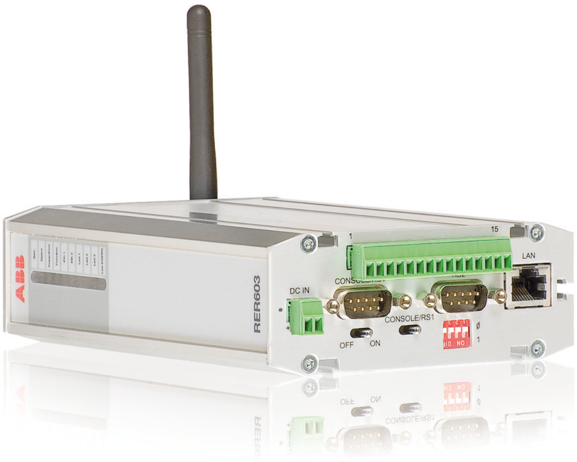
Wireless Gateway RER601/603 Technical Manual

Power and productivity
for a better world™



Document ID: 1MRS757105
Issued: 2014-08-18
Revision: B
Product version: 1.2

Copyright

Trademarks

Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

http://www.abb.com/substationautomation

Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/ or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This product has been designed to be connected and communicate data and information via a network interface which should be connected to a secure network. It is the sole responsibility of the person or entity responsible for network administration to ensure a secure connection to the network and to take the necessary measures (such as, but not limited to, installation of firewalls, application of authentication measures, encryption of data, installation of anti virus programs, etc.) to protect the product and the network, its system and interface included, against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for any such damages and/or losses.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.

Conformity

This product complies with the following Electro Magnetic Combatibility (EMC) standards: ETSI EN 301489-1 (V1.8.1 2008-04), IEC 61000-6-1 (Second edition 2005–01) and IEC 61000-6-3 (2006–07).

Table of contents

Section 1 Introduction

1.1 This manual

The technical manual contains product overview, installation and mounting instructions, descriptions of physical connections, Web configurator interface and IEC 60870-5-104 interoperability. The manual can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

1.2 Intended audience

This manual addresses system engineers and installation and commissioning personnel, who use technical data during engineering, installation and commissioning, and in normal service.

1.3 Product documentation

1.3.1 Document revision history

Document revision/date	Product series version	History
A/2011-09-02	1.0	First release
B/2014-08-18	1.2	Content updated

Download the latest documents from the ABB Website http://www.abb.com/substationautomation.

1.3.2 Related documentation

Product series- and product-specific manuals can be downloaded from the ABB Web site http://www.abb.com/substationautomation.

1.4 Symbols and conventions

1.4.1 Symbols

The electrical warning icon indicates the presence of a hazard which could result in electrical shock.

The warning icon indicates the presence of a hazard which could result in personal injury.

The caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.

The information icon alerts the reader of important facts and conditions.

The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

Although warning hazards are related to personal injury, it is necessary to understand that under certain operational conditions, operation of damaged equipment may result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warning and caution notices.

1.4.2 Manual conventions

Conventions used in manuals. A particular convention may not be used in this manual.

- Abbreviations and acronyms in this manual are spelled out in the glossary. The glossary also contains definitions of important terms.
- Parameter names are shown in italics.
  The function can be enabled and disabled with the *Operation* setting.
- Parameter values are indicated with quotation marks.
  The corresponding parameter values are “On“ and “Off”.

Section 2 RER601/603 overview

2.1 Overview

The IEC 60870-5-104 gateway offers industrial quality connectivity for the IEC 60870 protocol family. IEC 60870-5-104 is a vendor-independent communication standard for the electricity industry. With the IEC 60870-5-104 gateway, conventional IEC 60870-5-101 devices can be attached to a modern TCP/IP based IEC 60870-5-104 control system. The Ethernet and GPRS network interfaces provide seamless communication for most applications.

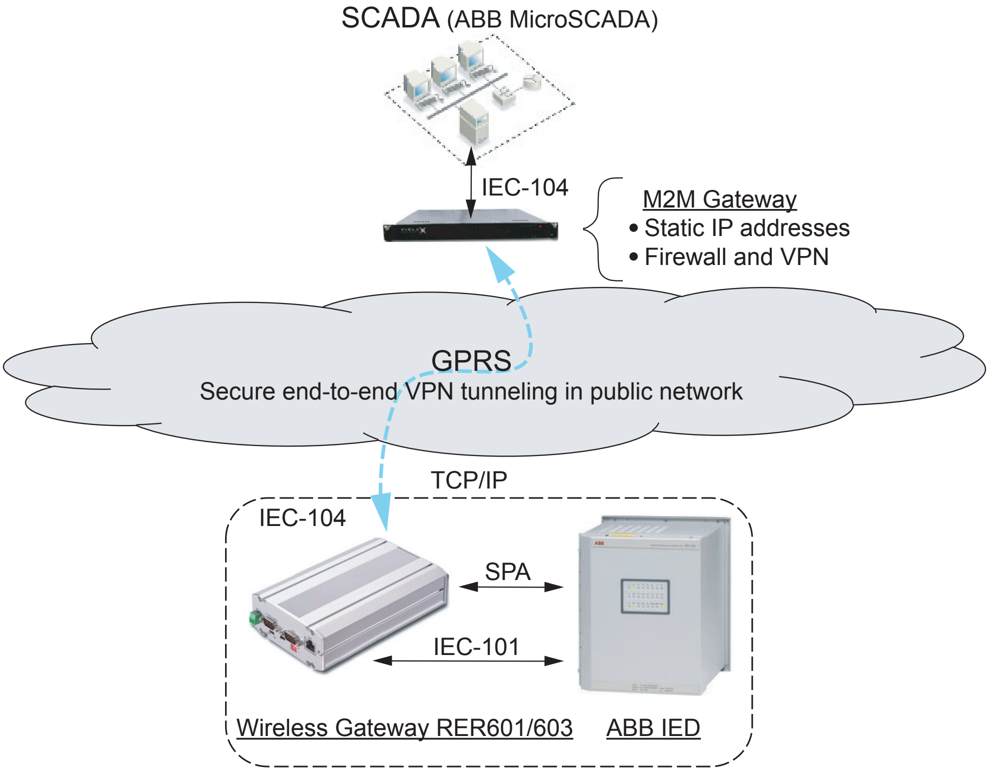


Figure 1: Typical connection

The device contains three panels for interface connections and status indication.

- The front panel includes all the connectors and switches for the device's operation, optional input and output connectors, and the connectors for the network and serial interface.
- The back panel contains the GPRS antenna connector and the SIM card holder.
- The side panel contains all the LEDs that indicate the status of the device.

2.1.1 Product version history

Product version	Product history
1.0	First release
1.2	Support for Viola Patrol remote device monitoring

2.2 Front panel

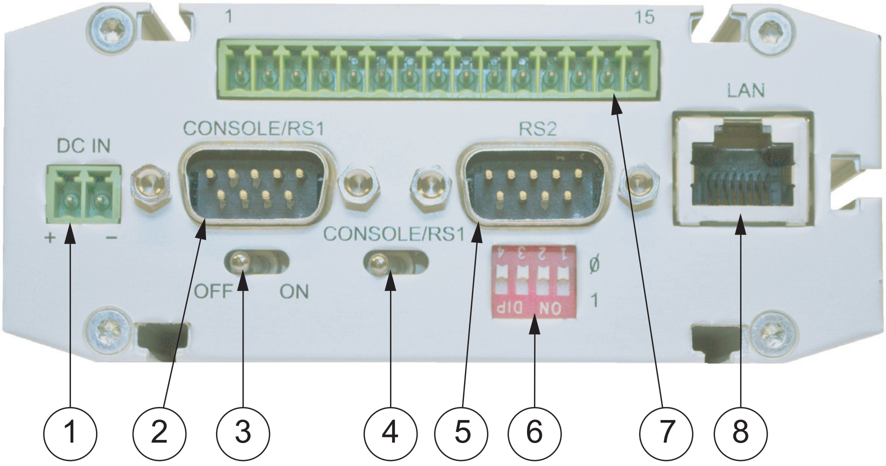


Figure 2: Front panel

1 Power supply connector

2 Console serial port (RS1)

3 Power switch

4 Console switch

5 Application serial port (RS2)

6 DIP switches

7 I/O extension (only available for RER603)

8 Ethernet connector

The device has rails for wall or rack mounting. The front panel contains slots for nuts or other optional mounting accessories to gain access to the rails.

2.2.1 Power switch

Use the power switch to switch the device's power on or off.

2.2.2 Console switch

The console switch enables or disables console access. When console access is disabled, both serial ports may be used as an application serial port. When the switch is in the right position, RS1 is in the serial port mode and when it is in the left position, RS1 is in the console mode.

2.2.3 DIP switches

The DIP switches are used to select an application port mode (RS-2) and settings (RS-232 or RS-485). By default, all are set to “0” when the port is in the RS-232 mode. DIP switches 2-4 apply only when the RS-485 mode is selected with DIP switch 1.

Table 1: DIP switches

Number	Function	State	Description
1	RS-232/RS-485	“0” = RS-232 ”1” = RS-485	Selects the RS-port operation
2	HALF/FULL	“0” = full “1” = half	Selects between half-duplex (2-wire) and full duplex (4-wire)
3	BIAS	“0” = OFF “1” = ON	Turns RS-485 biasing on or off
4	TERMINATION	“0” = OFF “1” = ON	Turns RS-485 termination on or off

2.3 Back panel

The IEC 60870-5-104 gateway has an antenna connector and a slot for a SIM card on the back panel.

Do not insert or remove the SIM card while the GPRS module is in operation. The SIM card contents may become corrupted if the card is removed while the GPRS module is writing data to it.

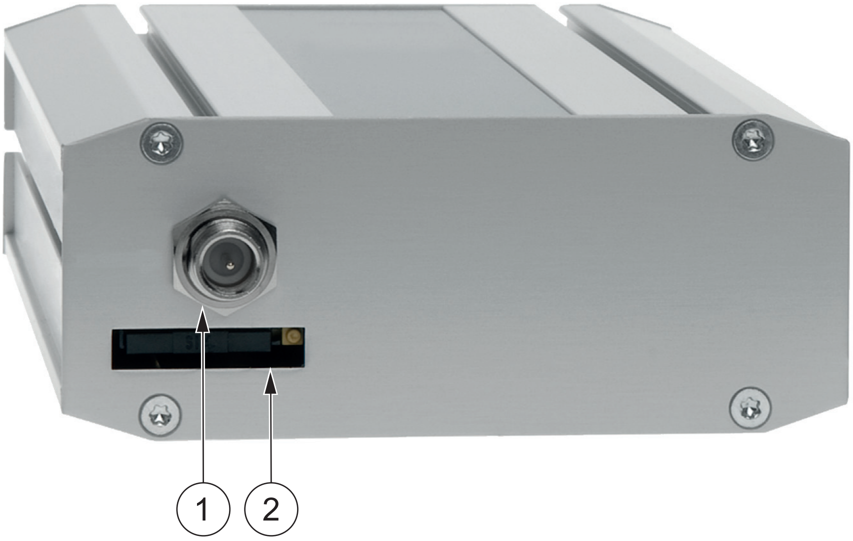


Figure 3: Back panel

1 FME connector for an antenna

2 SIM card slot

2.4 Console/serial port 1

The serial port 1 (RS1) is a full RS-232 port.

Table 2: RS-232 port PIN description

Pin number	Name	Direction	Description
1	DCD	IN	Data Carrier Detect
2	RXD	IN	Received data
3	TXD	OUT	Transmitted data
4	DTR	OUT	Data Terminal Ready, handshake output
5	GND	-	Signal ground
6	DSR	IN	Data Set Ready, handshake input
7	RTS	OUT	Ready To Send, handshake output
8	CTS	IN	Clear To Send, handshake input
9	RI	IN	Ring Indicator

2.5 Ethernet

The device has an RJ-45 connector for a 10/100 Mbps Ethernet connection. The maximum length of the Ethernet cable is 100 m.

The cross-connected cable is only used for connecting the device to the PC network interface card. Use a direct Ethernet cable to connect to the local network, for example, to a hub or a switch.

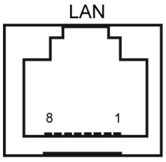


Figure 4: RJ-45 Ethernet connector

Table 3: RJ-45 Ethernet connector PIN description

Pin number	Name	Direction	Description
1	Rx+	IN	Data Receive Positive
2	Rx-	IN	Data Receive Negative
3	Tx+	OUT	Data Transmit Positive
4	NC	-	-
5	NC	-	-
6	Tx-	OUT	Data Transmit Negative
7	NC	-	-
8	NC	-	-

2.6 Power supply connector

The device has a 10–26 V DC power supply connector. The unit is protected against reversed polarity.

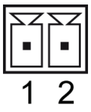


Figure 5: Power supply connector

1	Pin 1 (+)
2	Pin 2 (-)

2.7 Side panel

The side panel contains LEDs that indicate the status of the device. Only five of them are connected. The LEDs are numbered 1–10 starting from the rear panel side.

