescent lighting fixtures can interference with the device performance.
- Make sure the cabling is positioned away from equipment that can damage the cables.
- Operating environment is within the ranges listed range, see “Specifications” on page 2.
- Relative humidity around the switch does not exceed 95 percent (noncondensing).
- Altitude at the installation site is not higher than 10,000 feet.
- In 10/100 and 10/100/1000 fixed port devices, the cable length from the switch to connected devices can not exceed 100 meters (328 feet).
- Make sure airflow around the switch and respective vents is unrestricted. Without proper airflow the switch can overheat. To prevent performance degredation and damage to the switch, make sure there is clerance at the top and bottom and around the exhaust vents.

2.3 Installing the Gateway

2.3.1 Installing Antenna

1. Connect the antenna by screwing the antenna connectors in a clockwise direction.

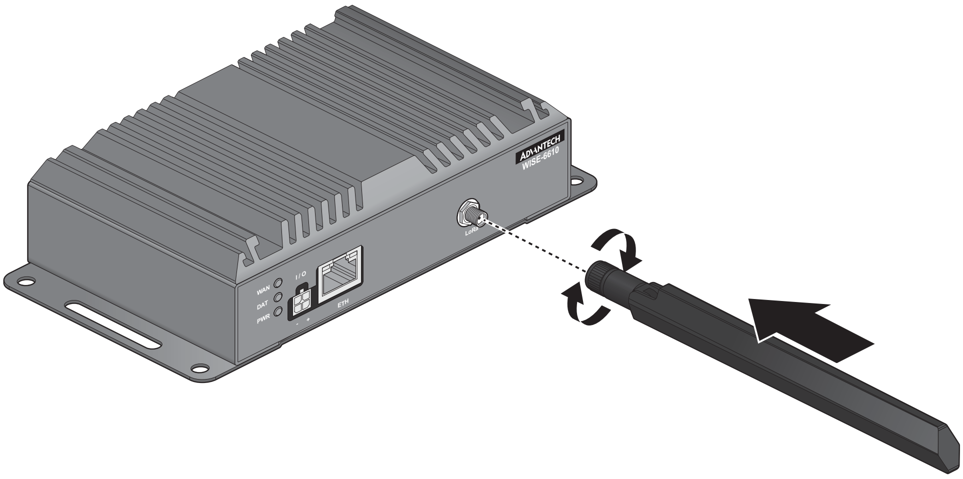


Figure 2.1 Installing the Antenna

2. Position the antenna for optimal signal strength.

Note! *The location and position of the antenna is crucial for effective wireless connectivity*

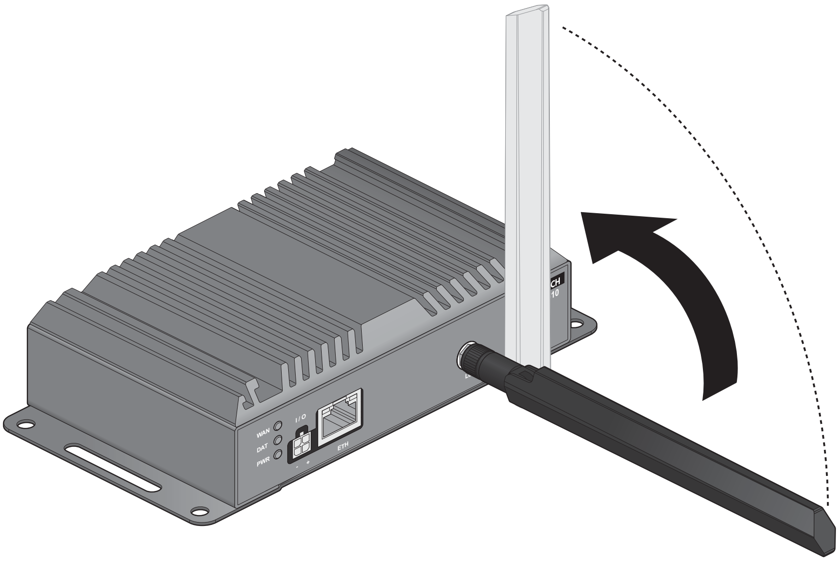


Figure 2.2 Positioning the Antenna

2.3.2 Wall Mounting

1. Locate the area to install and mark the four screw locations. It is suggested to place the device on the installation location and use the mounting locations to mark the location of the screw holes).
2. If necessary first drill pilot holes. Drill four holes over the four marked locations on the wall. On concrete, it is recommended to install wall sinks
3. Align the SmartSwarm over the installation location on the wall.
4. Secure the SmartSwarm with screws (Ø 5.0 mm).

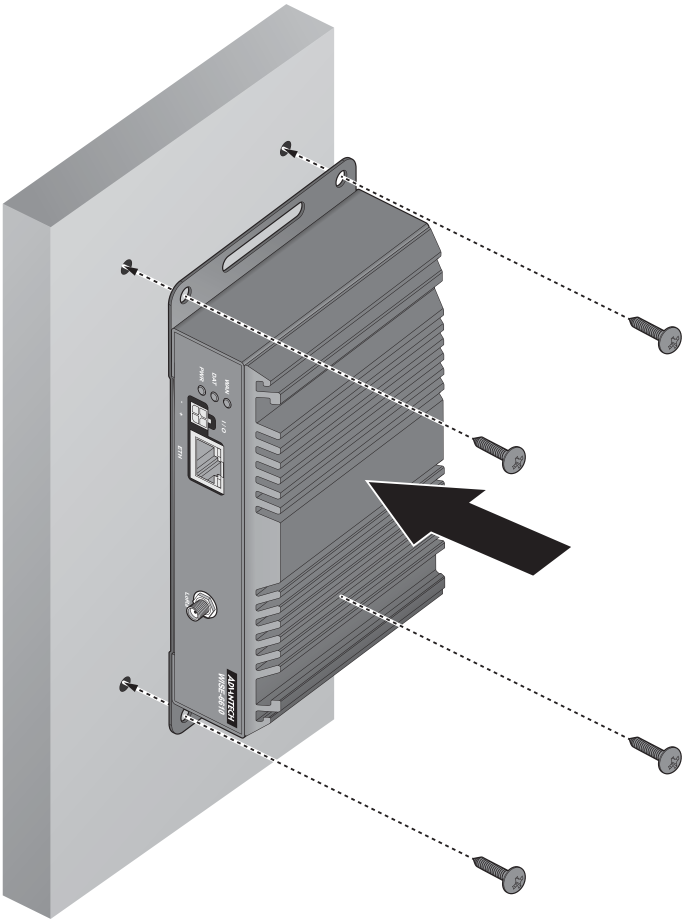


Figure 2.3 Wall Mount Installation

2.3.3 DIN Rain Mounting

2.3.3.1 Installing the DIN Rail Mounting Kit

1. Align the DIN rail clip with the rear of SmartSwarm.
2. Secure the DIN rail clip and the SmartSwarm with screws.

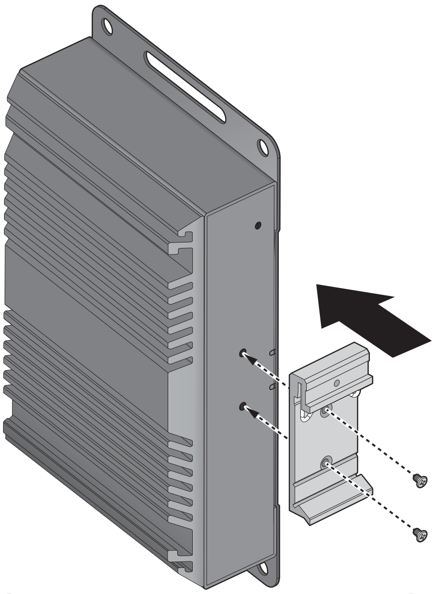


Figure 2.4 Wall Mount Installation

3. Position the rear panel of the SmartSwarm directly in front of the DIN rail, making sure that the top of the DIN rail clip hooks over the top of the DIN rail, as shown in the following illustration.

   Make sure the DIN rail is inserted behind the spring mechanism.
4. Once the DIN rail is seated correctly in the DIN rail clip, press the front of the SmartSwarm to rotate the SmartSwarm down and into the release tab on the DIN rail clip. If seated correctly, the bottom of the DIN rail should be fully inserted in the release tab.

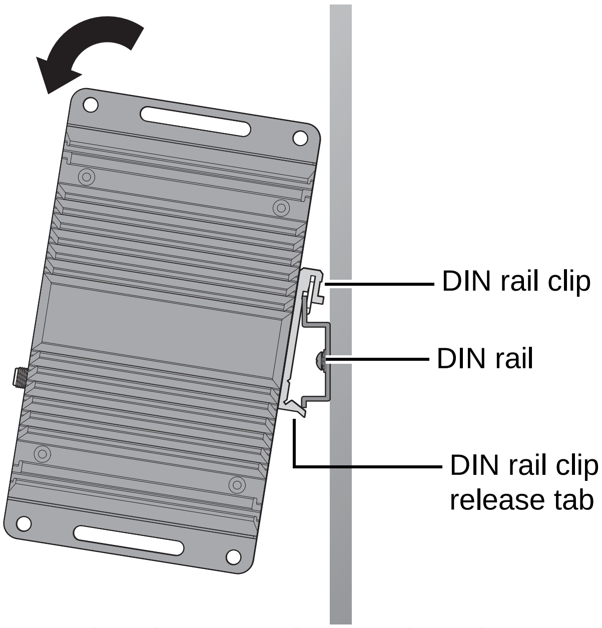


Figure 2.5 Installing the DIN-Rail Mounting Kit

See the following figure demonstrating the correct position of a completed DIN installation.

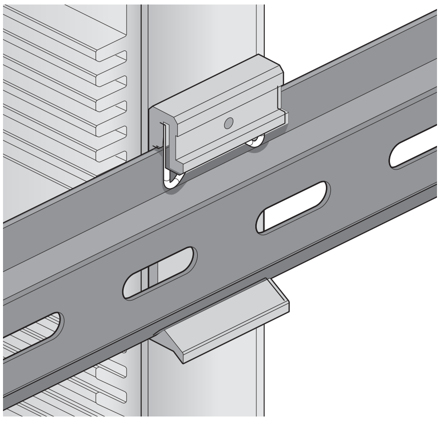


Figure 2.6 Correctly Installed DIN Rail Kit

2.3.3.2 Removing the DIN Rail Mounting Kit

1. Ensure that power is removed from the SmartSwarm, and disconnect all cables and connectors from the front panel of the SmartSwarm.
2. Push down on the top of the DIN rail clip release tab with your finger. As the clip releases, lift the bottom of the SmartSwarm, as shown in the following illustration.

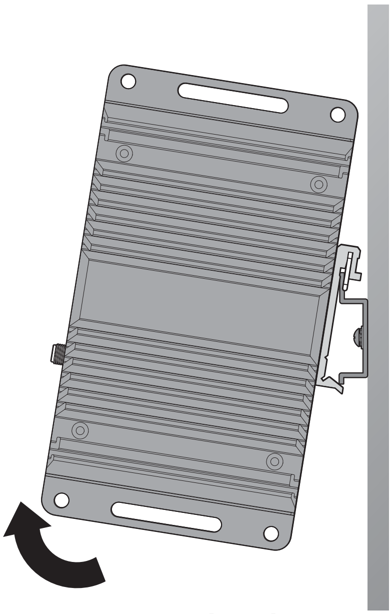


Figure 2.7 Removing the DIN-Rail

2.4 Connecting the Gateway to Ethernet Port

2.4.1 RJ45 Ethernet Cable Wiring

For RJ45 connectors, data-quality, twisted pair cabling (rated CAT5 or better) is recommended. The connector bodies on the RJ45 Ethernet ports are metallic and connected to the GND terminal. For best performance, use shielded cabling. Shielded cabling may be used to provide further protection.

Straight-thru Cable Wiring		**Cross-over Cable Wiring**	
Pin 1	Pin 1	Pin 1	Pin 3
Pin 2	Pin 2	Pin 2	Pin 6
Pin 3	Pin 3	Pin 3	Pin 1
Pin 6	Pin 6	Pin 6	Pin 2

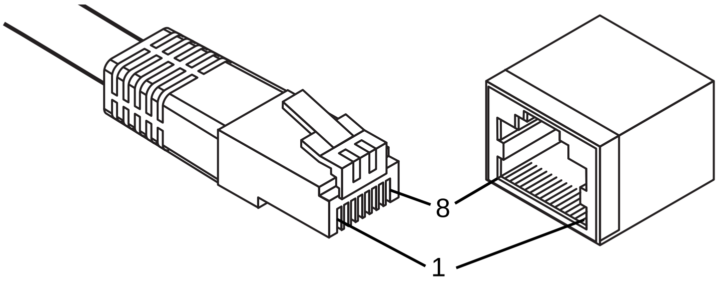


Figure 2.8 Ethernet Plug & Connector Pin Position

Maximum cable length: 100 meters (328 ft.) for 10/100BaseT.

2.5 Power Supply Installation

1. Insert the power cable into the power socket. The cable locks in place if installed correctly.
2. Connect the other end to a wall outlet.

   The LEDs light when the device is connected to the power source

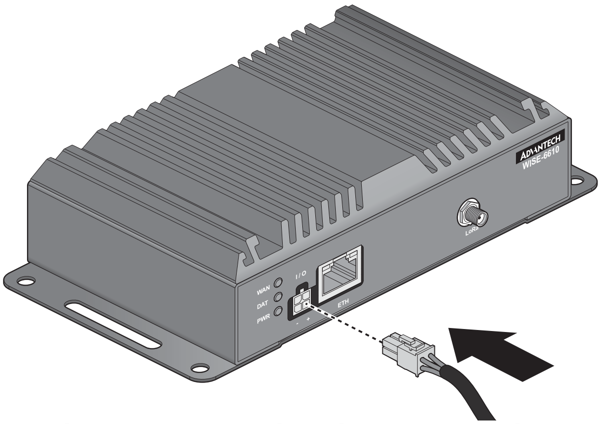


Figure 2.9 Installing the Power Cable

The following table show the color lines definition:

V+	**DI**	**GND**	**D0**
Red	Yellow	Black	Gray

Chapter 3

Managing Gateway

3.1 Access Interface

To access the login window, connect the device to the network, see “Connecting the Gateway to Ethernet Port” on page 12. When WISE-6610 Series is first installed, make sure the network environment is configured to enable access to the device. Your computer and the device must be on the same network subnet to allow them to establish a network connection.