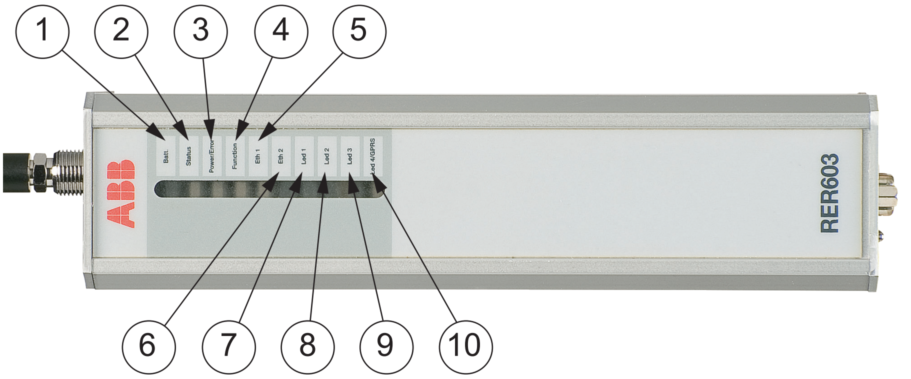


Figure 6: LED description

Table 4: Description of available LEDs o the side panel

LED number	LED	LED status	Description
1	Batt.	-	LED unassigned
2	Status	On Blinking Off	VPN connection is up VPN onnection is starting VPN connection is disabled
3	Power/Error	On Off	Operating power is turned on Operating power is turned off
4	Function	On Blinking Off	Device is starting Device is operating normally Device is not operational
5	Eth 1	On Blinking Off	Ethernet link is up Ethernet link is transferring data Ethernet link is down
6	Eth 2	-	LED reserved for future functionality
7	Led 1	-	LED reserved for future functionality
8	Led 2	-	LED reserved for future functionality

Table continues on next page

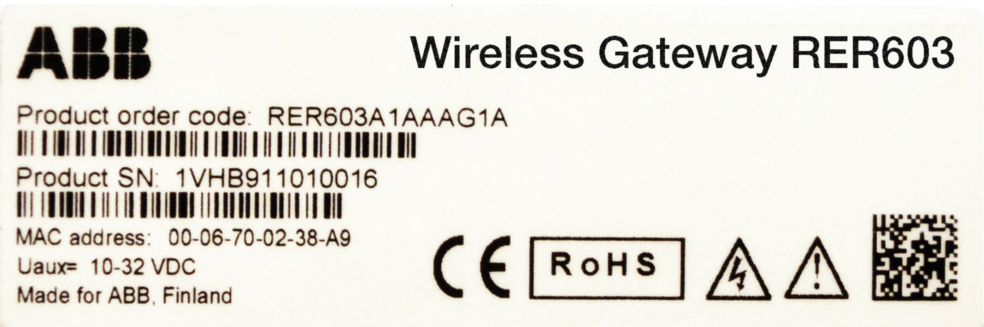
LED number	LED	LED status	Description
9	Led 3	-	LED reserved for future functionality
10	Led 4/GPRS	Blinking Off	GPRS is starting or transferring data GPRS is inactive

2.8 DIN rail mounting

The device has mounting holes for DIN rail mounting brackets.

2.9 Product label

The product label is located on the bottom of the device. It contains the basic information about the unit such as product name, serial number and Ethernet MAC address.



ABB

Wireless Gateway RER603

Product order code: RER603A1AAAG1A

Product SN: 1VHB911010016

MAC address: 00-06-70-02-38-A9

Uaux= 10-32 VDC

Made for ABB, Finland

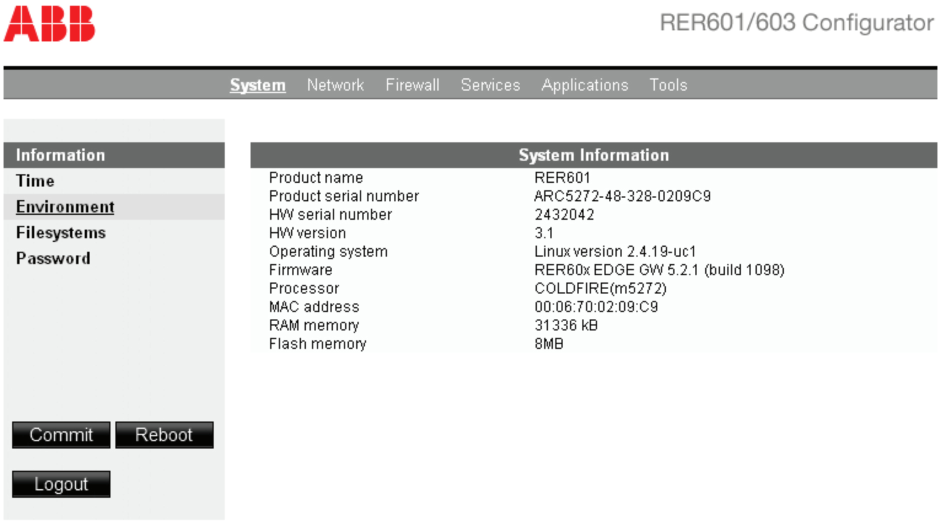
CE RoHS

Figure 7: Product label

2.10 Firmware version

The device firmware version can be checked from the REC601/603 configurator start page (**System/Information**), or by executing the “firmware” command via the console.

This manual describes the RER601 and RER603 Ver.1.2 firmware 5.2.8.



System Information	
Product name	RER601
Product serial number	ARC5272-48-328-0209C9
HW serial number	2432042
HW version	3.1
Operating system	Linux version 2.4.19-uc1
Firmware	RER60x EDGE GW 5.2.1 (build 1098)
Processor	COLDFIRE(m5272)
MAC address	00:06:70:02:09:C9
RAM memory	31336 kB
Flash memory	8MB

Figure 8: Firmware version

Section 3 Physical connections

3.1 Serial ports

The device has two 9-pin male serial port connectors (DB9). A null modem cable can be used to connect the device to a serial device or a PC. The device supports CTS/RTS flow control.

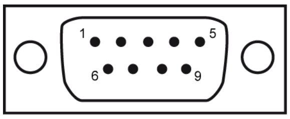


Figure 9: DB9 (DTE) male connector

3.1.1 Serial port 2

The serial port 2 (RS2) can be configured either as a half-RS-232 or an RS-422/485 (DTE Master). The pin description is the same as in RS1, when the port is in the RS-232 mode.

Do not connect the RS-422 or RS-485 devices to a port which has been configured to operate as an RS-232 port.

Table 5: RS-485 port PIN description

Pin number	RS-485 full duplex (4-wire)	RS-485 half-duplex (2-wire)
1	NC	NC
2	RXD+ (in)	NC
3	TXD- (out)	TXD/RXD- (out/in)
4	NC	NC
5	GND	GND
6	NC	NC
7	TXD+ (out)	TXD/RXD+ (out/in)
8	RXD- (in)	NC
9	NC	NC

3.2 GPRS

The device with GPRS includes an FME male type connector for an external antenna. Any kind of external 50 Ω dual-band antenna can be used intended for GSM900 (880–960 MHz) and GSM1800, also known as PCN, (1710–1880 MHz) frequency bands. The antenna is connected directly to the connector located on the device's back panel.

Commercially available antennas are usually provided with a flexible 50 Ω cable with a length of 2–3 meters and a female type FME connector.

The device's IEC 60870-5-104 gateway is tested with antennas from Hirschmann Rheinmetall Elektronik GmbH. Examples of tested external antennas include the sticker type and magnetic mount antennas.

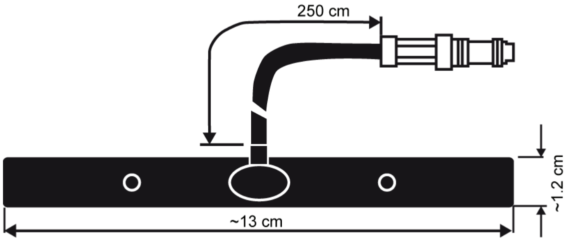


Figure 10: Sticker type patch antenna (MCA 18 90 STRIPE)

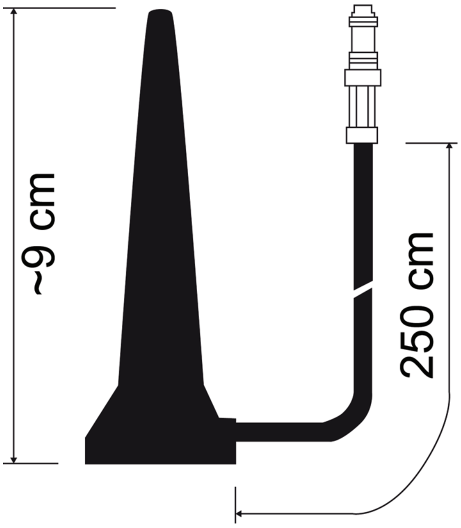


Figure 11: Magnetic mount antenna (MCA 18 90 MH)

Both antennas have an FME connector (female) and a 250 cm RG174 cable.

A SIM card with enabled data transfer is required for using the wireless connection. Standard 3 V SIM cards may be used with the IEC 60870-5-104 gateway. A SIM card holder is located on the back panel near the GPRS antenna connector.

If the PIN code query is enabled, check that the RER601/603 configurator has the correct PIN code entered in the GPRS submenu.

3.3 RER603 I/O extension

Wireless Gateway RER603 has eight binary inputs for monitoring and fault indication applications, and two binary outputs for disconnector control and alarm acknowledgement.

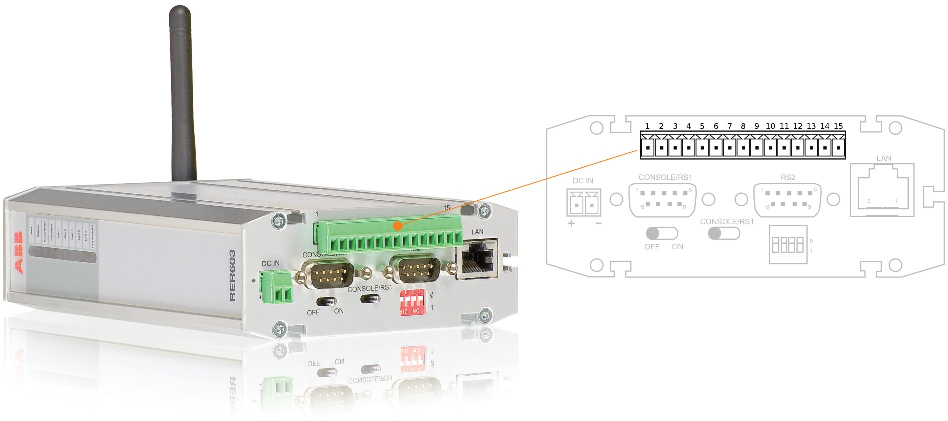


Figure 12: RER603 I/O extension

Table 6: RER603 I/O connector pins

PIN	Symbol	Description
1	V+	Vcc out, 50 mA
2	DI_1	Digital input, 0...60V
3	DI_2	Digital input, 0...60V
4	DI_3	Digital input, 0...60V
5	DI_4	Digital input, 0...60V
6	DI_5	Digital input, 0...60V
7	DI_6	Digital input, 0...60V
8	DI_7	Digital input, 0...60V
9	DI_8	Digital input, 0...60V
10	DI_COM	Digital inputs referense input
11	DO_1A	Digital output pole 1, 0...60V, 50 mA

Table continues on next page

PIN	Symbol	Description
12	DO_1B	Digital output pole 2
13	DO_2A	Digital output pole 2, 0...60V, 50 mA
14	DO_2B	Digital output pole 2
15	GND	GND output

Section 4 Cyber security

Cyber security aims to secure the properties of the organization against security risks. To strengthen the system and increase the security level towards any cyber security attacks from the Internet, certain actions are recommended while configuring the device.

- The device should be installed physically secure, for example, in a locked cabinet.
- The latest security updates need to be installed for all network devices.
- The network inventory needs to be documented and kept up to date.
- Unused services and interfaces should always be disabled.
- Only VPN connections should be used to access remote networks.

4.1 Enhancing operator and subscription security

Network subscription and SIM card must be stored safely and configured to prevent misuse of services.

- Disable unused services from SIM cards.
  - Voice calls
  - SMS
  - Paid services
  - Roaming
- Use pin code in SIM cards.
- Prefer a private APN service from the operator.
- Prefer M2M subscription SIM cards from the operator.
- Use private IP addressing from the operator for GPRS communications.
- If connected to a public IP network, do not use plain text protocols such as http, SNMP and telnet. Always use VPN to connect to the device.

4.2 Configuring firewall and services

Enable the firewall and disable the unused services and interfaces in the device. To start, disallow traffic and allow only the needed traffic. Use the default policy to drop connections.

- Check that the firewall is enabled.
- For incoming connections, always filter (drop) all unused ports which may include DNS, L2TP-VPN, SNMP and so on.
- Check that the default action is “drop” in firewalls and allow only the needed ports.
- Set unique passwords for each device.
- Keep passwords stored in a safe place, for example, Encrypted password management tool.
- Check that all unused services are disabled.
- If possible, allow IP connections only via VPN.
- Disable all unused services, for example, Dial-in, SMSconfig, serial and SNMP.
- Back up the configuration.

Section 5 RER601/603 Configurator

5.1 Overview

RER601/603 configurator is a tool which is used to manage the device properties via a user-friendly, Web-based interface.

To use the Web configurator, only a computer with an HTML browser and a connection to the device are needed. With the configurator, it is possible to receive status information and set parameters and variables that control which applications and processes are used with the device.

After a successful login, the main window is displayed. It consists of the main navigation menu on the top, the navigation bar on the left, and the content area that displays the currently active content and controls.

When the program starts for the first time, the System/Information window is displayed in the content area. The main navigation menu on the top of the window is used to navigate between the different subsets of the available settings. Selecting an item from the main menu displays the available items related to this subset in the navigation bar. The first of these is displayed in the content area by default.

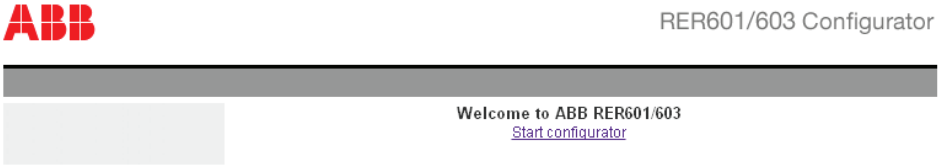
The navigation bar on the left contains the parameter groups in the subset. Selecting an item from this menu displays the content related to the selected group in the content area.

Three buttons are always visible at the bottom of the navigation bar.

- The **Commit** button is used to save the memory-resident data for “soft” parameters permanently to the nonvolatile memory. The values for the previous parameters are not saved permanently unless this button is pressed.
- The **Reboot** button is used to reboot the device.
- The **Logout** button ends the current session and returns to the login window.

5.2 Login to the Web Configurator

1. Open the device from the URL where the device is located.
2. On the device main page, click the **Start Configurator** link.

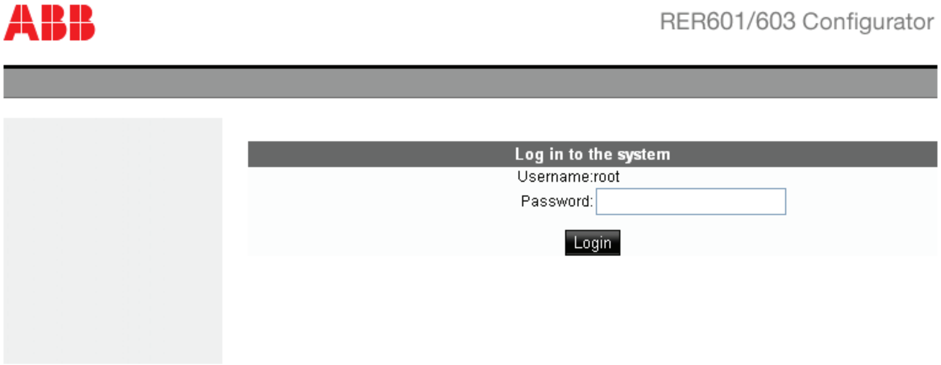


Welcome to ABB RER601/603
Start configurator

Figure 13: Start Configurator link

3. Enter the password for the device's root account and click the **Login** button to start the Web configurator tool.

The default password for the root is empty. Set the password before connecting the device to a public network. Change the password from the **System/Password** menu.



Log in to the system
Username:root
Password:

Figure 14: System login

5.3 System menu

The System menu can be used to view information about the system or the current executing environment and to set the date and time.

Updated time information is not saved permanently until the Commit button is pressed.

Information

Contains general information about the device. Information on this submenu should be provided, if possible, when contacting technical support.

Time

For adjusting time information. The device has a real-time clock with battery backup.

Environment

Contains information about the device's memory usage, uptime and inside temperature.

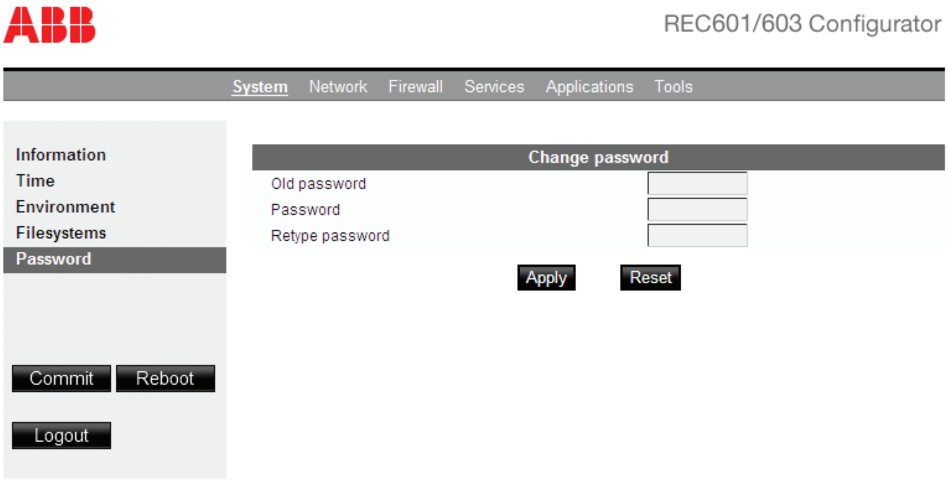
Password

For changing the password. The default password is blank.

5.3.1 Changing the password

It is recommended that the default password is changed before connecting the device to a public network. The default password for the root account is empty.

1. Click **Password**.
   - When changing the password for the first time, type the new password in all three fields, **Old password**, **Password** and **Retype password**.
   - When changing an old password, type the old password in the **Old password** field, type the new password in the **Password** field and retype the new password in the **Retype password** field.
2. Click **Apply** and then **Commit** to store the settings.
3. Click **Reboot** for the settings to take effect.



Change password

Old password

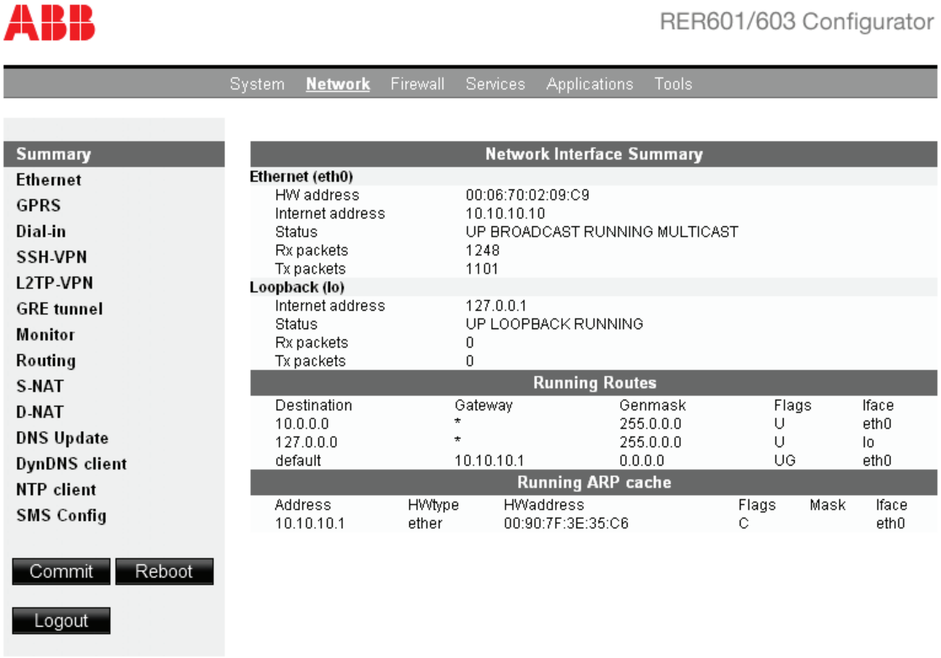
Password

Retype password

Figure 15: Changing the password

5.4 Network menu

The network interface properties are controlled through the Network menu. The menu contains items for the Ethernet, GPRS and VPN interfaces. The Network Interface Summary page shows the currently active interfaces and routing information.



Network Interface Summary

Ethernet (eth0)	
HW address	00:06:70:02:09:C9
Internet address	10.10.10.10
Status	UP BROADCAST RUNNING MULTICAST
Rx packets	1248
Tx packets	1101
Loopback (lo)	
Internet address	127.0.0.1
Status	UP LOOPBACK RUNNING
Rx packets	0
Tx packets	0

Running Routes

Destination	Gateway	Genmask	Flags	Iface
10.0.0.0	*	255.0.0.0	U	eth0
127.0.0.0	*	255.0.0.0	U	lo
default	10.10.10.1	0.0.0.0	UG	eth0

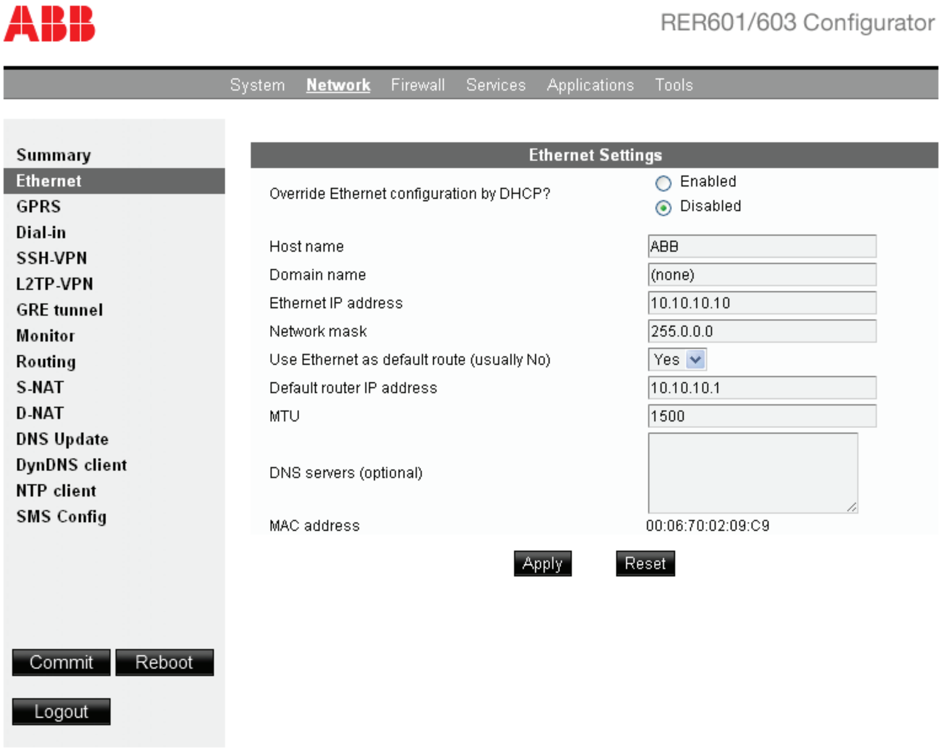
Running ARP cache

Address	HWtype	HWaddress	Flags	Mask	Iface
10.10.10.1	ether	00:90:7F:3E:35:C6	C		eth0

Figure 16: Network interface summary

5.4.1 Ethernet

The device's Ethernet interface is configured via the Ethernet command in the Network menu. Clicking this command displays the Ethernet settings in the content area.



Ethernet Settings

Override Ethernet configuration by DHCP?	○ Enabled ● Disabled
Host name	ABB
Domain name	(none)
Ethernet IP address	10.10.10.10
Network mask	255.0.0.0
Use Ethernet as default route (usually No)	Yes
Default router IP address	10.10.10.1
MTU	1500
DNS servers (optional)	
MAC address	00:06:70:02:09:C9

Figure 17: Ethernet settings

Override Ethernet configuration by DHCP? If enabled, the device gets the IP address and other related information from a local DHCP server. When enabled, all other settings are disabled on this page.

Host name sets the device host name. Each device connected to the gateway must have a unique host name. This is important to set up correctly when using the gateway and VPN.

Domain name determines the domain name for name resolution (optional).

Ethernet IP address determines the IP address used by the eth0 interface.

Network mask determines the network mask used by the eth0 interface.

Use Ethernet as default route should be set to “Yes” only if Ethernet is used as the default gateway or router. Usually this parameter is set to “No”, because either GPRS or VPN is used as the default route. This parameter overrides the next parameter *Default Route IP Address*, so that parameter has no effect if *Use Ethernet as default route* is set to “No“

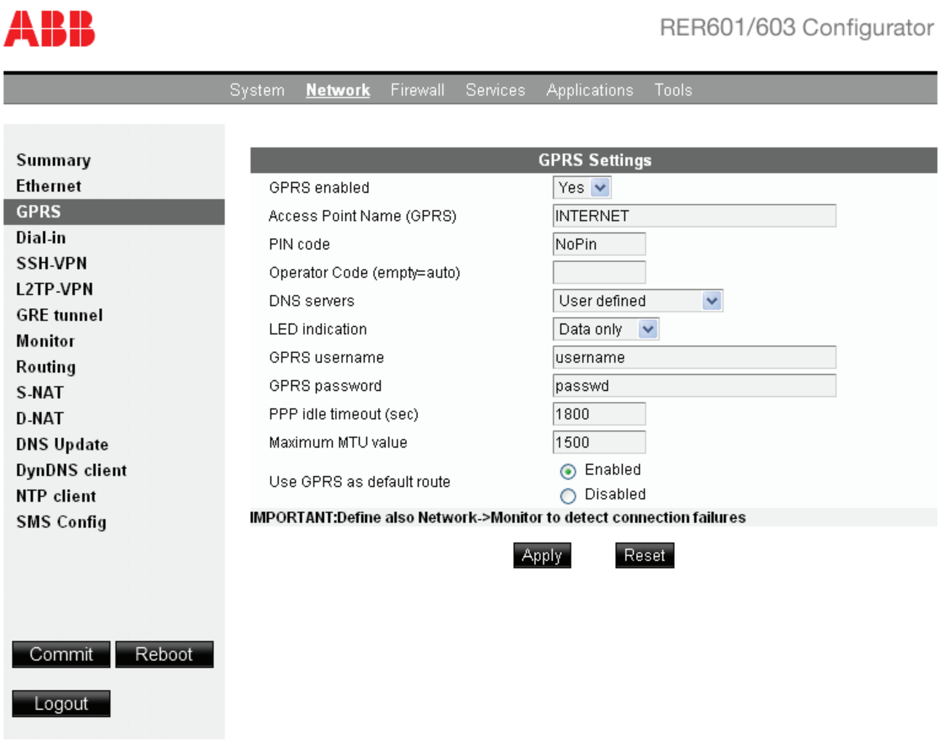
Default Router IP address determines the default router or default gateway used when the direct route to the host or network is not known. Applies to the eth0 interface only. When GPRS or VPN is used as the default gateway, this parameter is set to “0”.