Before you begin, make sure the device is powered on, see “Power Supply Installation” on page 13 for further information.

1. Launch a web browser on a computer.
2. In the browser's address bar type in the default IP address (192.168.1.1). The login screen displays.
3. Enter the default user name and password (root/root) to log into the management interface. You can change the default password after a successfully log in. See “Changing Default Password” on page 15.
4. Click **Login** to enter the management interface.

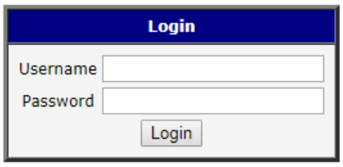


Figure 3.1 Login Screen

When you successfully enter login information on the login page, web interface will be displayed. The left side of the web interface contains a menu tree with sections for monitoring (Status), configuration (Configuration), customization (Customization) and administration (Administration) of the device.

Name and Location items in the right upper corner display the name and location of the device in the SNMP configuration (see “SNMP” on page 47). These fields are user-defined for each device.

After the green LED starts to blink you may restore the initial device settings by pressing the reset (RST) button on the back panel. If the reset button is pressed, all configuration will revert to factory defaults and the device will reboot (the green LED will be on during the reboot).

3.2 Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.

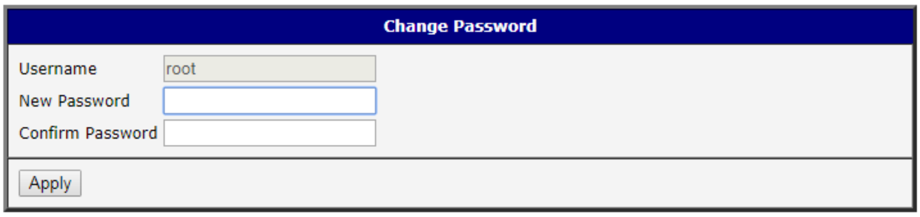
After you have performed the basic configurations on your switches, the following is a recommendation which is considered best practice policy.

3.2.1 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the WISE-6610 Series is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:

1. Navigate to **Administration** > **Change Password**.
2. In the **New Password** field, type in the new password. Re-type the same password in the **Confirm Password** field.
3. Click **Apply** to change the current account settings.



Change Password

Username	root
New Password	
Confirm Password	

Figure 3.2 Changing a Default Password

Note! *To change other user's password, go to* ***Administration*** *>* ***User****. From the* ***User Administration*** *menu, click* ***Change Password*** *behind the user's account*

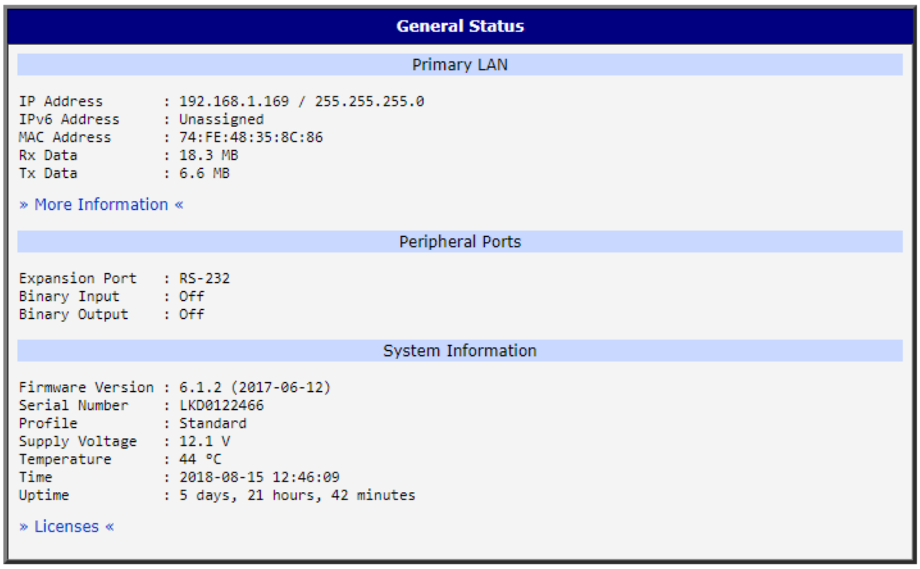
3.3 Status

3.3.1 General

Selecting the General item will open a screen displaying a summary of basic information about the device and its activities. This page is also displayed when you login to the web interface. Information is divided into several sections, based upon the type of device activity or the properties area: Mobile Connection, Primary LAN, Peripheral Ports and System Information. If the device is WiFi equipped, there will be a WiFi section.

IPv6 Address item can show multiple different addresses for one network interface. This is standard behavior since an IPv6 interface uses more addresses. The second IPv6 Address showed after pressing More Information is automatically generated EUI-64 format link local IPv6 address derived from MAC address of the interface. It is generated and assigned the first time the interface is used (e.g. cable is connected, Mobile WAN connecting, etc.).

To access this page, click **Status** > **General**.



General Status

Primary LAN

```
IP Address       : 192.168.1.169 / 255.255.255.0
IPv6 Address     : Unassigned
MAC Address      : 74:FE:48:35:8C:86
Rx Data          : 18.3 MB
Tx Data          : 6.6 MB
```

» More Information «

Peripheral Ports

```
Expansion Port   : RS-232
Binary Input     : Off
Binary Output    : Off
```

System Information

```
Firmware Version : 6.1.2 (2017-06-12)
Serial Number    : LKD0122466
Profile          : Standard
Supply Voltage   : 12.1 V
Temperature      : 44 °C
Time             : 2018-08-15 12:46:09
Uptime           : 5 days, 21 hours, 42 minutes
```

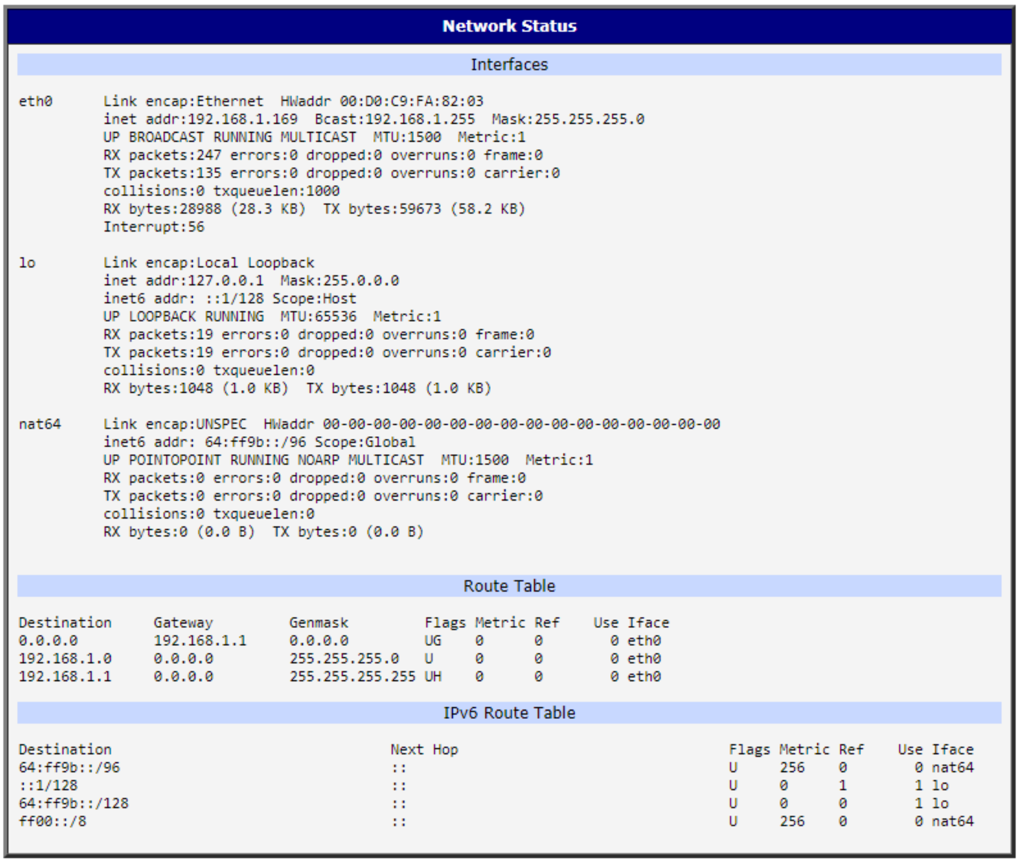
» Licenses «

Figure 3.3 Status > General

3.3.2 Network

To view information about the interfaces and the routing table, open the Network item in the Status menu.

To access this page, click **Status** > **Network**.



Network Status

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 00:D0:C9:FA:82:03
          inet addr:192.168.1.169  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:247 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28988 (28.3 KB)  TX bytes:59673 (58.2 KB)
          Interrupt:56

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1048 (1.0 KB)  TX bytes:1048 (1.0 KB)

nat64     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet6 addr: 64:ff9b::/96 Scope:Global
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.1.1     0.0.0.0         255.255.255.255 UH    0      0        0 eth0
```

IPv6 Route Table

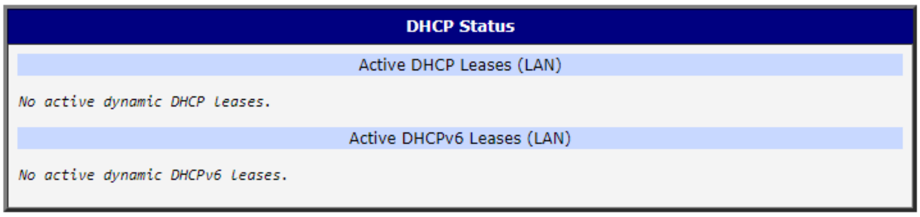
```
Destination                                 Next Hop                                Flags Metric Ref    Use Iface
64:ff9b::/96                                ::                                      U     256    0        0 nat64
::1/128                                     ::                                      U     0      1        1 lo
64:ff9b::/128                               ::                                      U     0      0        1 lo
ff00::/8                                    ::                                      U     256    0        0 nat64
```

Figure 3.4 Status > Network

3.3.3 DHCP

Information about the DHCP server activity is accessible via DHCP item. The DHCP server provides automatic configuration of the client devices connected to the device. The DHCP server assigns each device an IP address, subnet mask, default gateway (IP address of device) and DNS server (IP address of device). DHCPv6 server is supported.

To access this page, click **Status** > **DHCP**.



DHCP Status

Active DHCP Leases (LAN)

No active dynamic DHCP leases.

Active DHCPv6 Leases (LAN)

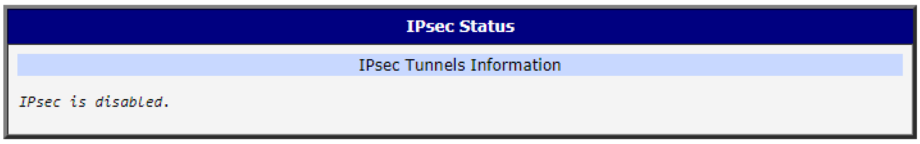
No active dynamic DHCPv6 leases.

Figure 3.5 Status > DHCP

3.3.4 IPsec

Selecting the IPsec option in the status menu of the web page will bring up the information for any IPsec Tunnels that have been established. If the tunnel has been built correctly, the screen will display IPsec SA established (highlighted in red in the figure below.) If there is no such text in log, the tunnel was not created.

To access this page, click **Status** > **IPsec**.



IPsec Status

IPsec Tunnels Information

IPsec is disabled.

Figure 3.6 Status > IPsec

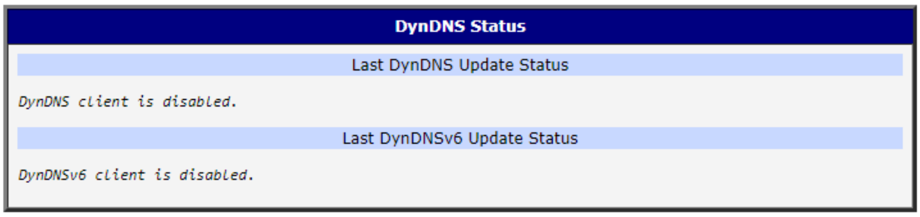
3.3.5 DynDNS

The device supports DynamicDNS using a DNS server on www.dyndns.org. If Dynamic DNS is configured, the status can be displayed by selecting menu option DynDNS. Refer to www.dyndns.org for more information on how to configure a Dynamic DNS client.

You can use the following listed servers for the Dynamic DNS service. It is possible to use the DynDNSv6 service with IP Mode switched to IPv6 on DynDNS Configuration page.

- www.dyndns.org
- www.spdns.de
- www.dnsdynamic.org
- www.noip.com

To access this page, click **Status** > **DynDNS**.



DynDNS Status

Last DynDNS Update Status

DynDNS client is disabled.

Last DynDNSv6 Update Status

DynDNSv6 client is disabled.

Figure 3.7 Status > DynDNS

When the device detects a DynDNS record update, the dialog displays one or more of the following messages:

- DynDNS client is disabled.
- Invalid username or password.
- Specified hostname doesn't exist.
- Invalid hostname format.
- Hostname exists, but not under specified username.
- No update performed yet.
- DynDNS record is already up to date.
- DynDNS record successfully update.
- DNS error encountered.
- DynDNS server failure.

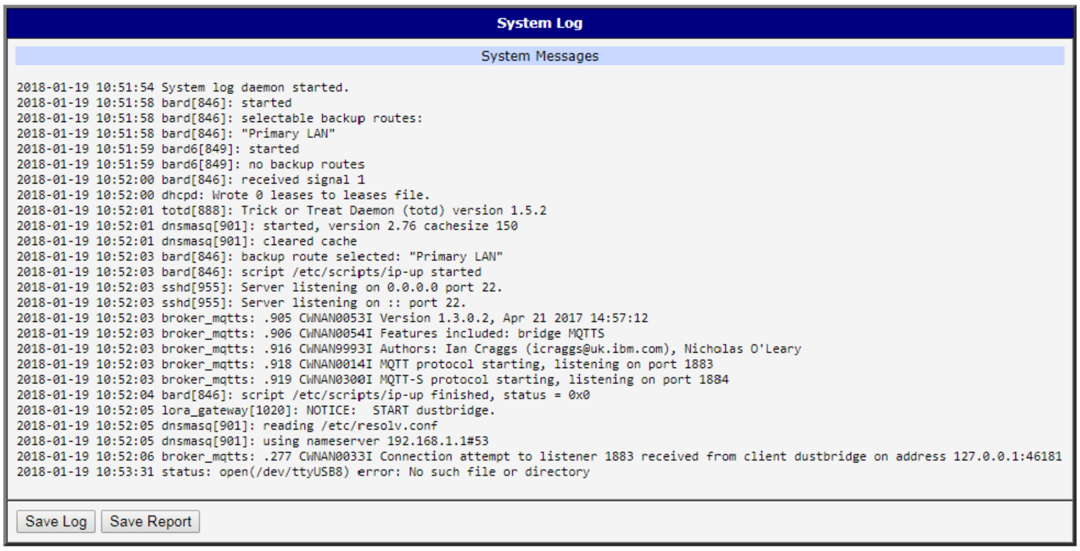
3.3.6 System Log

If there are any connection problems you may view the system log by selecting the System Log menu item. Detailed reports from individual applications running in the device will be displayed. Use the **Save Log** button to save the system log to a connected computer. (It will be saved as a text file with the .log extension.) The **Save Report** button is used for creating detailed reports. (It will be saved as a text file with the .txt extension. The file will include statistical data, routing and process tables, system log, and configuration.)

The default length of the system log is 1000 lines. After reaching 1000 lines a new file is created for storing the system log. After completion of 1000 lines in the second file, the first file is overwritten with a new file.

The Syslogd program will output the system log. It can be started with two options to modify its behavior. Option "-S" followed by decimal number sets the maximal number of lines in one log file. Option "-R" followed by hostname or IP address enables logging to a remote syslog daemon. (If the remote syslog daemon is Linux OS, there has to be remote logging enabled (typically running "syslogd -R"). If it's the Windows OS, there has to be syslog server installed, e.g. Syslog Watcher). To start syslogd with these options, the "/etc/init.d/syslog" script can be modified via SSH or lines can be added into Startup Script (accessible in Configuration section) according to Figure 3.9.

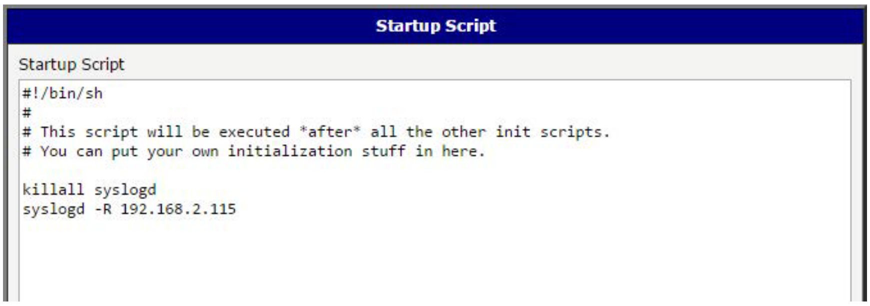
To access this page, click **Status** > **System Log**.