MTU determines the maximum transfer unit (MTU) for the Ethernet interface (usually 1500).

DNS servers (optional) determines the name server IP (DNS) address for resolving host names to the IP address and vice versa. Applicable when the GPRS parameter *DNS servers* is set to “User defined”.

5.4.2 GPRS

The GPRS settings include APN and other settings for the GPRS network connection.



GPRS Settings

GPRS enabled	Yes
Access Point Name (GPRS)	INTERNET
PIN code	NoPin
Operator Code (empty=auto)	
DNS servers	User defined
LED indication	Data only
GPRS username	username
GPRS password	passwd
PPP idle timeout (sec)	1800
Maximum MTU value	1500
Use GPRS as default route	● Enabled ○ Disabled

IMPORTANT:Define also Network->Monitor to detect connection failures

Figure 18: GPRS settings

GPRS enabled When set to ”Yes”, the GPRS interface is automatically connected to the GPRS network.

Access Point Name (GPRS) determines the GPRS Access Point Name (APN) for the connection.

PIN code determines the SIM card PIN code.

Operator Code (empty=auto) is a manually selected operator code. Leave empty for automatic network selection (default).

DNS servers When set to “User defined”, DNS servers defined on the Ethernet page are used. If set to “From GPRS network”, the device receives the DNS server IP addresses automatically from the GPRS network.

Led indication When set to “Data only”, the GPRS LED blinks green when transmitting data. When set to “Informative”, the LED blinks also when connected to the GPRS network without data transfer (GPRS context is active).

GPRS username determines the user name used for authentication, if APN requires it.

GPRS password determines the password used for authentication, if APN requires it.

PPP idle timeout determines the maximum idle time for the GPRS interface. If the GPRS interface has been idle (no traffic) for this period, the GPRS connection is restarted.

Maximum MTU value determines the maximum transfer unit (MTU) for GPRS.

Use GPRS as default route If enabled, GPRS is used as the default route. The Ethernet default gateway has to be disabled by setting the parameter *Use Ethernet as default route* to “No” in **Network/Ethernet**.

5.4.3 Dial-in

The device's PPP dial-in interface is configured via the Dial-in command in the Network menu. Clicking this command displays the Dial-in settings in the content area.

Dial-in enabled If enabled, PPP connections can be made to the device (GSM data).

Require authentication (PAP) determines if password authentication is used for incoming data calls.

Required username determines the PAP user name.

Required password determines the PAP password used for authentication.

Idle timeout determines the length of idle time before the PPP connection is terminated.

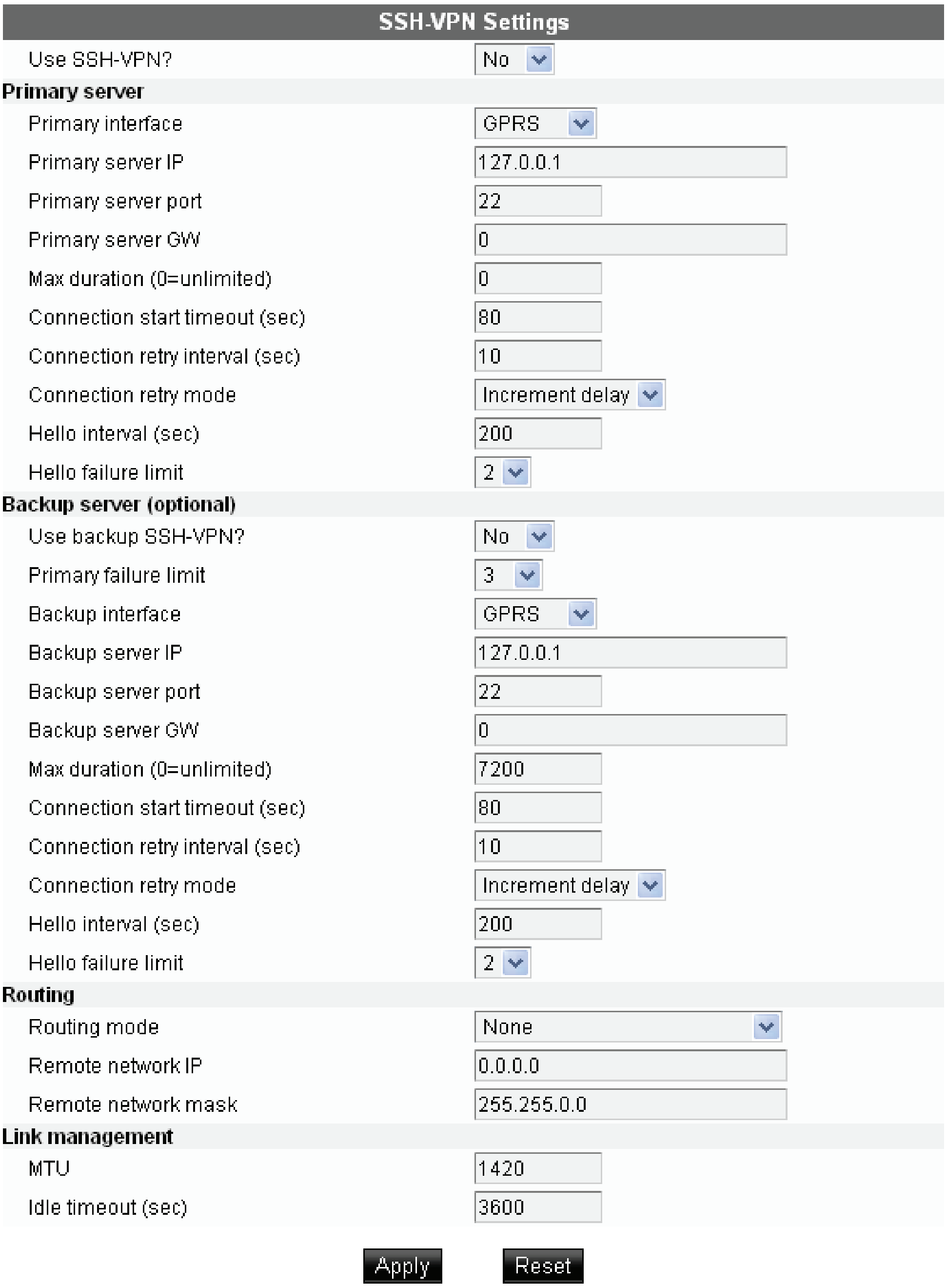
Local IP address determines the IP address used in the PPP peer.

Peer's IP address determines the IP address used in the PPP peer.

Maximum MTU value determines the maximum transfer unit (MTU) for dial-in connections.

5.4.4 SSH-VPN

The device has a VPN client that can be used with the gateway.



SSH-VPN Settings	
Use SSH-VPN?	No
Primary server	
Primary interface	GPRS
Primary server IP	127.0.0.1
Primary server port	22
Primary server GW	0
Max duration (0=unlimited)	0
Connection start timeout (sec)	80
Connection retry interval (sec)	10
Connection retry mode	Increment delay
Hello interval (sec)	200
Hello failure limit	2
Backup server (optional)	
Use backup SSH-VPN?	No
Primary failure limit	3
Backup interface	GPRS
Backup server IP	127.0.0.1
Backup server port	22
Backup server GW	0
Max duration (0=unlimited)	7200
Connection start timeout (sec)	80
Connection retry interval (sec)	10
Connection retry mode	Increment delay
Hello interval (sec)	200
Hello failure limit	2
Routing	
Routing mode	None
Remote network IP	0.0.0.0
Remote network mask	255.255.0.0
Link management	
MTU	1420
Idle timeout (sec)	3600

Figure 19: SSH-VPN settings

Primary server

Use SSH-VPN? When set to “Yes”, the device automatically establishes a SSH-VPN connection to the primary gateway.

Primary interface determines the interface used to reach the gateway server.

Primary server IP determines the IP address of the gateway SSH-VPN server.

Primary server port determines the SSH-VPN TCP port on the primary server. The default is 22.

Primary server GW is used if another gateway than the default route is needed to reach the gateway.

Max duration (0=unlimited) determines the maximum duration of the VPN connection. On the primary server, this should be set to zero. With the backup server, the primary server is tried again after this time-out.

Connection start timeout (sec) determines the time to wait until the connection is established.

Connection retry interval (sec) determines the time interval after which the connection is retried.

Connection retry mode increases incrementally the retry interval on each connection attempt. Constant delay always uses the same delay.

Hello interval (sec) determines the Hello packet interval for the VPN. This can be used as a keep-alive message on very critical links.

Hello failure limit determines the number of Hello packets that can be lost before restarting the connection.

Backup server (optional)

Use backup SSH-VPN? When set to “Yes”, the device tries to establish a VPN connection to back up the gateway, if the primary gateway cannot be reached.

Primary failure limit determines the number of times the primary must not be reached before changing to the secondary. The other parameters are same as in the primary server. The duration of the connection can be set, for example, to 3600 seconds, so after one hour's connection time to the backup server, the system tries to reach the secondary gateway.

Routing

Routing mode has three modes.

- Tunnel the following network. This adds the “Remote network IP” to be reached via the SSH-VPN. The parameters *Remote network IP* and *Remote network mask* must be set.
- Default route. The VPN interface is used as the default route.
- None. No routing is added when the VPN is established. The VPN peer IPs can be used for communications.

Remote network IP determines the remote network IP behind the VPN on the gateway side that the device needs to reach.

Remote network mask determines the network mask for the remote network IP.

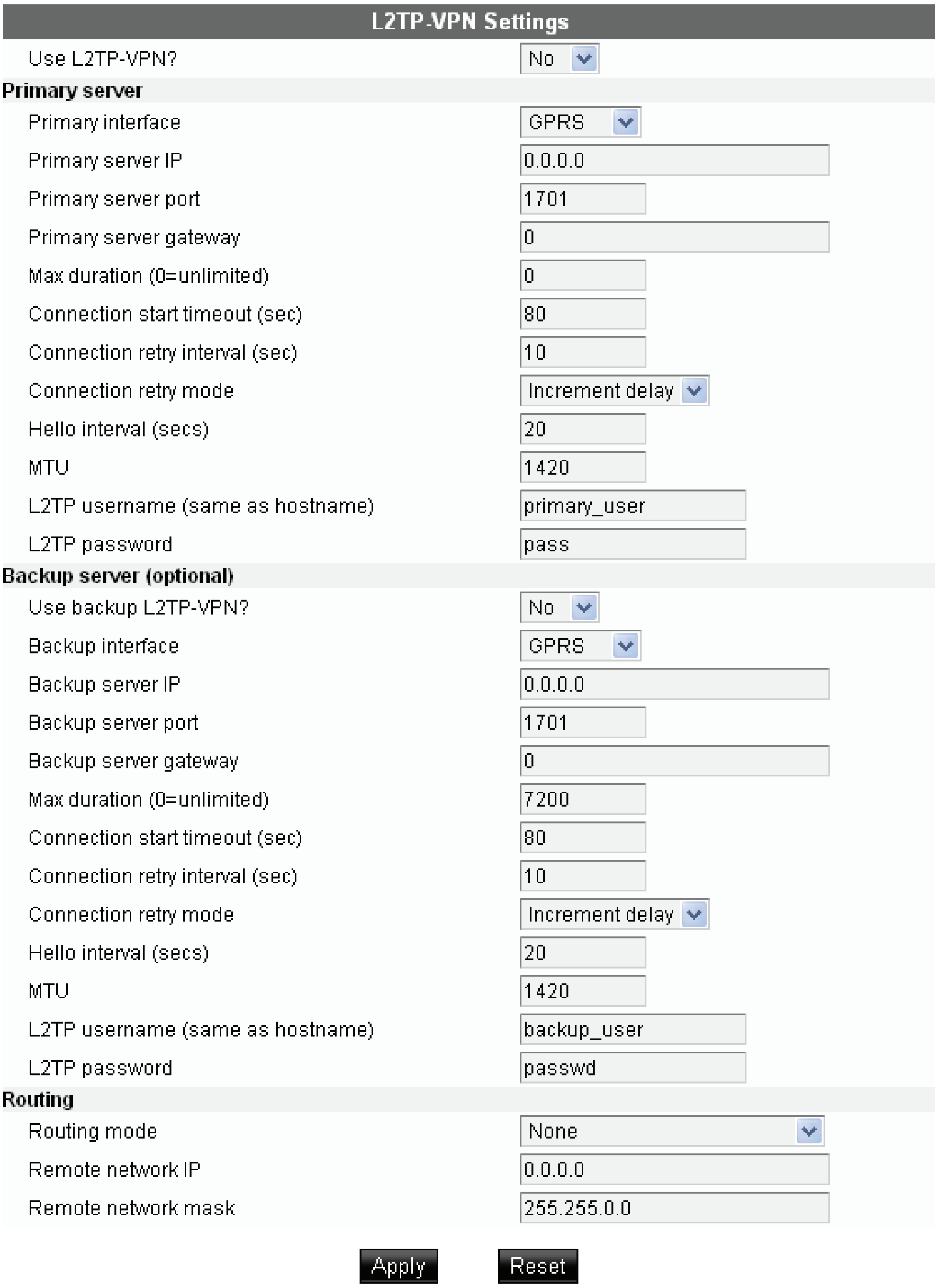
Link management

MTU determines the maximum transfer unit (MTU) for the SSH-VPN interface.