```
2018-01-19 10:51:54 System log daemon started.
2018-01-19 10:51:58 bard[846]: started
2018-01-19 10:51:58 bard[846]: selectable backup routes:
2018-01-19 10:51:58 bard[846]: "Primary LAN"
2018-01-19 10:51:59 bard6[849]: started
2018-01-19 10:51:59 bard6[849]: no backup routes
2018-01-19 10:52:00 bard[846]: received signal 1
2018-01-19 10:52:00 dhcpd: Wrote 0 leases to leases file.
2018-01-19 10:52:01 totd[888]: Trick or Treat Daemon (totd) version 1.5.2
2018-01-19 10:52:01 dnsmasq[901]: started, version 2.76 cachesize 150
2018-01-19 10:52:01 dnsmasq[901]: cleared cache
2018-01-19 10:52:03 bard[846]: backup route selected: "Primary LAN"
2018-01-19 10:52:03 bard[846]: script /etc/scripts/ip-up started
2018-01-19 10:52:03 sshd[955]: Server listening on 0.0.0.0 port 22.
2018-01-19 10:52:03 sshd[955]: Server listening on :: port 22.
2018-01-19 10:52:03 broker_mqtts: .905 CWNAN0053I Version 1.3.0.2, Apr 21 2017 14:57:12
2018-01-19 10:52:03 broker_mqtts: .906 CWNAN0054I Features included: bridge MQTTS
2018-01-19 10:52:03 broker_mqtts: .916 CWNAN9993I Authors: Ian Craggs (icraggs@uk.ibm.com), Nicholas O'Leary
2018-01-19 10:52:03 broker_mqtts: .918 CWNAN0014I MQTT protocol starting, listening on port 1883
2018-01-19 10:52:03 broker_mqtts: .919 CWNAN0300I MQTT-S protocol starting, listening on port 1884
2018-01-19 10:52:04 bard[846]: script /etc/scripts/ip-up finished, status = 0x0
2018-01-19 10:52:05 lora_gateway[1020]: NOTICE:  START dustbridge.
2018-01-19 10:52:05 dnsmasq[901]: reading /etc/resolv.conf
2018-01-19 10:52:05 dnsmasq[901]: using nameserver 192.168.1.1#53
2018-01-19 10:52:06 broker_mqtts: .277 CWNAN0033I Connection attempt to listener 1883 received from client dustbridge on address 127.0.0.1:46181
2018-01-19 10:53:31 status: open(/dev/ttyUSB8) error: No such file or directory
```

Figure 3.8 Status > System Log

The following example (figure) shows how to send syslog information to a remote server at 192.168.2.115 on startup.



```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.