Idle timeout (sec) determines the idle time-out for the SSH-VPN interface. If the time-out is reached, the VPN connection is restarted.

5.4.5 L2TP-VPN

The device has an L2TP client that can be used with an L2TP server.



L2TP-VPN Settings	
Use L2TP-VPN?	No
Primary server	
Primary interface	GPRS
Primary server IP	0.0.0.0
Primary server port	1701
Primary server gateway	0
Max duration (0=unlimited)	0
Connection start timeout (sec)	80
Connection retry interval (sec)	10
Connection retry mode	Increment delay
Hello interval (secs)	20
MTU	1420
L2TP username (same as hostname)	primary_user
L2TP password	pass
Backup server (optional)	
Use backup L2TP-VPN?	No
Backup interface	GPRS
Backup server IP	0.0.0.0
Backup server port	1701
Backup server gateway	0
Max duration (0=unlimited)	7200
Connection start timeout (sec)	80
Connection retry interval (sec)	10
Connection retry mode	Increment delay
Hello interval (secs)	20
MTU	1420
L2TP username (same as hostname)	backup_user
L2TP password	passwd
Routing	
Routing mode	None
Remote network IP	0.0.0.0
Remote network mask	255.255.0.0

Figure 20: L2TP-VPN Settings

If the primary server cannot be reached, the L2TP VPN connection is established with a backup server.

Primary server

Use L2TP-VPN? When set to “Yes”, the device establishes an L2TP VPN connection with the primary gateway.

Primary interface determines the interface used to reach the gateway server.

Primary server IP determines the IP address of the gateway L2TP server.

Primary server port determines the L2TP VPN server port (UDP, default 1701).

Primary server gateway is used if another gateway than the default route is needed to reach the gateway.

Max duration (0=unlimited) determines the maximum duration of the VPN connection. On the primary server, this should be set to zero.

Hello interval (secs) determines the Hello interval for keeping the connection alive. The default is 20 seconds.

MTU determines the maximum transfer unit for the L2TP interface.

L2TP username (usually hostname) determines the user name for authentication.

L2TP password determines the L2TP password for authentication.

Routing

Routing mode is used if routing is needed with the L2TP interface. The parameters are the same as for SSH-VPN.

5.4.6 GRE

The GRE tunnel command in the Network menu is used to configure the GRE settings.

GRE tunnel enabled When set to “Yes”, the device establishes the GRE connection automatically.

Interface determines the interface used for the GRE server.

GRE server IP determines the IP address of the GRE server.

Gw to GRE server (Ethernet mode) (Optional) is used if another gateway than the default route is needed for the GRE server.

Local GRE interface IP (usually eth0 IP) determines the local IP address used in the GRE tunnel.

Remote GRE interface IP (Optional) determines the remote IP address used in the GRE tunnel.

TTL value determines the time to live value for the interface.

Checksum (Optional) determines the checksum value.

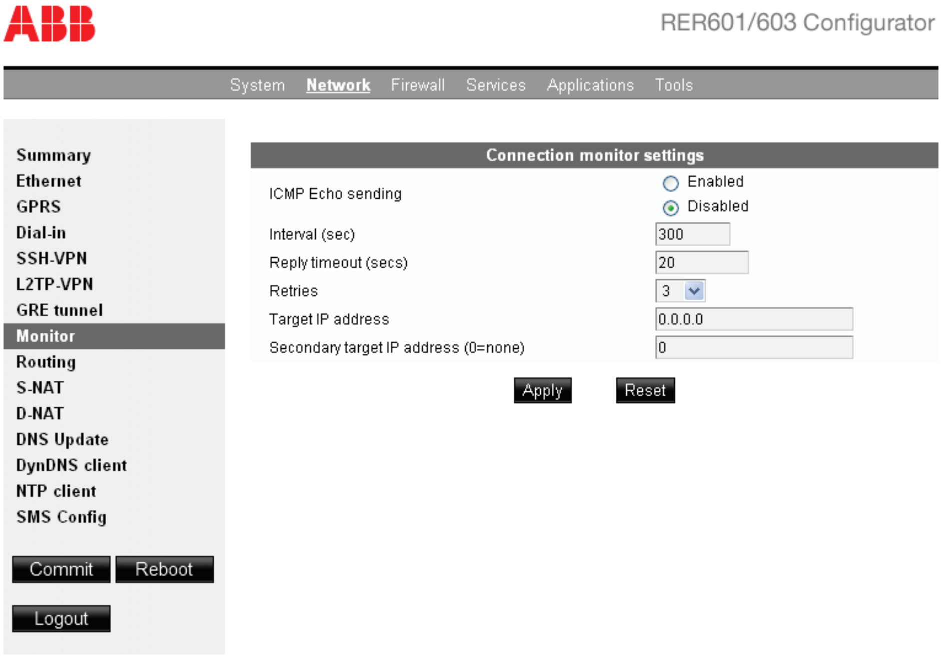
Incoming key determines the authentication key.

Outgoing key (Optional) determines the outgoing key for the server.

The optional routing parameters *Routing mode*, *Remote network* and *Remote network mask* are the same as in SSH-VPN and L2TP.

5.4.7 Monitor

The monitor settings are used for checking the GPRS and VPN connections. If the connection to the selected IP address is lost, the connection is restarted. The monitor uses ICMP echo (ping) packets to check the connection. The monitor also keeps the connection alive, so that idle time-out does not end the connection.



Connection monitor settings

ICMP Echo sending	○ Enabled ● Disabled
Interval (sec)	300
Reply timeout (secs)	20
Retries	3
Target IP address	0.0.0.0
Secondary target IP address (0=none)	0

Figure 21: Monitor settings

ICMP Echo sending is used to enable the monitor. The monitor must always be enabled for the correct IP. When VPN is used, the remote VPN peer IP address (or other IP address reached only via VPN) must be used for checking the connection.

Interval (sec) determines how often the connection is checked by sending ICMP echo packets. The interval should be smaller than the GPRS idle time-out (typically maximum 2/3 of GPRS idle time-out) for uninterrupted communication.

Reply timeout (secs) determines the waiting time for reply packets.

Retries determines the number of retries before the connection is restarted.

Target IP address determines the host IP address to which the ICMP echo packets are sent.

Secondary target IP address determines the secondary host IP address to which ICMP echo packets are sent if sending to the primary target host IP address fails.

5.4.8 Routing

The routing settings of the device can be configured in the Routing menu.

5.4.8.1 S-NAT

These parameters are used to configure the S-NAT settings. When enabled, the private IP address used in the LAN is changed to the GPRS interface IP address.

From IP determines that only S-NAT connections from the defined IP address are allowed. If defined with wildcard (0/0), all IP addresses are handled in the same way.

5.4.8.2 D-NAT

These parameters are used to configure the D-NAT settings. When enabled, packets coming to the defined GPRS interface port are forwarded to the local IP address.

Source IP determines the D-NAT connections coming from the IP address. If defined with wildcard (0/0), all IP addresses are handled in the same way.

Protocol determines the protocol that is forwarded. If the value “Any” is selected, other parameters are ignored.

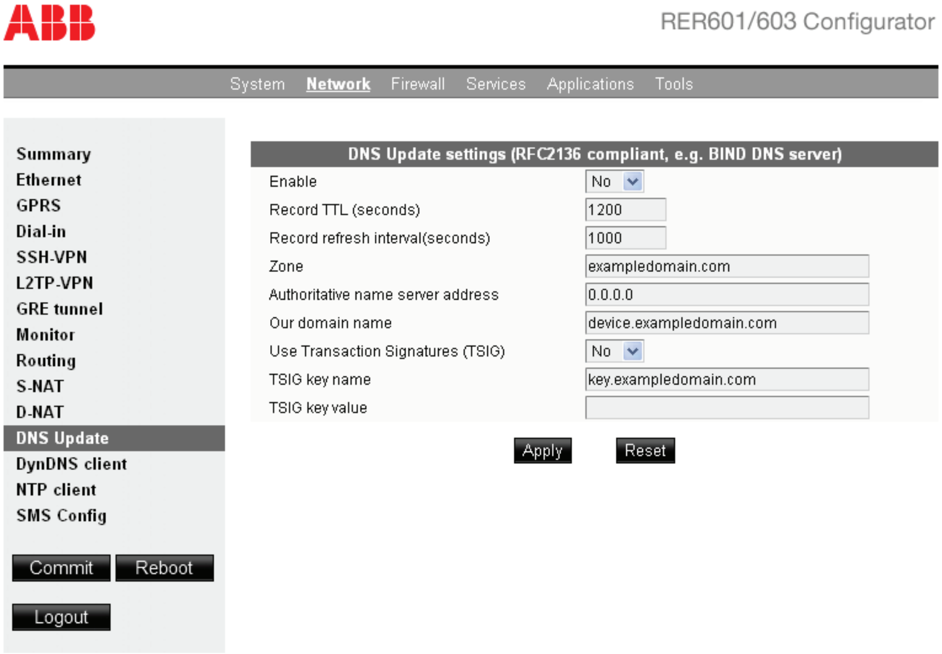
Dest.port determines the GPRS interface that is forwarded to the local Ethernet.

Redirect to IP determines the IP address used in the forwarding.

Redir. port determines the port used in the forwarding.

5.4.8.3 DNS Update

The DNS Update parameters are used to configure the dynamic DNS. The device can report its dynamic IP address to a DNS server. These settings are RFC2136 compliant, for example, for BIND DNS server.



DNS Update settings (RFC2136 compliant, e.g. BIND DNS server)

Enable	No
Record TTL (seconds)	1200
Record refresh interval(seconds)	1000
Zone	exampledomain.com
Authoritative name server address	0.0.0.0
Our domain name	device.exampledomain.com
Use Transaction Signatures (TSIG)	No
TSIG key name	key.exampledomain.com
TSIG key value	

Figure 22: DNS Update settings

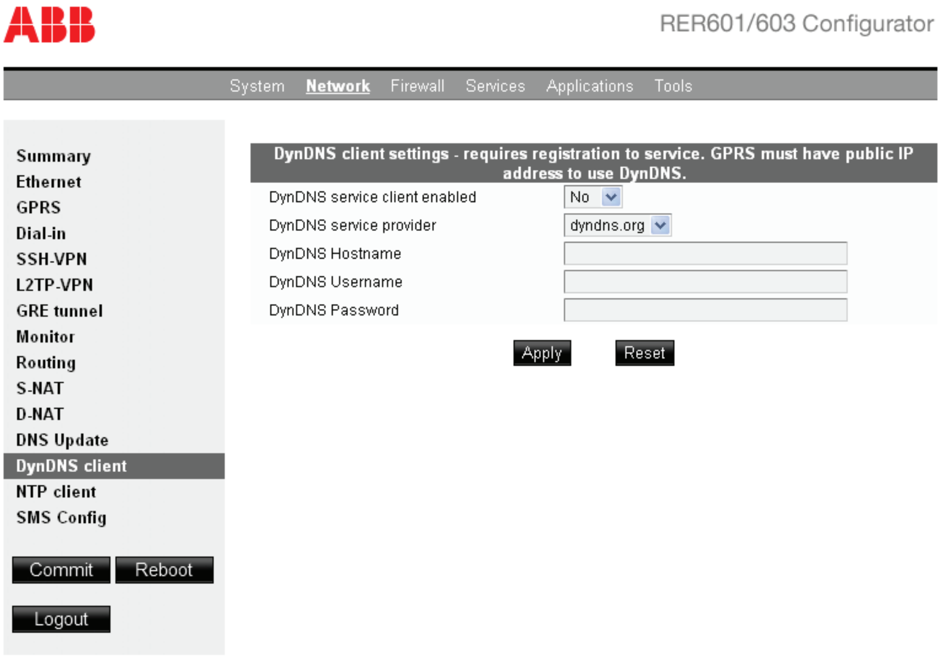
Authoritative name server determines the server that must be configured to accept the incoming DNS update messages, for example, the company's own DNS server, such as ISC BIND.

TSIG key name TSIG keys can be used for better security in DNS updates.

5.4.8.4 DynDNS client

These settings can be used with the DynDNS service available at http://www.dyndns.org.

The public IP address is required for GPRS and the user account from the DynDNS service operator.



DynDNS client settings - requires registration to service. GPRS must have public IP address to use DynDNS.

DynDNS service client enabled	No
DynDNS service provider	dyndns.org
DynDNS Hostname	
DynDNS Username	
DynDNS Password	

Figure 23: DynDNS client settings

DynDNS service client enabled disables or enables the DNS name update.