killall syslogd
syslogd -R 192.168.2.115
```

Figure 3.9 Example Program Syslogd Start with the Parameter -R

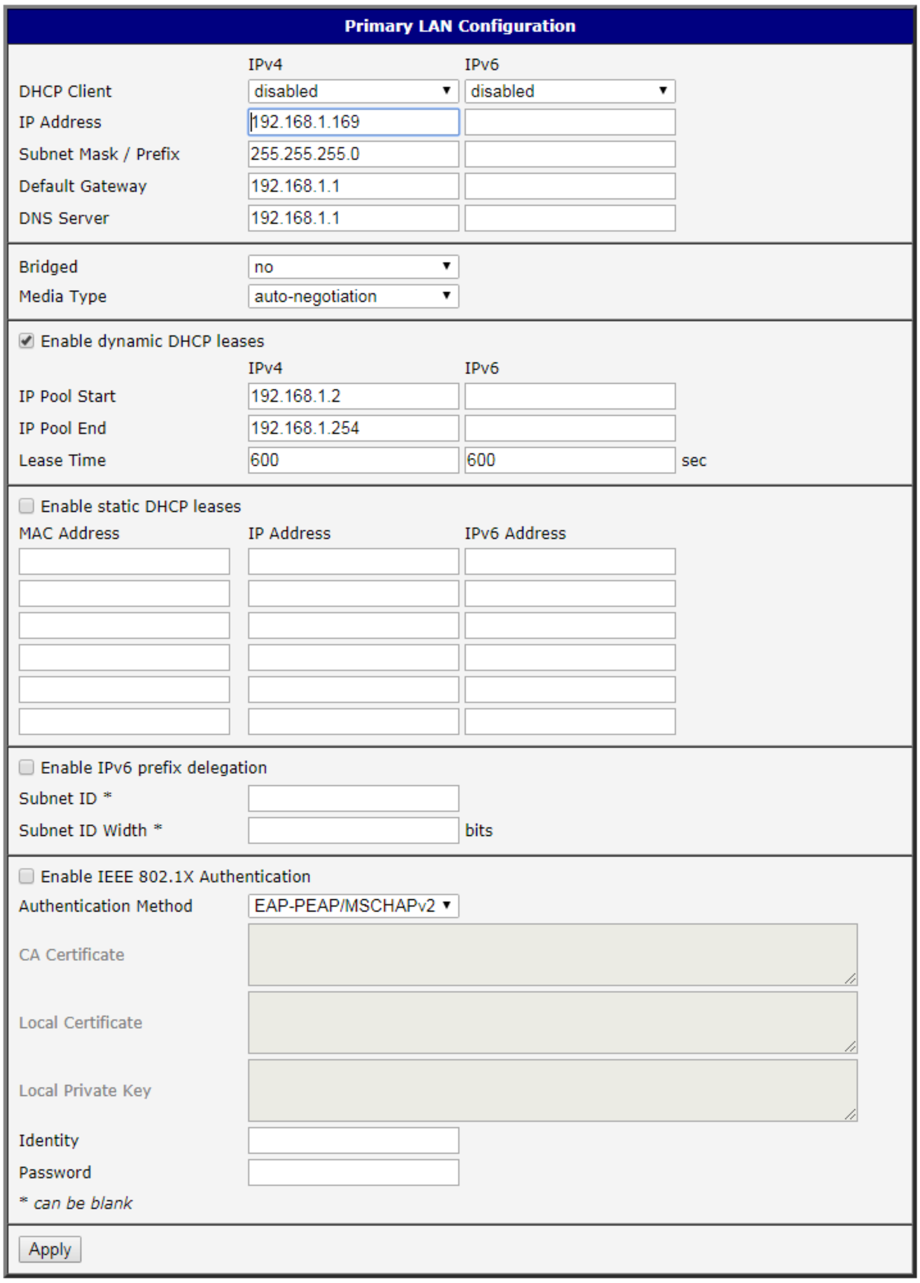
3.4 Configuration

3.4.1 LAN

To enter the Local Area Network configuration, select the LAN menu item in the Configuration section.

LAN Configuration page is divided into IPv4 and IPv6 columns, see Figure 3.10. There is dual stack support of IPv4 and IPv6 protocols - they can run alongside, you can configure either one of them or both. If you configure both IPv4 and IPv6, other network devices will choose the communication protocol. Configuration items and IPv6 to IPv4 differences are described in the tables below.

To access this page, click **Configuration** > **LAN**.



Primary LAN Configuration

	IPv4	IPv6	
DHCP Client	disabled ▾	disabled ▾	
IP Address	192.168.1.169		
Subnet Mask / Prefix	255.255.255.0		
Default Gateway	192.168.1.1		
DNS Server	192.168.1.1		

Bridged: no ▾

Media Type: auto-negotiation ▾

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.254		
Lease Time	600	600	sec

☐ Enable static DHCP leases

MAC Address	IP Address	IPv6 Address

☐ Enable IPv6 prefix delegation

Subnet ID *

Subnet ID Width * bits

☐ Enable IEEE 802.1X Authentication

Authentication Method: EAP-PEAP/MSCHAPv2 ▾

CA Certificate

Local Certificate

Local Private Key

Identity

Password

** can be blank*

Apply

Figure 3.10 Configuration > LAN

Item	**Description**
DHCP Client	Enables/disables the DHCP client function supporting both IPv4 and IPv6. ■ disabled - The device does not allow automatic allocation of an IP address from a DHCP server in LAN network. ■ enabled - The device allows automatic allocation of an IP address from a DHCP server in LAN network.
IP Address	A fixed IP address of the Ethernet interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address - number in range 0 to 128.

Item	Description
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent to this IP address. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the device forwards the request to DNS server specified here. Use proper IP address notation in IPv4 and IPv6 column.

The Default Gateway and DNS Server items are only used if the DHCP Client item is set to disabled and if the Primary or Secondary LAN is selected by the Backup Routes system as the default route. Since FW 5.3.0, Default Gateway and DNS Server are also supported on bridged interfaces.

The following items (in the table below) are global for the configured Ethernet interface. Only one bridge can be active on the device at a time. The DHCP Client, IP Address and Subnet Mask / Prefix parameters of the only one of the interfaces are used to for the bridge. Primary LAN has higher priority when other interfaces (wlan0) are added to the bridge. Other interfaces (wlan0 - wifi) can be added to or deleted from an existing bridge at any time. The bridge can be created on demand for such interfaces, but not if it is configured by their respective parameters.

Item	Description
Bridged	Activates/deactivates the bridging function on the device. ■ no - The bridging function is inactive (default). ■ yes - The bridging function is active.
Media Type	Specifies the type of duplex and speed used in the network. ■ Auto-negation - The device automatically sets the best speed and duplex mode of communication according to the network's possibilities. ■ 100 Mbps Full Duplex - The device communicates at 100 Mbps, in the full duplex mode. ■ 100 Mbps Half Duplex - The device communicates at 100 Mbps, in the half duplex mode. ■ 10 Mbps Full Duplex - The device communicates at 10 Mbps, in the full duplex mode. ■ 10 Mbps Half Duplex - The device communicates at 10 Mbps, in the half duplex mode.

3.4.1.1 DHCP Server

The DHCP server assigns the IP address, gateway IP address (IP address of the device) and IP address of the DNS server (IP address of the device) to the connected clients. If these values are filled in by the user in the configuration form, they will be preferred.

The DHCP server supports static and dynamic assignment of IP addresses. Dynamic DHCP assigns clients IP addresses from a defined address space. Static DHCP assigns IP addresses that correspond to the MAC addresses of connected clients.

If IPv6 column is filled in, the DHCPv6 server is used - it is dual stack IPv4 and IPv6.

Note! *Do not to overlap ranges of static allocated IP addresses with addresses allocated by the dynamic DHCP server. IP address conflicts and incorrect network function can occur if you overlap the ranges.*

Configuration of Dynamic DHCP Server

Item	Description
Enable dynamic DHCP leases	Select this option to enable a dynamic DHCP server.
IP Pool Start	Starting IP addresses allocated to the DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of IP addresses allocated to the DHCP clients. Use proper IP address notation in IPv4 and IPv6 column.
Lease time	Time in seconds that the IP address is reserved before it can be re-used.

Configuration of Static DHCP Server

Item	Description
Enable static DHCP leases	Select this option to enable a static DHCP server.
MAC Address	MAC address of a DHCP client.
IPv4 Address	Assigned IPv4 address. Use proper notation.
IPv6 Address	Assigned IPv6 address. Use proper notation.

3.4.1.2 IPv6 Prefix Delegation

Note! *This is an advanced configuration option. IPv6 prefix delegation works automatically with DHCPv6 - use only if different configuration is desired and if you know the consequences.*

If you want to override the automatic IPv6 prefix delegation, you can configure it in this form. You have to know your Subnet ID Width (part of IPv6 address), see Figure 3.11 below for the calculation help - it is an example: 48 bits is Site Prefix, 16 bits is Subnet ID (Subnet ID Width) and 64 bits is Interface ID.

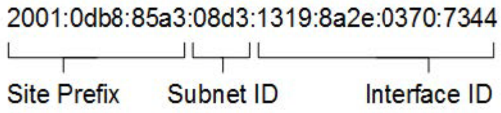


Figure 3.11 IPv6 Address with Prefix Example

Item	Description
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Enable IPv6 prefix delegation	The decimal value of the Subnet ID of the Ethernet interface. Maximum value depends on the Subnet ID Width.
Subnet ID Width	The maximum Subnet ID Width depends on your Site Prefix - it is the remainder to 64 bits.

3.4.1.3 IEEE 802.1X Authentication

To prevent unauthorized radios from accessing data transmitting over wireless transmission, WISE-6610 Series provides rock solid security settings.

Navigate to **Configuration** > **LAN and locate Enable IEEE 802.1X Authentication**.

Item	Description
Enable IEEE 802.1X Authentication	Tick the radio button to enable the authentication function.
Authentication Method	Click the drop-down menu to select the method type. Range: EAP-PEAP/MSCHAPv2 or EAP-TLS.
CA Certificate	Enter the trusted digital certificate (required for EAP-PEAP).
Local Certificate	Enter the self-signed digital certificate (required for EAP-PEAP).
Local Private Key	Enter the secret key variable used to encrypt or decrypt the transmission.
Identity	Enter the Identity profile authorized to access the authentication server.
Password	Enter the string associated with the defined Identity profile in the previous frame.
Apply	Click **Apply** to accept the configuration changes.

The following are LAN configuration illustrations defining possible network topology.

Example 1: IPv4 Dynamic DHCP Server, Default Gateway and DNS Server

- The range of dynamic allocated IPv4 addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 second (10 minutes).
- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20

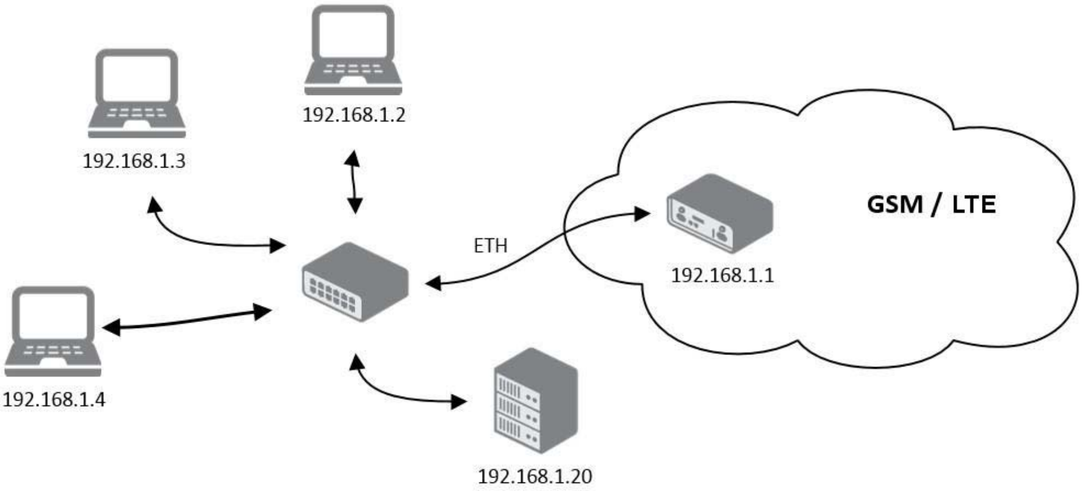
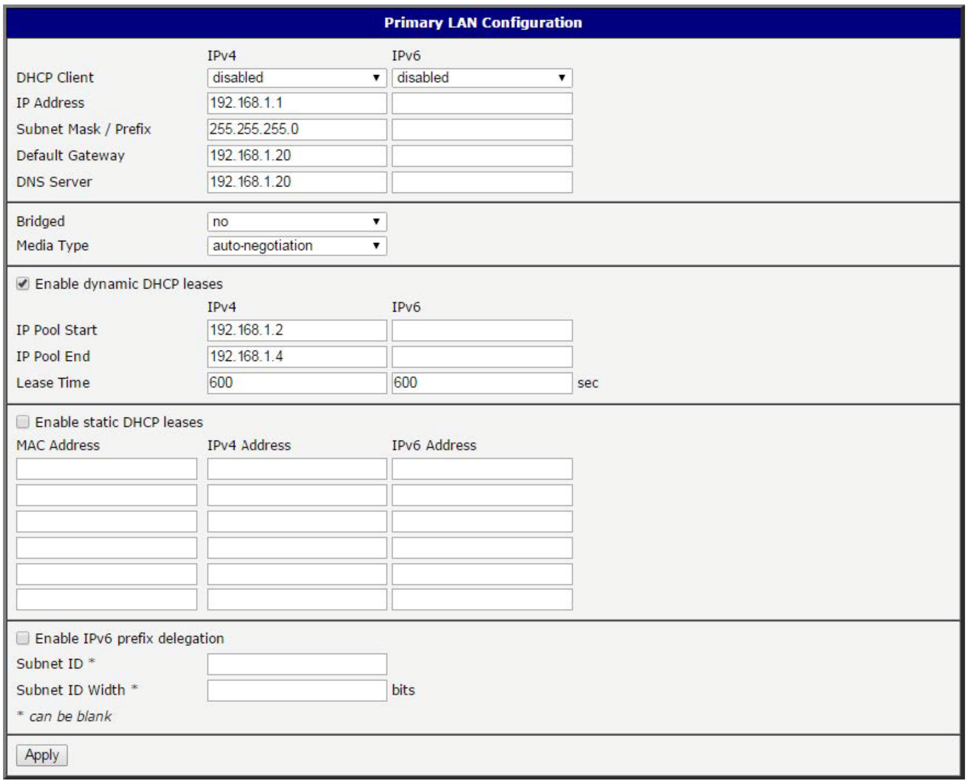


Figure 3.12 IPv4 Dynamic DHCP Network Topology

The settings required in the LAN configuration menu for an IPv4 Dynamic DHCP configuration are shown in the following figure.



Primary LAN Configuration

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway	192.168.1.20	
DNS Server	192.168.1.20	

Bridged	no
Media Type	auto-negotiation

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600	600	sec

☐ Enable static DHCP leases

MAC Address	IPv4 Address	IPv6 Address

☐ Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *		bits

* can be blank

Apply

Figure 3.13 LAN Configuration for a Dynamic Network Typology

Example 2: IPv4 Dynamic and Static DHCP server

- The range of allocated addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 seconds (10 minutes).
- The client with the MAC address 01:23:45:67:89:ab has the IP address 192.168.1.10.
- The client with the MAC address 01:54:68:18:ba:7e has the IP address 192.168.1.11.

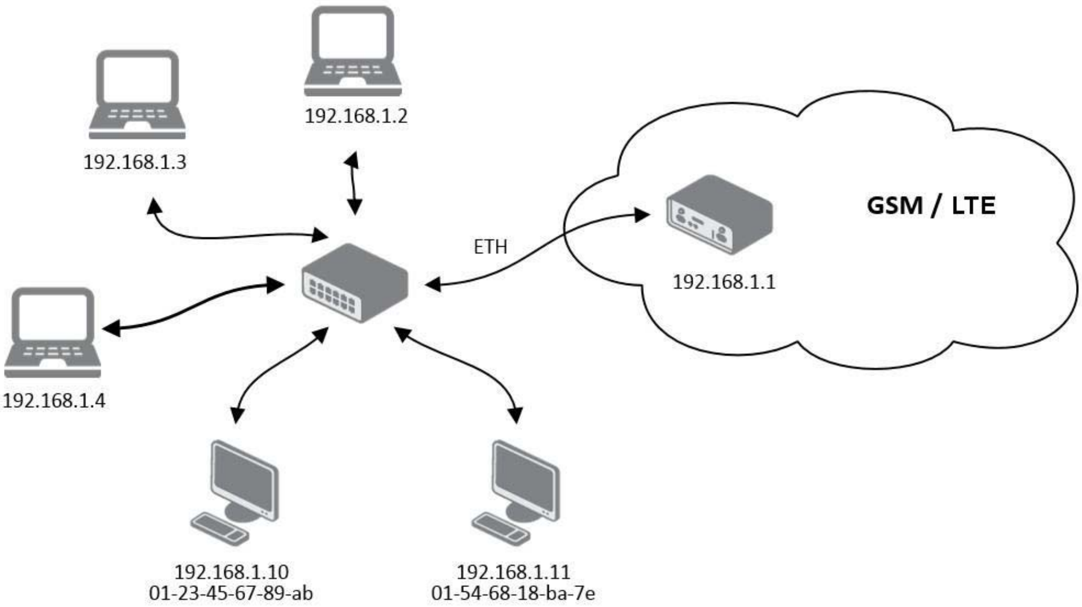
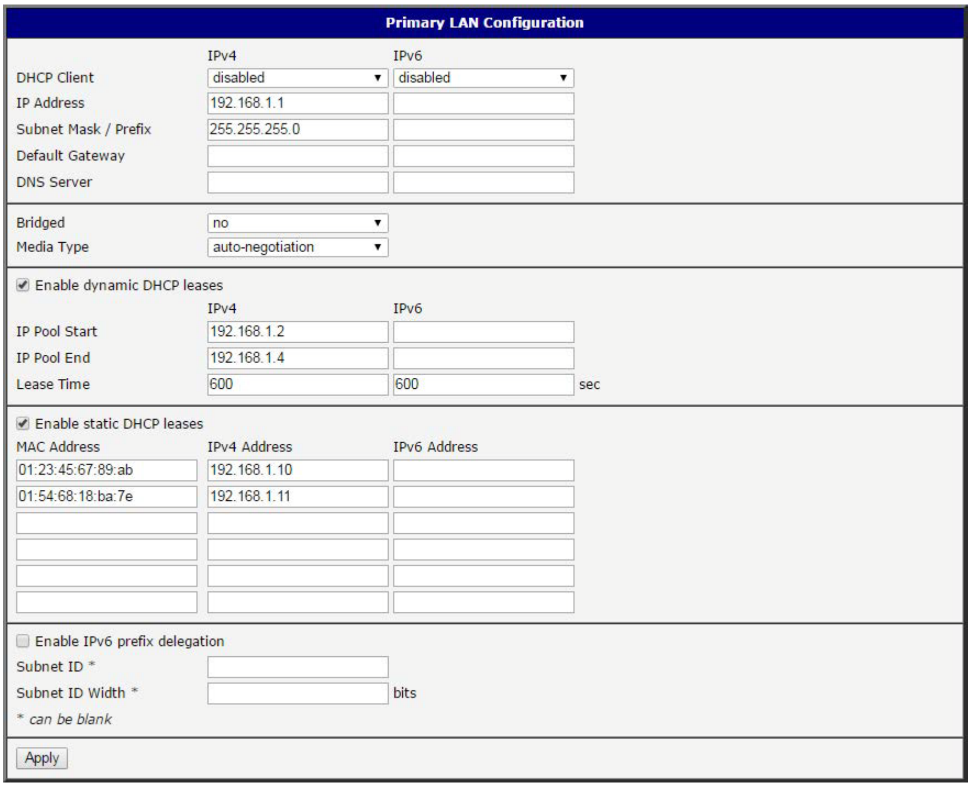


Figure 3.14 IPv4 Dynamic and Static DHCP Network Topology

The settings required in the LAN configuration menu for an IPv4 Dynamic and Static DHCP configuration are shown in the following figure.



Primary LAN Configuration

	IPv4	IPv6
DHCP Client	disabled ▾	disabled ▾
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway		
DNS Server		

Bridged	no ▾
Media Type	auto-negotiation ▾

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600	600	sec

☑ Enable static DHCP leases

MAC Address	IPv4 Address	IPv6 Address
01:23:45:67:89:ab	192.168.1.10	
01:54:68:18:ba:7e	192.168.1.11	

□ Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *		bits

* *can be blank*

Apply

Figure 3.15 LAN Configuration for an IPv4 Dynamic and Static DHCP Network Topology

Example 3: IPv6 Dynamic DHCP Server

- The range of dynamic allocated IPv6 addresses is from 2001:db8::1 to 2001:db8::ffff.
- The address is allocated for 600 second (10 minutes).
- The device is still accessible via IPv4 (192.168.1.1).

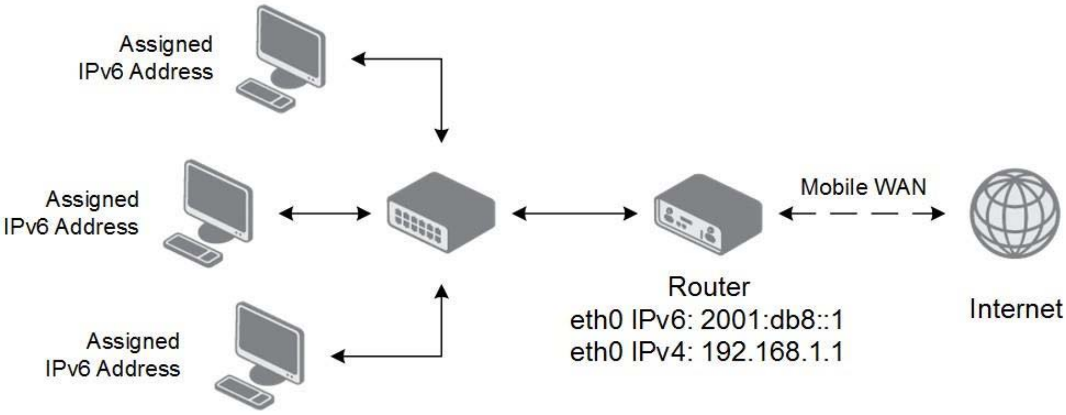
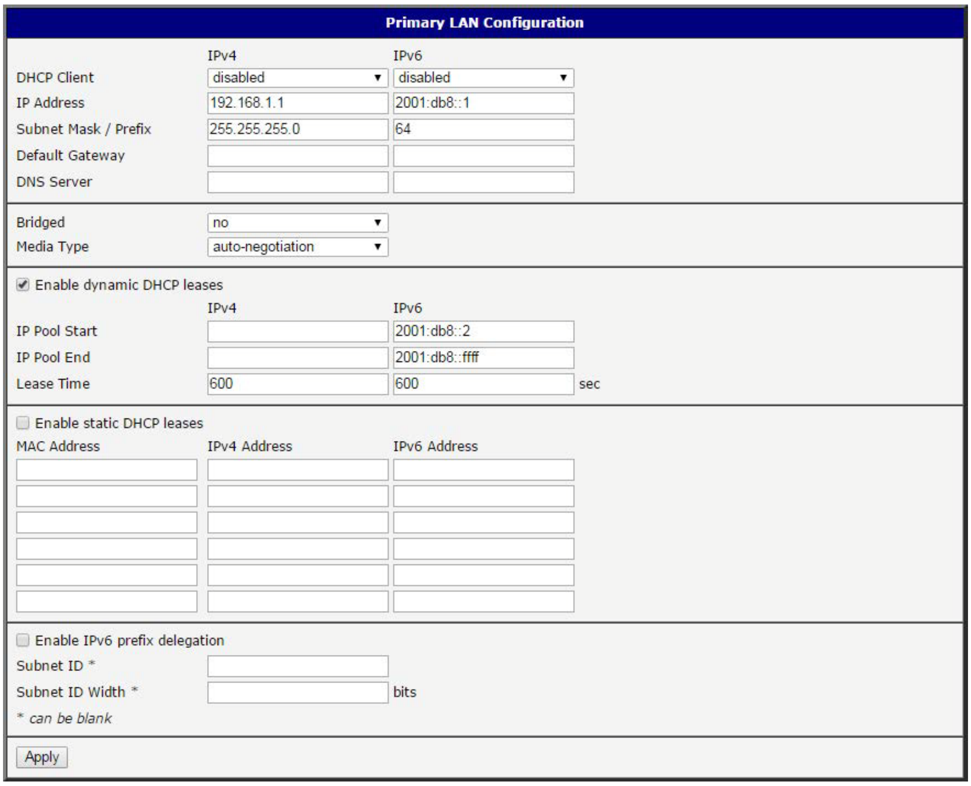


Figure 3.16 IPv6 Dynamic DHCP Server Network Topology



Primary LAN Configuration

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	192.168.1.1	2001:db8::1
Subnet Mask / Prefix	255.255.255.0	64
Default Gateway		
DNS Server		

Bridged	no
Media Type	auto-negotiation

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start		2001:db8::2	
IP Pool End		2001:db8::ffff	
Lease Time	600	600	sec

□ Enable static DHCP leases

MAC Address	IPv4 Address	IPv6 Address

□ Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *		bits

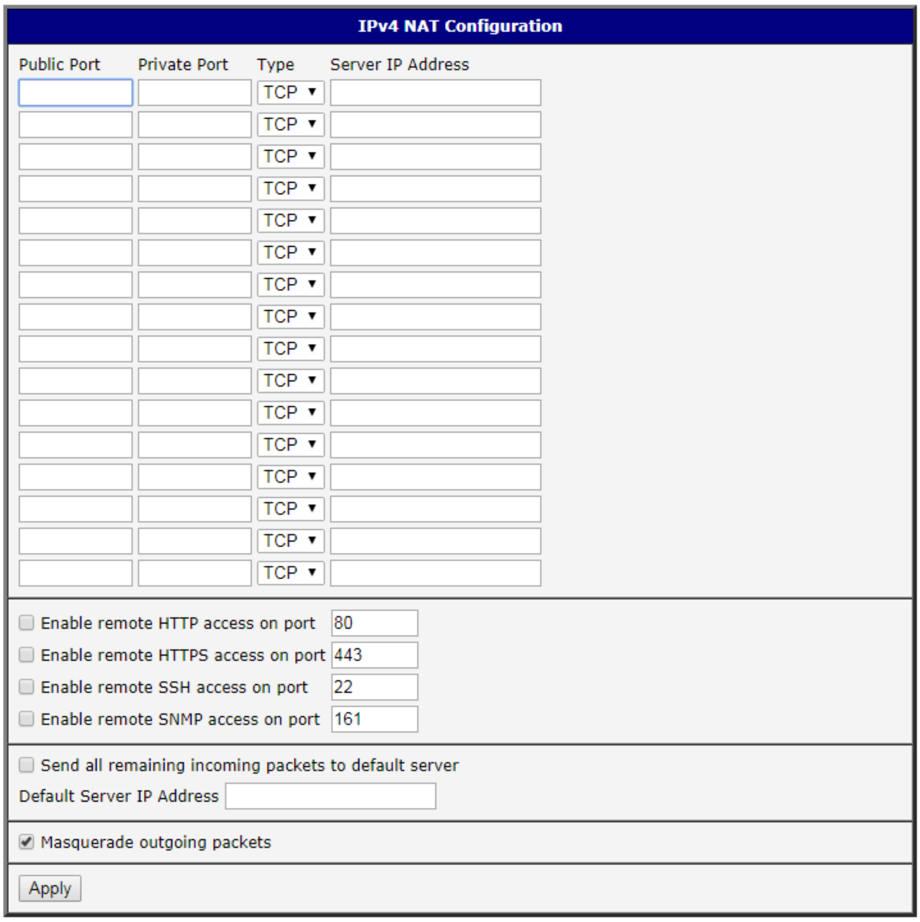
** can be blank*

Figure 3.17 LAN Configuration for an IPv6 Dynamic DHCP Server Network Topology

3.4.2 NAT

To configure the address translation function, click on NAT in the Configuration section of the main menu. There is independent IPv4 and IPv6 NAT configuration since there is dual stack IPv4 and IPv6 implemented in the router. The NAT item in the menu on the left will expand to IPv4 and IPv6 options and you can click IPv6 to enable and configure the IPv6 NAT - see Figure below. The configuration fields have the same meaning in the IPv4 NAT Configuration and IPv6 NAT Configuration forms.

To access this page, click **Configuration** > **NAT**.



IPv4 NAT Configuration

Public Port	Private Port	Type	Server IP Address
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	

□ Enable remote HTTP access on port 80

□ Enable remote HTTPS access on port 443

□ Enable remote SSH access on port 22

□ Enable remote SNMP access on port 161

□ Send all remaining incoming packets to default server

Default Server IP Address

☑ Masquerade outgoing packets

Apply

Figure 3.18 Configuration > NAT

The router actually uses Port Address Translation (PAT), which is a method of mapping a TCP/UDP port to another TCP/UDP port. The router modifies the information in the packet header as the packets traverse a router. This configuration form allows you to specify up to 16 PAT rules.

Item	Description
Public Port	Public port for the translation rule.
Private Port	Private port for the translation rule.
Type	Protocol type - TCP or UDP.
Server IP Address	IP address where the router forwards incoming data.

If you require more than sixteen NAT rules, insert the remaining rules into the Startup Script. The Startup Script dialog is located on Scripts page in the Configuration section of the menu. When creating your rules in the Startup Script, use this command for IPv4 NAT:

```
iptables -t nat -A napt -p tcp -dport [PORT_PUBLIC] -j DNAT
-to-destination [IPADDR]:[PORT_PRIVATE]
```

Enter the IP address [IPADDR], the public ports numbers [PORT_PUBLIC], and private [PORT_PRIVATE] in place of square brackets. For IPv6 NAT use ip6tables command with same options.

If you enable the following options and enter the port number, the router allows you to remotely access to the router from WAN (Mobile WAN) interface.

Caution! *Enable remote HTTP access on port activates the redirect from HTTP to HTTPS protocol only. The router doesn't allow unsecured HTTP protocol to access the web configuration. To access the web configuration, always check the Enable re- mote HTTPS access on port item. Never enable the HTTP item only to access the web configuration from the Internet (configuration would not be accessible from the Internet). Always check the HTTPS item or HTTPS and HTTP items together (to set the redirect from HTTP).*

Item	**Description**
Enable remote HTTP access on port	This option sets the redirect from HTTP to HTTPS only (disabled in default configuration).
Enable remote HTTPS access on port	If field and port number are filled in, configuration of the router over web interface is allowed (disabled in default configuration).
Enable remote SSH access on port	Select this option to allow access to the router using SSH (disabled in default configuration).
Enable remote SNMP access on port	Select this option to allow access to the router using SNMP (disabled in default configuration).
Masquerade outgoing packets	Activates/deactivates the network address translation function.

Use the following parameters to set the routing of incoming data from the WAN (Mobile WAN) to a connected computer.

Item	**Description**
Send all remaining incoming packets to default server	Activates/deactivates forwarding unmatched incoming packets to the default server. The prerequisite for the function is that you specify a default server in the De- fault Server IPv4/IPv6 Address field. The router can for- ward incoming data from a GPRS to a computer with the assigned IP address.
Default Server IP Address	The IP address.

Example1: IPv4 NAT Configuration with Single Device Connected

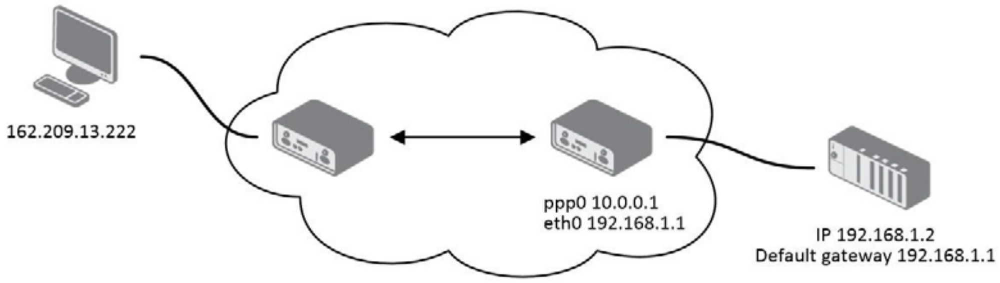
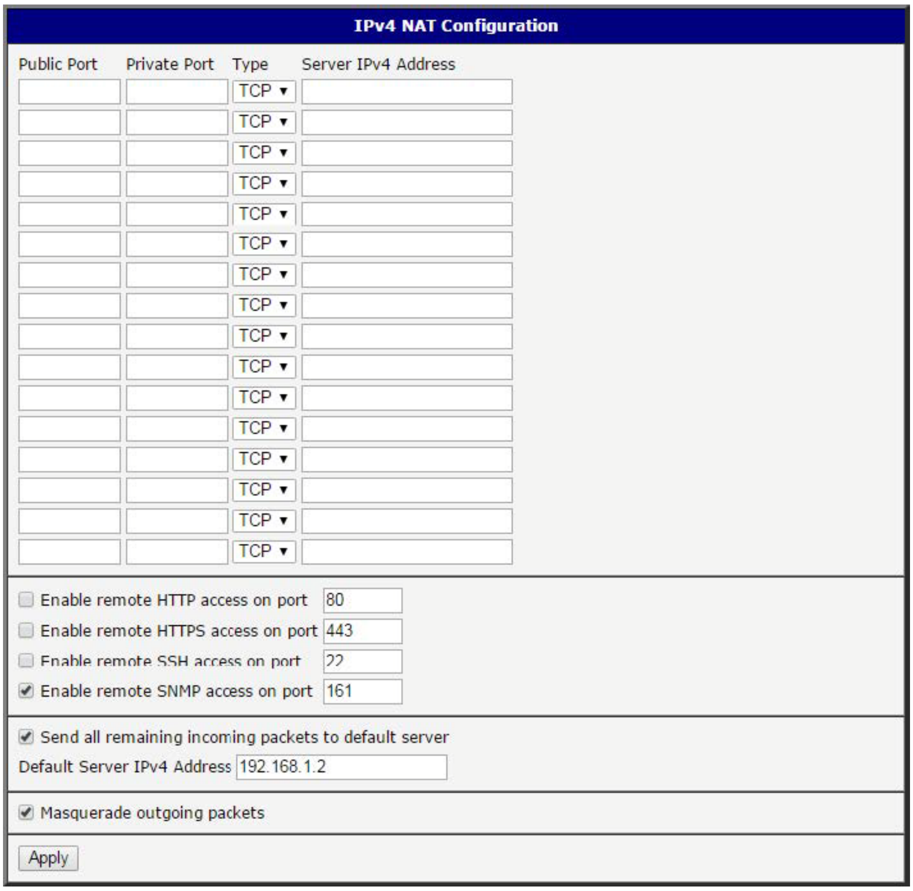


Figure 3.19 Topology for NAT Configuration Example 1

It is important to mark the Send all remaining incoming packets to default server check box for this configuration. The IP address in this example is the address of the device behind the router. The default gateway of the devices in the subnetwork connected to router is the same IP address as displayed in the Default Server IPv4 Address field.



IPv4 NAT Configuration

Public Port	Private Port	Type	Server IPv4 Address
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	
		TCP ▾	

□ Enable remote HTTP access on port 80

□ Enable remote HTTPS access on port 443

□ Enable remote SSH access on port 22

☑ Enable remote SNMP access on port 161

☑ Send all remaining incoming packets to default server

Default Server IPv4 Address 192.168.1.2

☑ Masquerade outgoing packets

Figure 3.20 NAT Configuration for Example 1

Example 2: IPv4 NAT Configuration with More Equipment Connected

In this example, using the switch you can connect more devices behind the router. Every device connected behind the router has its own IP address. Enter the address in the Server IPv4 Address field in the NAT dialog. The devices are communicating on port 80, but you can set port forwarding using the Public Port and Private Port fields in the NAT dialog. You have now configured the router to access the 192.168.1.2:80 socket behind the router when accessing the IP address 10.0.0.1:81 from the Internet. If you send a ping request to the public IP address of the router (10.0.0.1), the router responds as usual (not forwarding). And since the Send all remaining incoming packets to default server is inactive, the router denies connection attempts.

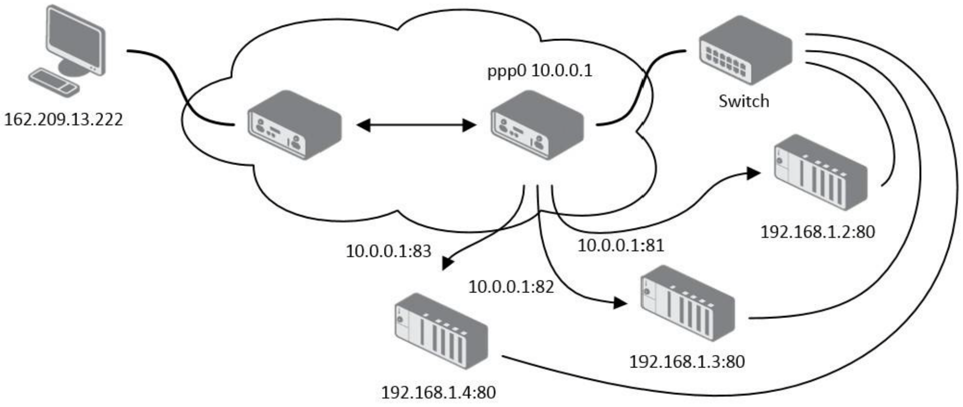
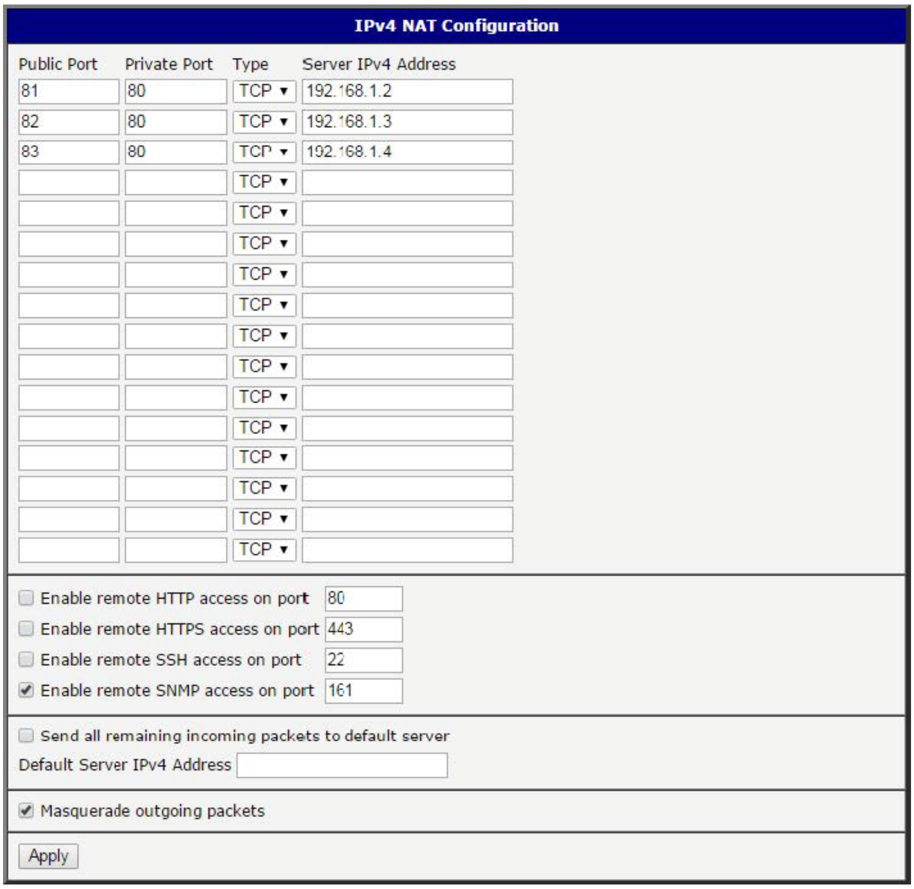


Figure 3.21 Topology for NAT Configuration Example 2



IPv4 NAT Configuration

Public Port	Private Port	Type	Server IPv4 Address
81	80	TCP	192.168.1.2
82	80	TCP	192.168.1.3
83	80	TCP	192.168.1.4
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☐ Enable remote HTTP access on port 80
☐ Enable remote HTTPS access on port 443
☐ Enable remote SSH access on port 22
☑ Enable remote SNMP access on port 161

☐ Send all remaining incoming packets to default server
Default Server IPv4 Address

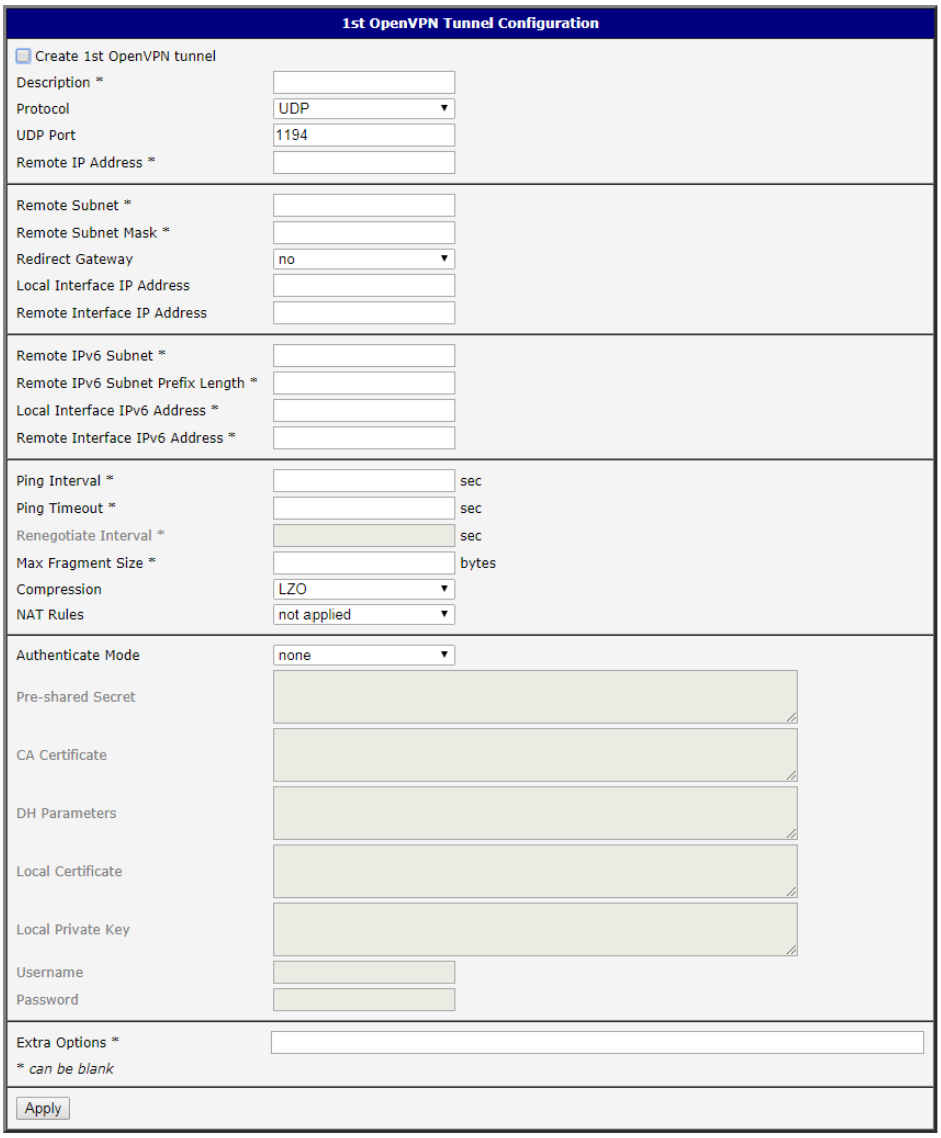
☑ Masquerade outgoing packets

Figure 3.22 NAT Configuration for Example 2

3.4.3 OpenVPN

Select the OpenVPN item to configure an OpenVPN tunnel. The OpenVPN tunnel function allows you to create a secure connection between two separate LAN networks. The device allows you to create up to four OpenVPN tunnels. IPv4 and IPv6 dual stack is supported.

To access this page, click **Configuration** > **OpenVPN**.



1st OpenVPN Tunnel Configuration

☐ Create 1st OpenVPN tunnel

Description *		
Protocol	UDP ▾	
UDP Port	1194	
Remote IP Address *		
Remote Subnet *		
Remote Subnet Mask *		
Redirect Gateway	no ▾	
Local Interface IP Address		
Remote Interface IP Address		
Remote IPv6 Subnet *		
Remote IPv6 Subnet Prefix Length *		
Local Interface IPv6 Address *		
Remote Interface IPv6 Address *		
Ping Interval *		sec
Ping Timeout *		sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO ▾	
NAT Rules	not applied ▾	
Authenticate Mode	none ▾	
Pre-shared Secret		
CA Certificate		
DH Parameters		
Local Certificate		
Local Private Key		
Username		
Password		
Extra Options *		

* *can be blank*

Figure 3.23 Configuration > OpenVPN > 1st Tunnel

Item	Description
Description	Specifies the description or name of tunnel.

Item	Description
Protocol	Specifies the communication protocol. ■ UDP - The OpenVPN communicates using UDP. ■ TCP server - The OpenVPN communicates using TCP in server mode. ■ TCP client - The OpenVPN communicates using TCP in client mode. ■ UDPv6 - The OpenVPN communicates using UDP over IPv6. ■ TCPv6 server - The OpenVPN communicates using TCP over IPv6 in server mode. ■ TCPv6 client - The OpenVPN communicates using TCP over IPv6 in client mode.
UDP Port	Specifies the port of the relevant protocol (UDP or TCP).
Remote IP Address	Specifies the IPv4, IPv6 address or domain name of the opposite side of the tunnel.
Remote Subnet	IPv4 address of a network behind opposite side of the tunnel.
Remote Subnet Mask	IPv4 subnet mask of a network behind opposite tunnel's side.
Redirect Gateway	Activates/deactivates redirection of data on Layer 2.
Local Interface IP Address	Specifies the IPv4 address of a local interface. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.
Remote IPv6 Subnet	Specify the subnet associated with the listed remote interface.
Remote IPv6 Subnet Prefix Length	IPv6 address and prefix of the remote IPv6 network. Equivalent of the Remote Subnet and Remote Subnet Mask in IPv4 section.
Local Interface IPv6 Address	Specifies the IPv6 address of a local interface.
Remote Interface IPv6 Address	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Interval	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Timeout	Specifies the time interval the device waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the Ping Timeout to greater than the Ping Interval.
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the Authenticate Mode is set to username/password or X.509 certificate. After this time period, the device changes the tunnel encryption to help provide the continues safety of the tunnel.
Max Fragment Size	Maximum size of a sent packet.
Compression	Compression of the data sent: ■ none - No compression is used. ■ LZO - A lossless compression is used, use the same setting on both sides of the tunnel.
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel: ■ not applied - NAT rules are not applied to the tunnel. ■ applied - NAT rules are applied to the OpenVPN tunnel.