DynDNS service provider determines the service provider. Only dyndsn.org is currently supported.

DynDNS Hostname determines the service provider account host name.

DynDNS Username determines the service provider user name.

DynDNS Password determines the service provider password.

5.4.8.5 NTP client

The NTP client settings can be used to update the real-time clock of the device using the NTP protocol.

NTP server When enabled, the device updates the system clock from the NTP server.

Query interval determines the time interval for an NTP query.

Minimum time difference (seconds) determines the minimum time difference when the clock is updated.

Maximum time difference determines the maximum time difference between local system time and NTP time when the clock is updated.

Time adjust mode adds or subtracts time from the received NTP value.

Time adjust value (minutes) determines the value to add or substract from the NTP value.

5.4.8.6 SMS Config

The SMS Config settings can be used to monitor the device status and to issue simple commands remotely via SMS messages.

Enabled enables or disables the SMS configuration.

Get commands

Access determines if the get commands are allowed for everybody or only for the defined phone, or if they are disabled.

Allowed phone determines the phone number for get commands.

Require password determines if the system password is required for get commands.

Set commands

Access determines if the set commands are allowed for everybody or only for the defined phone, or if they are disabled.

Allowed phone determines the phone number for set commands.

Require password determines if the system password is required for set commands.

Allow execute commands determines if execute commands are allowed to be run on the device.

Other

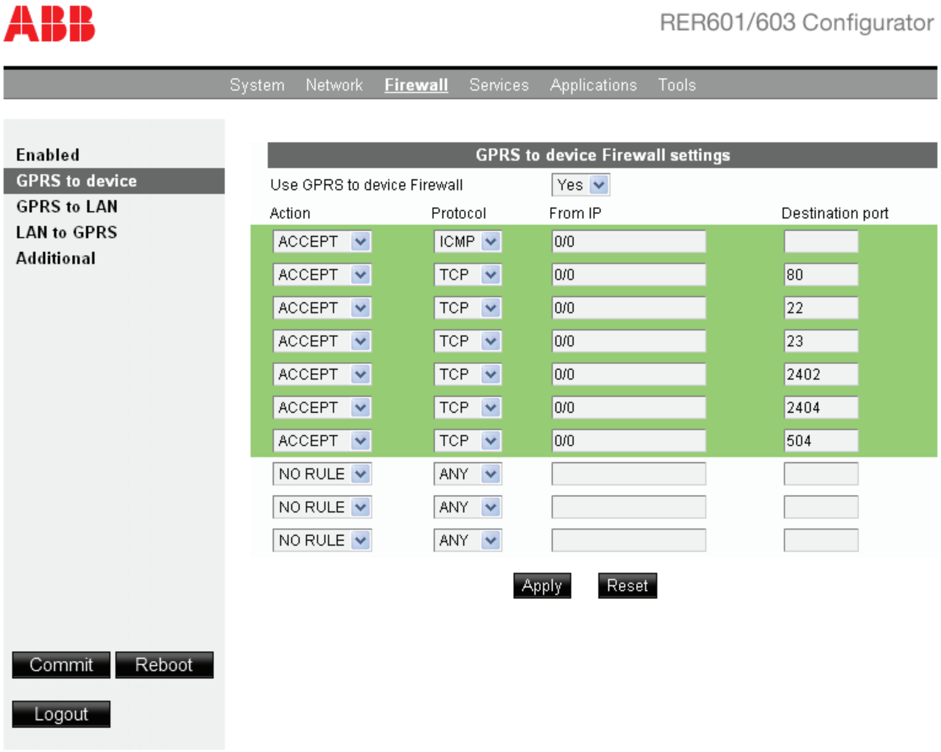
Reply error to unknown commands If set to “No”, incorrect commands are silently disregarded. If set to “Yes“ the device sends an error message via SMS.

Reply error to unauthorized commands If set to “No“ unauthorized commands are silently disregarded. If set to “Yes”, the device sends an error message via SMS.

Factory reset command (8 chars min) resets the device to the factory settings. Does not require a system password. After an SMS command is sent, the factory settings are applied. The password is also set back to the factory default.

5.5 Firewall menu

The Firewall menu is used to configure the device's built-in firewall. The firewall can be disabled or enabled and separate rules may be created for the GPRS to the device, GRPS to the LAN, and LAN to the GPRS configurations.



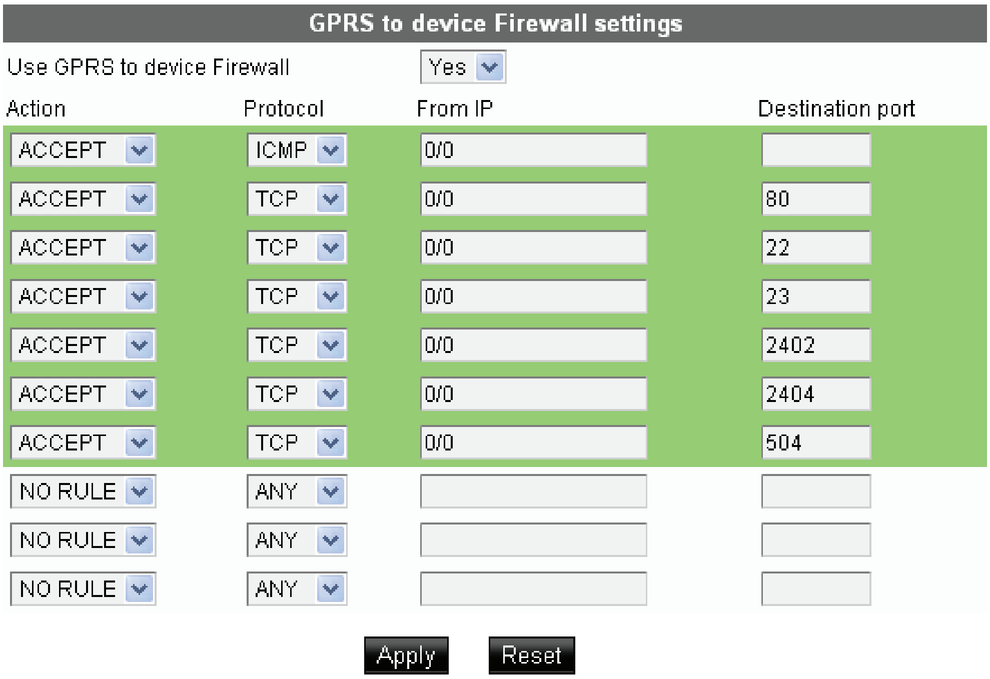
GPRS to device Firewall settings

Use GPRS to device Firewall: Yes

Action	Protocol	From IP	Destination port
ACCEPT	ICMP	0/0	
ACCEPT	TCP	0/0	80
ACCEPT	TCP	0/0	22
ACCEPT	TCP	0/0	23
ACCEPT	TCP	0/0	2402
ACCEPT	TCP	0/0	2404
ACCEPT	TCP	0/0	504
NO RULE	ANY		
NO RULE	ANY		
NO RULE	ANY		

Figure 24: GPRS to device firewall settings

The firewall rules are processed from top to bottom. If strict rules are wanted, the last rule should be DROP. The parameter *From IP* can be used to limit access based on the IP address. For example, “192.168.100.0/24” would limit access to packets coming from the 192.168.100.0 network only.



GPRS to device Firewall settings

Use GPRS to device Firewall: Yes

Action	Protocol	From IP	Destination port
ACCEPT	ICMP	0/0	
ACCEPT	TCP	0/0	80
ACCEPT	TCP	0/0	22
ACCEPT	TCP	0/0	23
ACCEPT	TCP	0/0	2402
ACCEPT	TCP	0/0	2404
ACCEPT	TCP	0/0	504
NO RULE	ANY		
NO RULE	ANY		
NO RULE	ANY		

Figure 25: Example rules of the GPRS settings

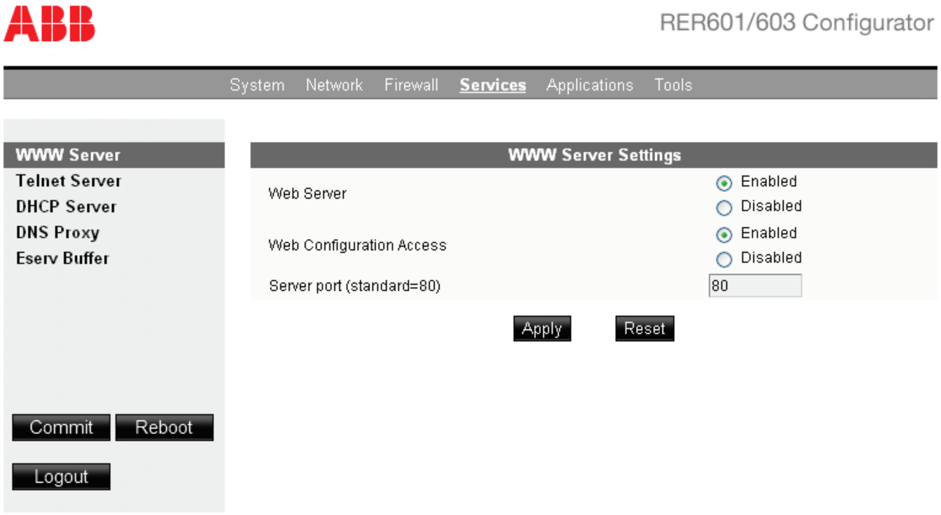
These example rules would allow incoming connection to the GPRS interface: ICMP, Web (TCP port 80) and Telnet (TCP port 22) from any IP access.

5.6 Service menu

The Service menu contains the settings for the WWW, SSH, Telnet and DHCP servers.

5.6.1 WWW

These settings are used to enable or disable the WWW server.



WWW Server Settings

Web Server ● Enabled ○ Disabled

Web Configuration Access ● Enabled ○ Disabled

Server port (standard=80) 80

Figure 26: WWW server settings

Web Server enables or disables the WWW server.

Web Configuration Access enables or disables the Web configuration access.

If the Web access settings are disabled, the Web configurator stops functioning and it must be enabled via the console.

5.6.2 SSH

The SSH server is available in the device for secure connections. The configuration file is located at `/etc/sshd_config`. It can be edited manually.

SSH Server enables or disables the SSH server.

5.6.3 Telnet

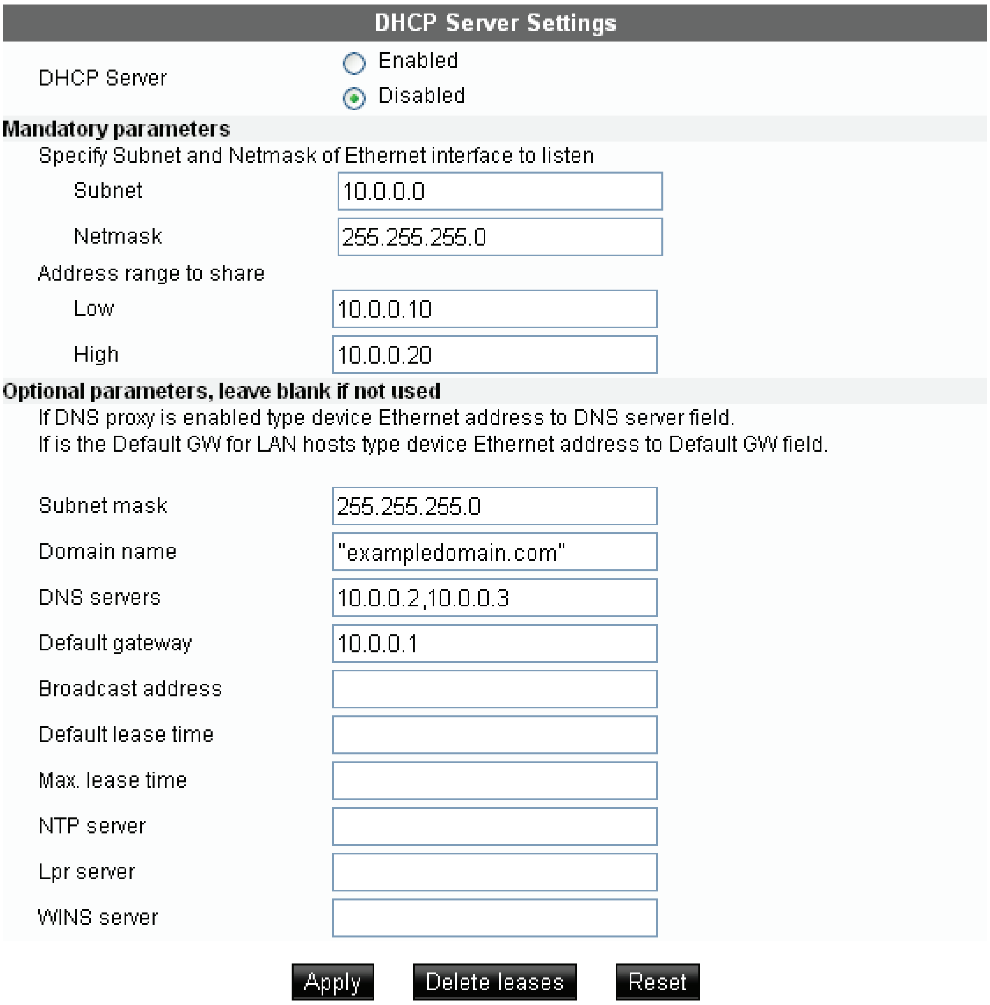
A Telnet server can be used to make terminal connections to the device shell. A more secure way of performing remote management is based on the SSH.

Telnet server enables or disables the Telnet server.

5.6.4 DHCP

The DHCP server listens to broadcast DHCP queries and assigns an IP address for the host from the configured pool. If needed, the device can act as a DHCP server. This is suitable for small remote networks that have, for example, few laptops connected to the device via an Ethernet hub or a switch.

Configuring the DHCP server in an erroneous way may cause the network to function badly or may prevent functioning altogether. Consult the network administrator for the necessary information before setting up the service.



DHCP Server Settings

DHCP Server ○ Enabled ● Disabled

Mandatory parameters

Specify Subnet and Netmask of Ethernet interface to listen

Subnet	10.0.0.0
Netmask	255.255.255.0

Address range to share

Low	10.0.0.10
High	10.0.0.20

Optional parameters, leave blank if not used

If DNS proxy is enabled type device Ethernet address to DNS server field.
If is the Default GW for LAN hosts type device Ethernet address to Default GW field.

Subnet mask	255.255.255.0
Domain name	"exampledomain.com"
DNS servers	10.0.0.2,10.0.0.3
Default gateway	10.0.0.1
Broadcast address	
Default lease time	
Max. lease time	
NTP server	
Lpr server	
WINS server	

Figure 27: DHCP Server settings

DNS Proxy enables computers connected to the device's Ethernet interface to use the device as a DNS server. The device forwards DNS queries to the correct DSN server and there is no need to change the local computer's DNS settings. This can be used with the GPRS settings (**Network/GPRS**) parameter *DNS servers: From GPRS network*.

DNS Proxy/Forwarder enables the use of the device as a DNS server for local computers.

SNMP Agent enables the use of the SNMP Agent. The device supports the MIB-II SNMP Agent.

SNMP agent (SNMP Set/Get) enables or disables the SNMP agent.

Read only SNMP community determines that the community string is read-only.

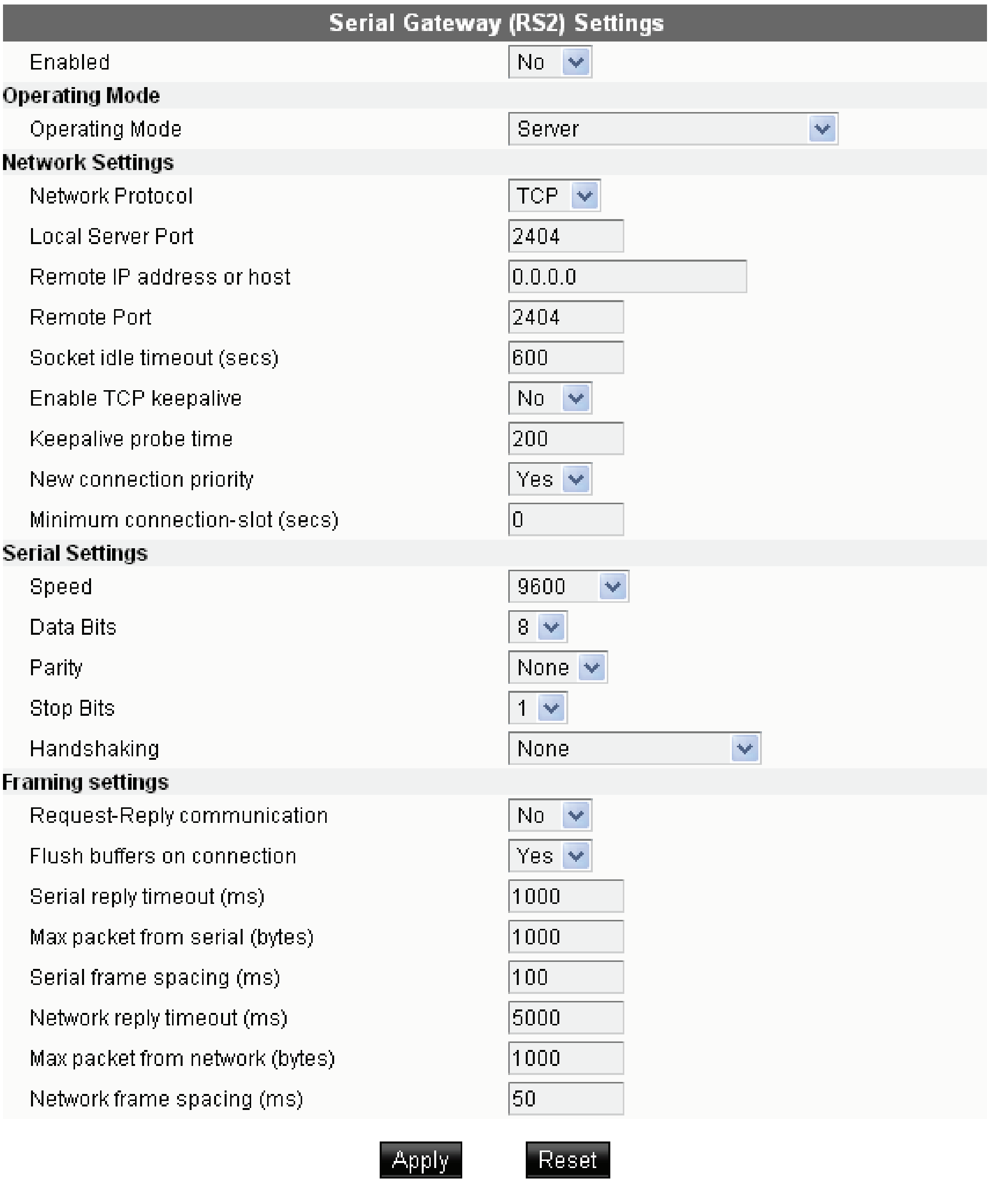
Read and write SNMP community determines that both read and write properties are enabled for the community string.

Server port (standard=161) determines the SNMP Agent listening port (UDP).

Bind to interface determines that the interface is used as a source address.

5.7 Application menu

The Application menu contains the serial device server application. With this application, serial devices can be connected to the gateway and used over the TCP/IP network.



Serial Gateway (RS2) Settings

Enabled	No
Operating Mode	
Operating Mode	Server
Network Settings	
Network Protocol	TCP
Local Server Port	2404
Remote IP address or host	0.0.0.0
Remote Port	2404
Socket idle timeout (secs)	600
Enable TCP keepalive	No
Keepalive probe time	200
New connection priority	Yes
Minimum connection-slot (secs)	0
Serial Settings	
Speed	9600
Data Bits	8
Parity	None
Stop Bits	1
Handshaking	None
Framing settings	
Request-Reply communication	No
Flush buffers on connection	Yes
Serial reply timeout (ms)	1000
Max packet from serial (bytes)	1000
Serial frame spacing (ms)	100
Network reply timeout (ms)	5000
Max packet from network (bytes)	1000
Network frame spacing (ms)	50

Figure 28: Serial Gateway settings

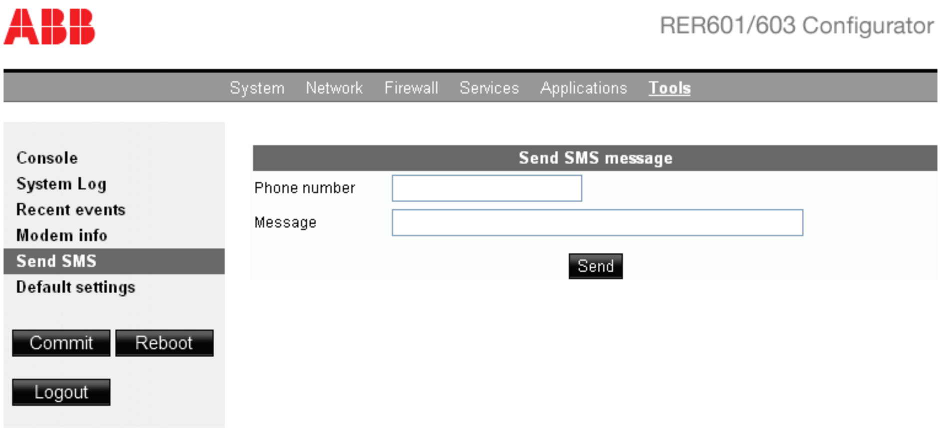
The serial gateway can be enabled from the Serial GW menu. When enabled with the *Server* operating mode, TCP/IP or UDP connections can be made to the device's local server port. In the *Client* operation mode, the gateway sends the received serial data via TCP/IP to the host (remote IP address or host) or to the remote host (remote port).

The IEC 60870-5-104 serial device can be connected to the RS1 or RS2 port. The RS2 serial port can be used either as an RS-232 or an RS-485 type port (IEC 60870-5-104). To enable the serial gateway on the console RS1 port, the console switch has to be set to “0”.

For example, in the *Server* operating mode a device connected to a gateway application serial port can be accessed with Telnet using `telnet<device IP address>2404`.

5.8 Tools menu

The Tools menu gives access to Web-based tools used for troubleshooting the device. It is possible to execute simple shell commands through the WHMI.



Send SMS message

Phone number

Message

Figure 29: Tools menu

Console

The console settings can be used for running commands over the WHMI.

Example commands

```
ping –c 10 172.30.30.1
```

```
firmware
```

System Log and Recent events

The device's system log can be viewed as a system log and a recent events log. When support for the device is needed, for example in a fault situation, the log files can be copy-pasted from the system log.

Modem info

Displays information about the GPRS and GSM status. Also the signal strength is shown here. This can be used to solve GPRS connection problems on site.

Send SMS

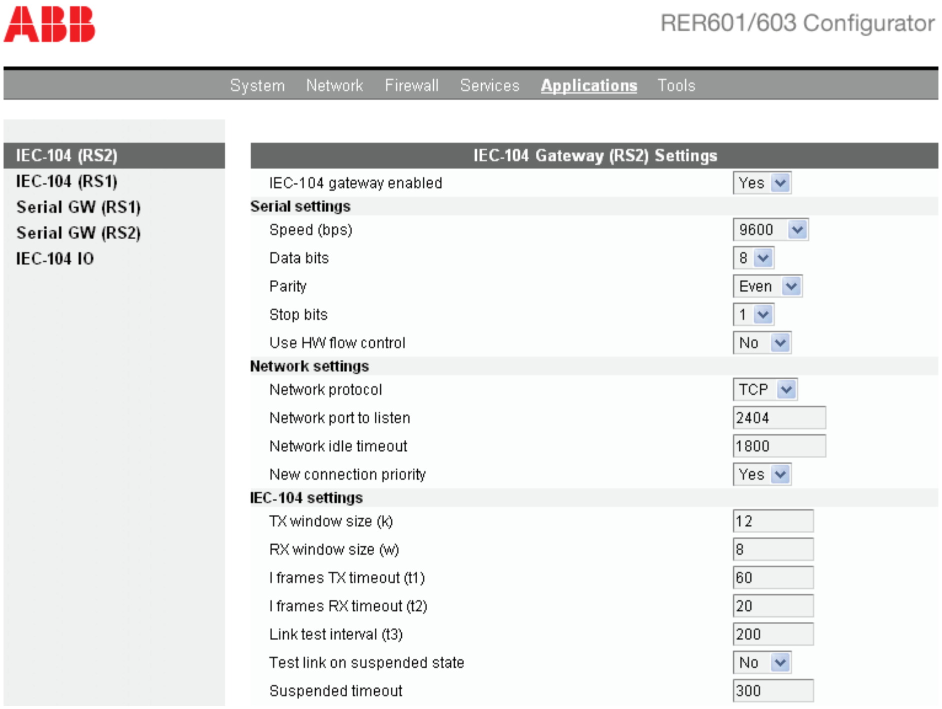
The device can be used for sending test SMS messages. This is useful, for example, for checking the phone number of the current SIM card.

Default settings

The device can be reset to the factory default settings. When resetting to the factory settings, the network settings are excluded.

5.9 IEC-104 application settings

The IEC 60870-5-104 and IEC 60870-5-101 protocols share the same ASDU level messaging but differ on the link level. IEC 60870-5-104 is intended for packet-switched TCP/IP communication and IEC 60870-5-101 for serial communication. By using the device's IEC 60870-5-104 gateway, the IEC 60870-5-101 slaves, for example, RTUs, can be connected to an IEC 60870-5-104 master (for example, SCADA). The device requests events from the IEC 60870-5-101 slave locally and sends them to the IEC 60870-5-104 master. This eliminates the need to continuously poll the data remotely and also reduces the communication costs on a pay-per-use GPRS network. This approach also eliminates the IEC 60870-5-101 parameter problems caused by variable round-trip delays on the GPRS network and makes the information exchange faster and more reliable.



IEC-104 Gateway (RS2) Settings	
IEC-104 gateway enabled	Yes
Serial settings	
Speed (bps)	9600
Data bits	8
Parity	Even
Stop bits	1
Use HW flow control	No
Network settings	
Network protocol	TCP
Network port to listen	2404
Network idle timeout	1800
New connection priority	Yes
IEC-104 settings	
TX window size (k)	12
RX window size (w)	8
I frames TX timeout (t1)	60
I frames RX timeout (t2)	20
Link test interval (t3)	200
Test link on suspended state	No
Suspended timeout	300

Figure 30: IEC-104 Application Settings

5.9.1 General settings

IEC-104 gateway enabled enables or disables the IEC 60870-5-104 to IEC 60870-5-101 gateway.