Item	Description
Authenticate Mode	Specifies the authentication mode: ■ none - No authentication is set. ■ Pre-shared secret - Specifies the shared key function for both sides of the tunnel. ■ Username/password - Specifies authentication using a CA Certificate, Username and Password. ■ X.509 Certificate (multiclient) - Activates the X.509 authentication in multi-client mode. ■ X.509 Certificate (client) - Activates the X.509 authentication in client mode. ■ X.509 Certificate (server) - Activates the X.509 authentication in server mode.
Pre-shared Secret	Specifies the pre-shared secret which you can use for every authentication mode.
CA Certificate	Specifies the CA Certificate which you can use for the username/ password and X.509 Certificate authentication modes.
DH Parameters	Specifies the protocol for the DH parameters key exchange which you can use for X.509 Certificate authentication in the server mode.
Local Certificate	Specifies the certificate used in the local device. You can use this authentication certificate for the X.509 Certificate authentication mode.
Local Private Key	Specifies the key used in the local device. You can use the key for the X.509 Certificate authentication mode.
Username	Specifies a login name which you can use for authentication in the username/password mode.
Password	Specifies a password which you can use for authentication in the username/password mode.
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are proceeded by two dashes. For possible parameters see the help text in the device using SSH - run the openvpnd --help command.

Example: OpenVPN Tunnel Configuration in IPv4 Network

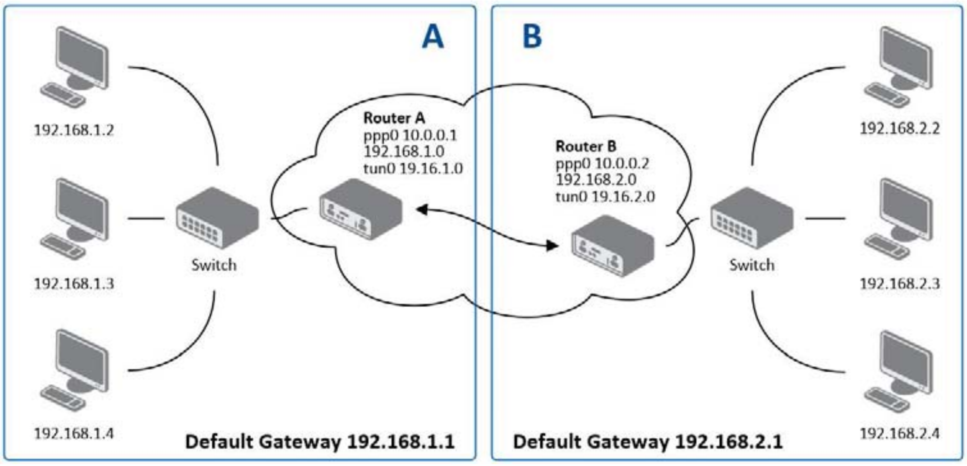


Figure 3.24 Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

Configuration	A	B
Protocol	UDP	UDP
UDP Port	1194	1194

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.16.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Examples of different options for configuration and authentication of OpenVPN tunnel can be found in the application note OpenVPN Tunnel [5].

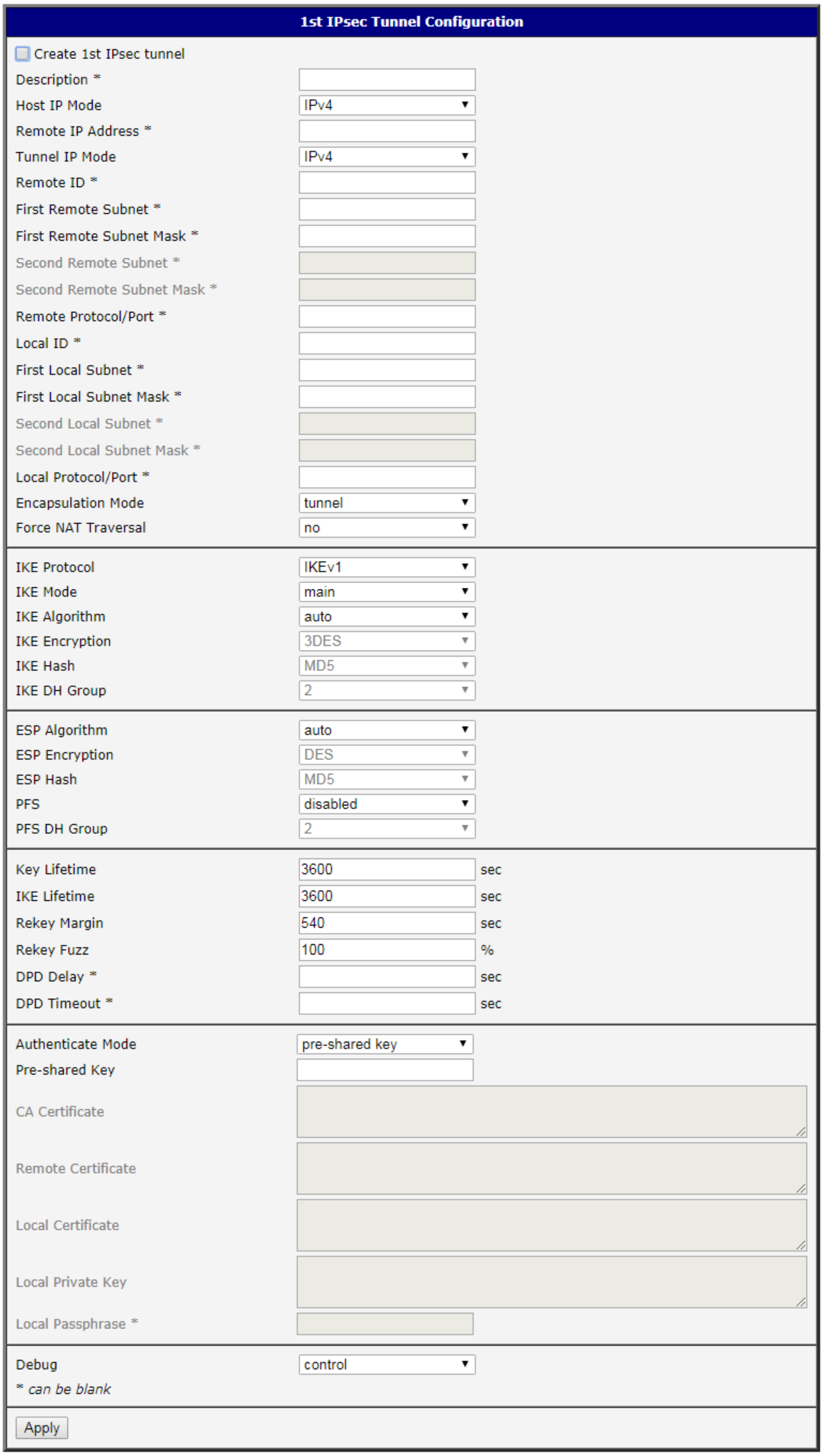
3.4.4 IPSec

To open the Tunnel Configuration page, click in the Configuration section of the main menu. The tunnel function allows you to create a secured connection between two separate LAN networks. The device allows you to create up to four tunnels. IPv4 and IPv6 tunnels are supported (dual stack), you can transport IPv6 traffic through IPv4 tunnel and vice versa.

To access this page, click **Configuration > IPSec**.

Note! *To encrypt data between the local and remote subnets, specify the appropriate values in the subnet fields on both devices. To encrypt the data stream between the devices only, leave the local and remote subnets fields blank.*

Note! *If you specify the protocol and port information in the Local Protocol/Port field, then the device encapsulates only the packets matching the settings.*



1st IPsec Tunnel Configuration

□ Create 1st IPsec tunnel

Description *		
Host IP Mode	IPv4	
Remote IP Address *		
Tunnel IP Mode	IPv4	
Remote ID *		
First Remote Subnet *		
First Remote Subnet Mask *		
Second Remote Subnet *		
Second Remote Subnet Mask *		
Remote Protocol/Port *		
Local ID *		
First Local Subnet *		
First Local Subnet Mask *		
Second Local Subnet *		
Second Local Subnet Mask *		
Local Protocol/Port *		
Encapsulation Mode	tunnel	
Force NAT Traversal	no	
IKE Protocol	IKEv1	
IKE Mode	main	
IKE Algorithm	auto	
IKE Encryption	3DES	
IKE Hash	MD5	
IKE DH Group	2	
ESP Algorithm	auto	
ESP Encryption	DES	
ESP Hash	MD5	
PFS	disabled	
PFS DH Group	2	
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
DPD Delay *		sec
DPD Timeout *		sec
Authenticate Mode	pre-shared key	
Pre-shared Key		
CA Certificate		
Remote Certificate		
Local Certificate		
Local Private Key		
Local Passphrase *		
Debug	control	

** can be blank*

Figure 3.25 Configuration > 1st Tunnel

Item	Description
Description	Name or description of the tunnel.
Host IP Mode	■ IPv4 - The device communicates via IPv4 with the opposite side of the tunnel. ■ IPv6 - The device communicates via IPv4 with the opposite side of the tunnel.
Remote IP Address	IPv4, IPv6 address or domain name of the remote side of the tunnel, based in the Host IP Mode above.
Tunnel IP Mode	■ IPv4 - The IPv4 communication runs inside the tunnel. ■ IPv6 - The IPv6 communication runs inside the tunnel.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: a hostname and a domain-name.
Remote Subnet	IPv4 or IPv6 address of a network behind remote side of the tunnel, based on Tunnel IP Mode above.
Remote Subnet Mask	IPv4 subnet mask of a network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128).
Remote Protocol/ Port	Specifies Protocol/Port of remote side of the tunnel. The general form is protocol /port, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: a hostname and a domain-name.
Local Subnet	IPv4 or IPv6 address of a local network, based on Tunnel IP Mode above.
First Local Subnet Mask	IPv4 subnet mask of a local network, or IPv6 prefix (single number 0 to 128).
Local Protocol/Port	Specifies Protocol/Port of a local network. The general form is protocol /port, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Encapsulation Mode	Specifies the mode, according to the method of encapsulation. You can select the tunnel mode in which the entire IP datagram is encapsulated or the transport mode in which only IP header is encapsulated.
Force NAT Traversal	Enable/disables NAT address translation on the tunnel. Enable if you use NAT between the end points of the tunnel.
IKE Protocol	Click the drop-down menu to select to define a protocol (IKEv1/IKEv2, IKEv1, or IKEv2). IKE Phase 1 is ISAKMP (Internet Security Association and Key Management Protocol), which is used to create private tunnelling between peers for a secure communication.
IKE Mode	Specifies the mode for establishing a connection (main or aggressive). If you select the aggressive mode, then the device establishes the tunnel faster, but the encryption is permanently set to 3DES-MD5. We recommend that you not use the aggressive mode due to lower security!
IKE Algorithm	Specifies the means by which the device selects the algorithm: ■ auto - The encryption and hash algorithm are selected automatically. ■ manual - The encryption and hash algorithm are defined by the user.
IKE Encryption	Encryption algorithm - 3DES, AES128, AES192, AES256.
IKE Hash	Hash algorithm - MD5, SHA1, SHA256, SHA384 or SHA512.

Item	Description
IKE DH Group	Specifies the Diffie-Hellman groups which determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require more time to compute the key.
ESP Algorithm	Specifies the means by which the device selects the algorithm: ■ auto - The encryption and hash algorithm are selected automatically. ■ manual - The encryption and hash algorithm are defined by the user.
ESP Encryption	Encryption algorithm - DES, 3DES, AES128, AES192, AES256.
ESP Hash	Hash algorithm - MD5, SHA1, SHA256, SHA384 or SHA512.
PFS	Enables/disables the Perfect Forward Secrecy function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future.
PFS DH Group	Specifies the Diffie-Hellman group number (see IKE DH Group).
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before a connection expires that the device attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage of time for the Rekey Margin extension.
DPD Delay	Time after which the tunnel functionality is tested.
DPD Timeout	The period during which device waits for a response.
Authenticate Mode	Specifies the means by which the device authenticates: ■ Pre-shared key - Sets the shared key for both sides of the tunnel. ■ X.509 Certificate - Allows X.509 authentication in multiclient mode.
Pre-shared Key	Specifies the shared key for both sides of the tunnel. The prerequisite for entering a key is that you select pre-shared key as the authentication mode.
CA Certificate	Certificate for X.509 authentication.
Remote Certificate	Certificate for X.509 authentication.
Local Certificate	Certificate for X.509 authentication.
Local Private Key	Private key for X.509 authentication.
Local Passphrase	Passphrase used during private key generation.
Debug	Choose the level of verbosity to System Log. Silent (default), audit, control, control-more, raw, private (most verbose including the private keys). See strongSwan documentation for more details.

The function supports the following types of identifiers (ID) for both sides of the tunnel, Remote ID and Local ID parameters:

- IP address (for example, 192.168.1.1)
- DN (for example, C=CZ, O=CompanyName, OU=TP, CN=A)
- FQDN (for example, @director.companyname.cz) - the @ symbol proceeds the FQDN.
- User FQDN (for example, director@companyname.cz)

The certificates and private keys have to be in the PEM format. Use only certificates containing start and stop tags.

The random time, after which the device re-exchanges new keys is defined as follows:

Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))

The default exchange of keys is in the following time range:

- Minimal time: 1h - (9m + 9m) = 42m
- Maximal time: 1h - (9m + 0m) = 51m

We recommend that you maintain the default settings. When you set key exchange times higher, the tunnel produces lower operating costs, but the setting also provides less security. Conversely, when you reducing the time, the tunnel produces higher operating costs, but provides for higher security.

The changes in settings will apply after clicking the **Apply** button.

Example: Tunnel Configuration in IPv4 Network

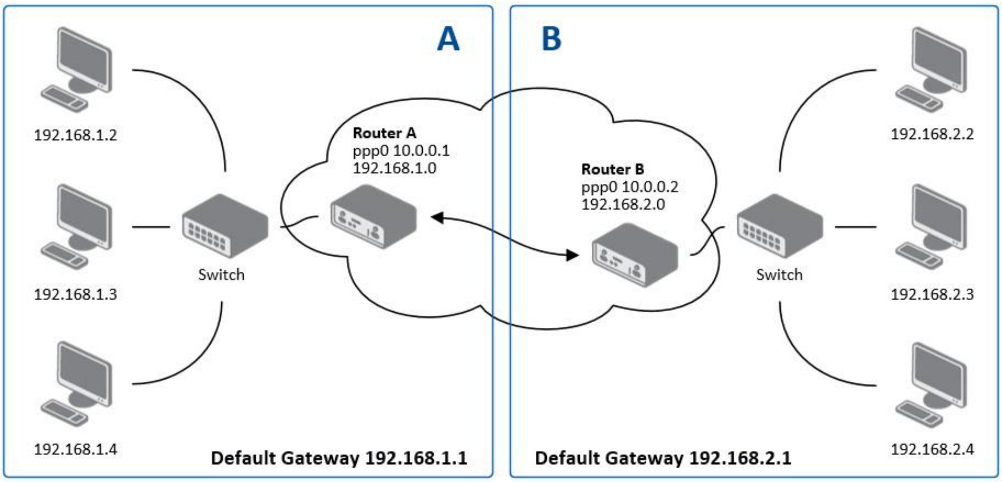


Figure 3.26 Topology of Configuration Example

tunnel configuration:

Configuration	A	B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mask	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

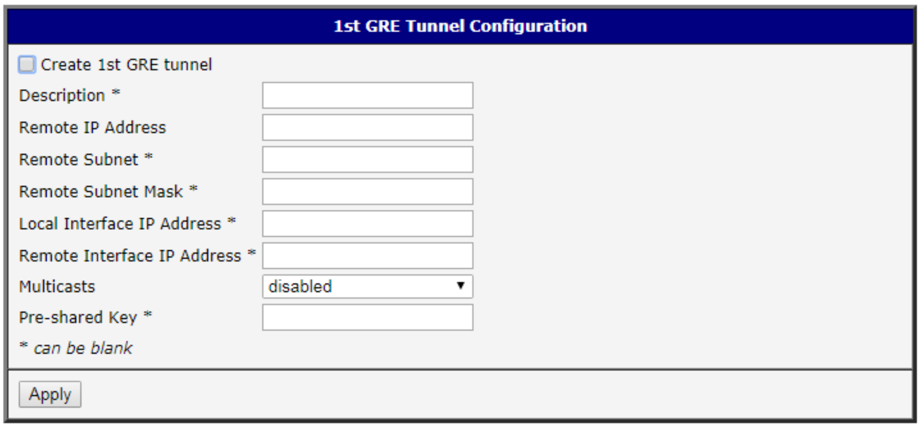
Examples of different options for configuration and authentication of tunnel can be found in the application note Tunnel [6].

3.4.5 GRE

Note! *GRE is an unencrypted protocol. GRE via IPv6 is not supported.*

To open the GRE Tunnel Configuration page, click GRE in the Configuration section of the main menu. The GRE tunnel function allows you to create an unencrypted connection between two separate LAN networks. The device allows you to create four GRE tunnels.

To access this page, click **Configuration** > **GRE**.



1st GRE Tunnel Configuration

□ Create 1st GRE tunnel

Description *	
Remote IP Address	
Remote Subnet *	
Remote Subnet Mask *	
Local Interface IP Address *	
Remote Interface IP Address *	
Multicasts	disabled
Pre-shared Key *	

* can be blank

Figure 3.27 Configuration > GRE > 1st Tunnel

Item	**Description**
Description	Description of the GRE tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	IP address of the network behind the remote side of the tunnel.
Remote Subnet Mask	Specifies the mask of the network behind the remote side of the tunnel.
Local Interface IP Address	IP address of the local side of the tunnel.
Remote Interface IP Address	IP address of the remote side of the tunnel.
Multicasts	Activates/deactivates sending multicast into the GRE tunnel: ■ disabled - Sending multicast into the tunnel is inactive. ■ enabled - Sending multicast into the tunnel is active.
Pre-shared Key	Specifies an optional value for the 32 bit shared key in numeric format, with this key the device sends the filtered data through the tunnel. Specify the same key on both devices, otherwise the device drops received packets.

Note! *The GRE tunnel does not pass through NAT.*

The changes in settings will apply after pressing the **Apply** button.

Example: GRE Tunnel Configuration

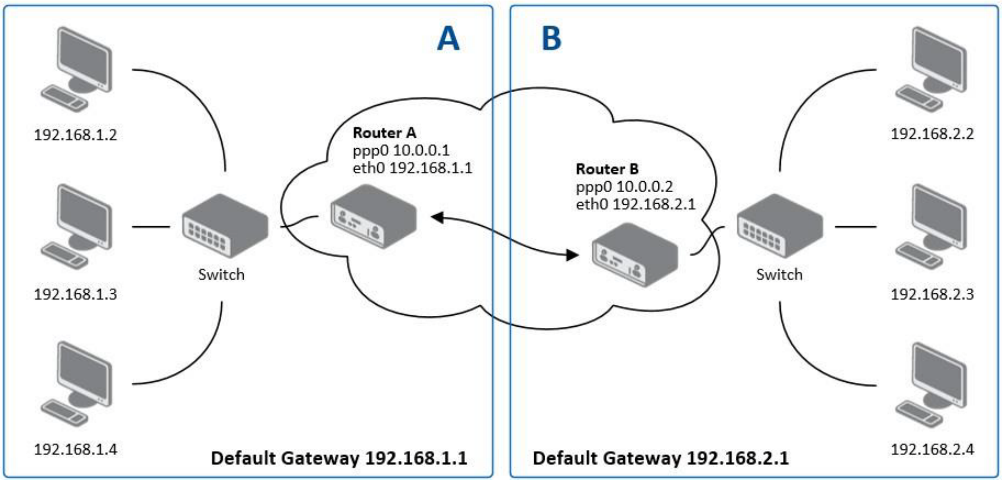


Figure 3.28 Topology of GRE Tunnel Configuration Example

GRE tunnel configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

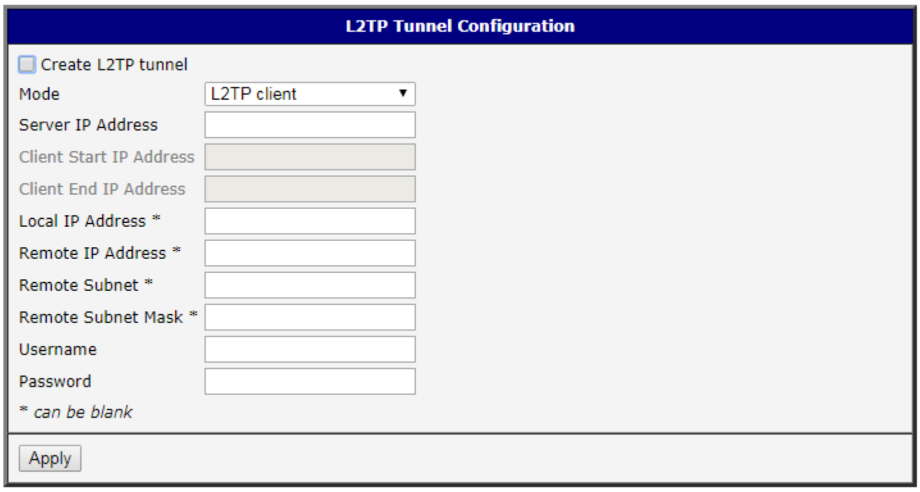
Examples of different options for configuration of GRE tunnel can be found in the application note GRE Tunnel [7].

3.4.6 L2TP

Note! *L2TP is an unencrypted protocol. L2TP via IPv6 is not supported.*

To open the L2TP Tunnel Configuration page, click L2TP in the Configuration section of the main menu. The L2TP tunnel function allows you to create a password protected connection between 2 LAN networks. The device activates the tunnels after you mark the Create L2TP tunnel check box.

To access this page, click **Configuration** > **L2TP**.



L2TP Tunnel Configuration

□ Create L2TP tunnel

Mode	L2TP client ▾
Server IP Address	
Client Start IP Address	
Client End IP Address	
Local IP Address *	
Remote IP Address *	
Remote Subnet *	
Remote Subnet Mask *	
Username	
Password	

** can be blank*

Apply

Figure 3.29 Configuration > L2TP

Item	**Description**
Mode	Specifies the L2TP tunnel mode on the device side: ■ L2TP server - Specify an IP address range offered by the server. ■ L2TP client - Specify the IP address of the server.
Server IP Address	IP address of the server.
Client Start IP Address	IP address to start with in the address range. The range is offered by the server to the clients.
Client End IP Address	The last IP address in the address range. The range is offered by the server to the clients.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.
Username	Username for the L2TP tunnel login.
Password	Password for the L2TP tunnel login.

Example: L2TP Tunnel Configuration

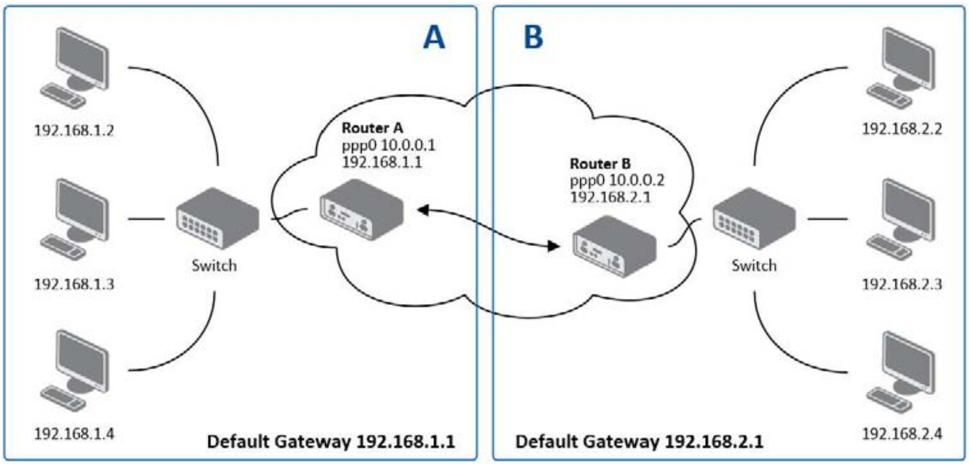


Figure 3.30 Topology of L2TP Tunnel Configuration Example

Configuration of the L2TP tunnel:

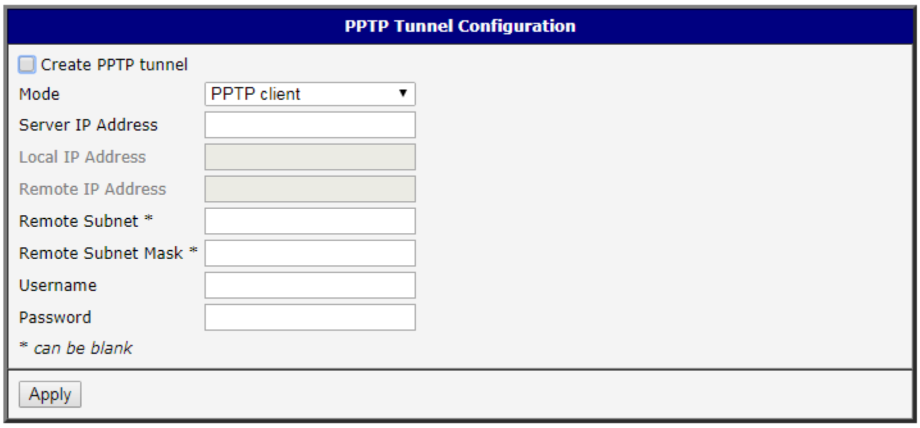
Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	N/A	10.0.0.1
Client Start IP Address	192.168.2.5	N/A
Client End IP Address	192.168.2.254	N/A
Local IP Address	192.168.1.1	N/A
Remote IP Address	N/A	N/A
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

3.4.7 PPTP

Note! *PPTP is an unencrypted protocol. PPTP via IPv6 is not supported.*

Select the PPTP item in the menu to configure a PPTP tunnel. PPTP tunnel allows password protected connections between two LANs. It is similar to L2TP. The tunnels are active after selecting Create PPTP tunnel.

To access this page, click **Configuration** > **PPTP**.



PPTP Tunnel Configuration

☐ Create PPTP tunnel

Mode	PPTP client ▾
Server IP Address	
Local IP Address	
Remote IP Address	
Remote Subnet *	
Remote Subnet Mask *	
Username	
Password	

* can be blank

Figure 3.31 Configuration > PPTP

Item	Description
Mode	Specifies the L2TP tunnel mode on the device side: ■ PPTP server - Specify an IP address range offered by the server. ■ PPTP client - Specify the IP address of the server.
Server IP Address	IP address of the server.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.

Item	Description
Username	Username for the PPTP tunnel login.
Password	Password for the PPTP tunnel login.

The changes in settings will apply after pressing the **Apply** button.

The firmware also supports PPTP pass through, which means that it is possible to create a tunnel through the device.

Example: PPTP Tunnel Configuration

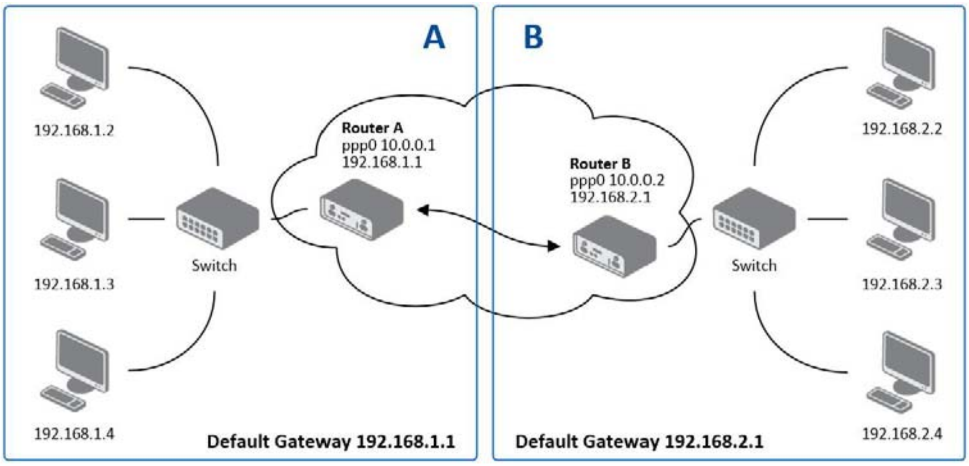


Figure 3.32 Topology of PPTP Tunnel Configuration Example

Configuration of the PPTP tunnel:

Configuration	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	N/A	10.0.0.1
Local IP Address	192.168.1.1	N/A
Remote IP Address	192.168.2.1	N/A
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

3.4.8 Services

3.4.8.1 DynDNS

The DynDNS function allows you to access the device remotely using an easy to remember custom hostname. This DynDNS client monitors the IP address of the device and updates the address whenever it changes. In order for DynDNS to function, you require a public IP address, either static or dynamic, and an active Remote Access service account at www.dyndns.org. Register the custom domain (third-level) and account information specified in the configuration form. You can use other services, too - see the table below, Server item. To open the DynDNS Configuration page, click DynDNS in the main menu.