Table 7: IEC-104 gateway enabled

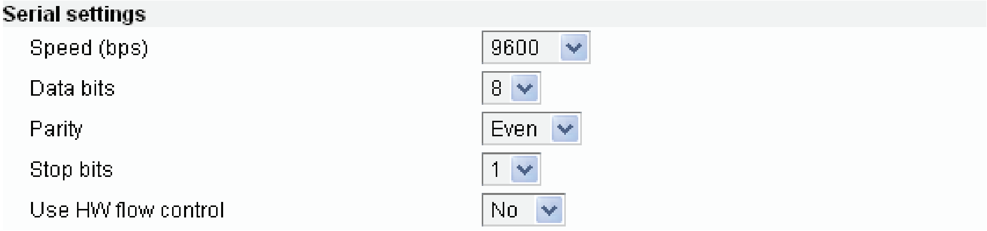
Description	Value
Type	Boolean
Units	N/A
Value range	No, Yes
Note	-

5.9.2 Serial settings

The serial settings define the physical serial communication properties between the device and an IEC 60870-5-101 slave. The selection between RS-232, RS-422 and RS-485 is made with the DIP switches located below the RS2 serial port.

The IEC-101 devices can be connected to the serial ports RS1 or RS2 (single device per port). When the serial port RS1 is used, the console switch below the RS1 should be in the “Data” position.

The settings for the IEC-104 gateway applications are available on WEB user interface applications IEC-104 (RS1) and IEC-104 (RS2).



Serial settings

Speed (bps)	9600
Data bits	8
Parity	Even
Stop bits	1
Use HW flow control	No

Figure 31: Serial settings

Speed (bps) defines the IEC 60870-5-101 serial communication speed (bps).

Table 8: IEC 60870-5-101 serial communication speed (bps)

Description	Value
Type	Serial speed
Units	Bits per second
Value range	1200, 2400, 4800, 9600, 19200, 38400, 57600
Note	-

Data bits defines the number of data bits used in the IEC-101 serial communication.

Table 9: Number of data bits used in the IEC 60870-5-101 serial communication

Description	Value
Type	Serial data bits
Units	Bits
Value range	5, 6, 7, 8
Note	-

Parity defines the parity method used in the IEC 60870-5-101 serial communication.

Table 10: Parity method used in the IEC 60870-5-101 serial communication

Description	Value
Type	Serial data parity
Units	Bits
Value range	None, Even, Odd
Note	-

Stop bits defines the number of stop bits used in the IEC 60870-5-101 serial communication.

Table 11: Number of stop bits used in the IEC 60870-5-101 serial communication

Description	Value
Type	Serial data stop bits
Units	Bits
Value range	1, 2
Note	-

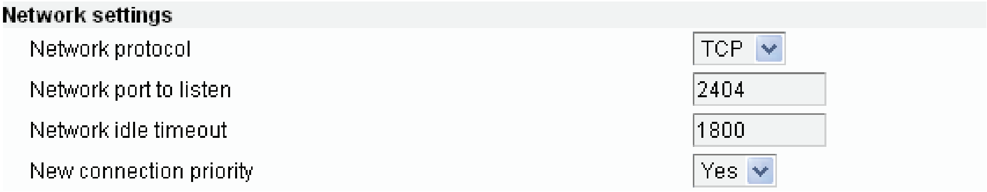
Use HW flow control defines if the HW flow control mechanism is used.

Table 12: HW flow control mechanism (RTS/CTS) in the IEC 60870-5-101 serial communication

Description	Value
Type	Boolean
Units	N/A
Value range	Yes, No
Note	The HW handshaking is available only in the RS-232 mode

5.9.3 Network settings

The Network settings define the general TCP/IP networking properties between the device and the IEC 60870-5-104 master.



Network settings

Network protocol	TCP
Network port to listen	2404
Network idle timeout	1800
New connection priority	Yes

Figure 32: Network settings

Network protocol defines the network transmission layer protocol (either TCP or UDP) used with IEC 60870-5-104 network communication. The IEC 60870-5-104 standard protocol uses TCP, but for reliable slow-speed packet-switched networks the UDP protocol can be used to minimize the packets transmitted over network.

Table 13: Network protocol in IEC 60870-5-104 communication

Description	Value
Type	Network transmission layer protocol
Units	N/A
Value range	UDP, TCP
Note	The IEC 60870-5-104 standard specifies only the TCP protocol

Network port to listen defines the network port to listen for incoming IEC 60870-5-104 connections.

Table 14: TCP or UDP port to listen for incoming IEC 60870-5-104 connections

Description	Value
Type	Network port
Units	Port number
Value range	0...65000
Note	The IEC 60870-5-104 standard specifies TCP port 2404

Network idle timeout defines the idle time-out of the network connection in seconds. If there is no network data received during the specified interval, the device closes the connection. This parameter is required to detect partially closed connections and to release the resources for new connections, especially if the *New connection priority* parameter is disabled. The value “0” disables the network idle time-out detection.

Table 15: Network idle time-out for IEC 60870-5-104 connections

Description	Value
Type	Time-out
Units	Seconds
Value range	0...65000
Note	The network idle time-out must be longer than the IEC 60870-5-104 link test interval (t3)

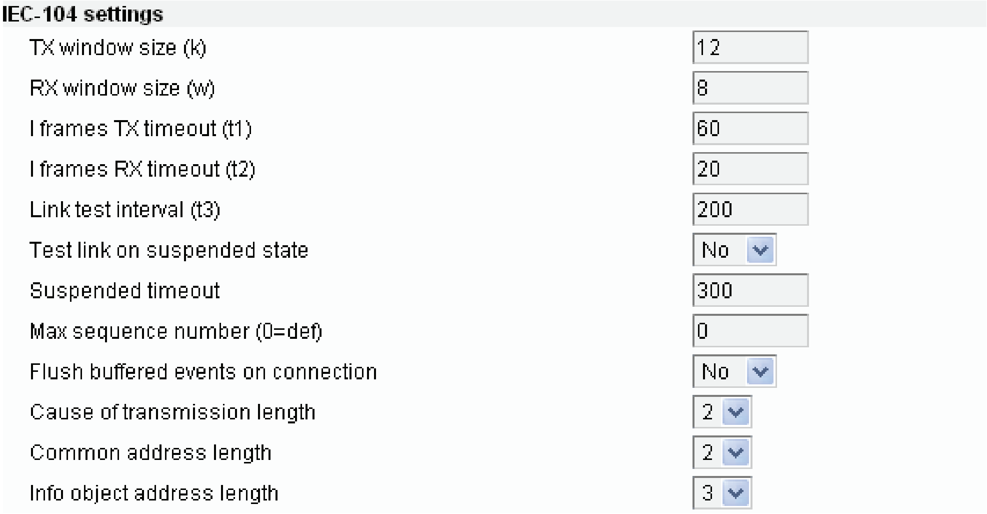
New connection priority defines the action when a new connection request arrives while a connection is already active. If the set value is ”No”, the new connection is rejected. If the set value is ”Yes”, the present connection is terminated and the new connection is accepted.

Table 16: New connection priority for IEC 60870-5-104 connections

Description	Value
Type	Boolean
Units	N/A
Value range	No, Yes
Note	This value must be set to “Yes” in normal configurations with only one IEC 60870-5-104 master

5.9.4 IEC-104 settings

The IEC-104 settings define the properties of the IEC 60870-5-104 link layer and application layer parameters as described in the IEC 60870-5-104 standard. The IEC 60870-5-104 communication is carried out between the device and the IEC 60870-5-104 master over the TCP/IP network.



IEC-104 settings

TX window size (k)	12
RX window size (w)	8
I frames TX timeout (t1)	60
I frames RX timeout (t2)	20
Link test interval (t3)	200
Test link on suspended state	No
Suspended timeout	300
Max sequence number (0=def)	0
Flush buffered events on connection	No
Cause of transmission length	2
Common address length	2
Info object address length	3

Figure 33: IEC-104 Settings

TX window size (k) defines the maximum number of I format APDUs the device may send before requiring the IEC 60870-5-104 master to acknowledge them. If there are unacknowledged “k” size frames sent, the device stops polling the IEC 60870-5-101 slave for events until acknowledgement is received.

Table 17: IEC 60870-5-104 TX window size (k)

Description	Value
Type	Window size
Units	Packets
Value range	1...20
Note	The value “k” must always be less than the maximum sequence number defined below. The IEC 60870-5-104 standard suggests k = 12.

RX window size (w) defines the maximum number of I format APDUs the device may receive before sending an acknowledgement to the IEC 60870-5-104 master.

Table 18: IEC 60870-5-104 RX window size (w)

Description	Value
Type	Window size
Units	Packets
Valule range	1...20
Note	The value “w” should not exceed two-thirds of the TX window size “k”. The IEC 60870-5-104 standard suggests w = 8.

I frames TX timeout (t1) defines the time-out in seconds the device waits for an acknowledgement from the IEC 60870-5-104 master after sending the last I format APDU or a control frame, such as a link test. If no acknowledgement is received during the defined time, the device closes the network connection and the IEC 60870-5-101 link.

Table 19: IEC 60870-5-104 I frames TX time-out (t1)

Description	Value
Type	Timeout
Units	Seconds
Value range	1...255
Note	The value ”t1” must be longer than the network round-trip time. The IEC 60870-5-104 standard suggests t1 = 15 seconds.

I frames RX timeout (t2) defines the time-out in seconds from the last received I format APDU before sending an acknowledgement.

Table 20: IEC 60870-5-104 I frames RX time-out (t2)

Description	Value
Type	Timeout
Units	Seconds
Value range	1...255
Note	The value “t2” must be smaller than “t1”. The IEC 60870-5-104 standard suggests t2 = 10 seconds.

Link test interval (t3) defines the interval in seconds how often the IEC 60870-5-104 link is tested if there is no other activity.

Table 21: IEC 60870-5-104 link test interval (t3)

Description	Value
Type	Timeout
Units	Seconds
Value range	1...65000
Note	This parameter must be adjusted according to the criticality of the link. The IEC 60870-5-104 standard suggests 20 seconds but the practical value may be substantially longer for pay-per-use GPRS connections.

Suspended timeout defines the time in seconds how long a connected IEC 60870-5-104 link can be in the suspended state (STOPD) before the device closes the connection.

Table 22: IEC 60870-5-104 suspended time-out

Description	Value
Type	Timeout
Units	Seconds
Value range	1...65000
Note	Using this parameter makes it easier to detect partially closed network connections, especially in the UDP mode

Max sequence number defines the maximum sequence number used in IEC 60870-5-104 communication. The value “0” selects the standard value “32767”.

Table 23: Max sequence number

Description	Value
Type	Sequence number
Units	Packets
Value range	1...32767
Note	0 = 32767 as suggested by the IEC 60870-5-104 standard

Cause of transmission length defines the length of the IEC 60870-5-104 Cause of transmission ASDU header field in bytes.

Table 24: IEC 60870-5-104 ASDU cause of transmission length

Description	Value
Type	Field length
Units	Bytes
Value range	1...3
Note	The IEC 60870-5-104 standard defines the value "2"

Common address length defines the length of the IEC 60870-5-104 Common address ASDU header field in bytes.

Table 25: IEC 60870-5-104 ASDU common address length

Description	Value
Type	Field length
Units	Bytes
Value range	1...3
Note	The IEC 60870-5-104 standard defines the value "2"

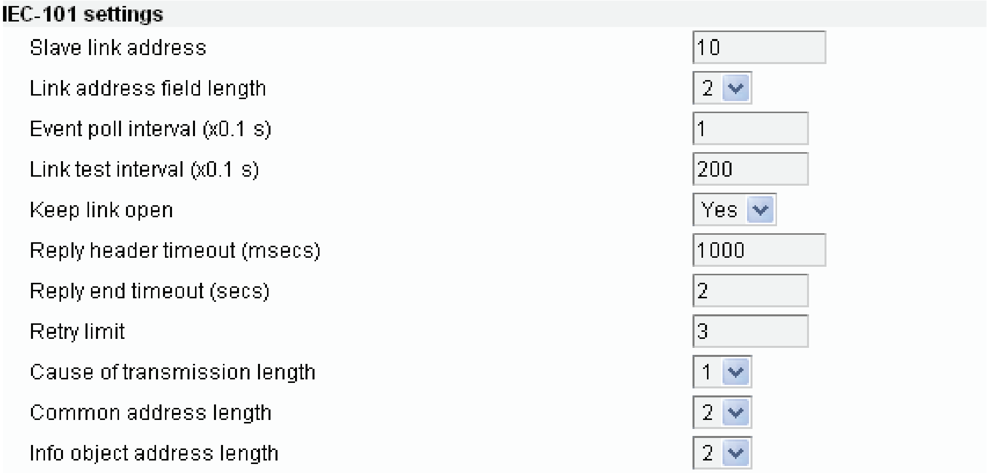
Info object address length defines the length of the IEC 60870-5-104 Information object address ASDU header field in bytes.

Table 26: IEC 60870-5-104 ASDU information object address length

Description	Value
Type	Field length
Units	Bytes
Value range	1...3
Note	The IEC 60870-5-104 standard defines the value "3"

5.9.5 IEC-101 settings

The IEC-101 settings define the properties of the IEC 60870-5-101 link layer and application layer parameters as described in the IEC 60870-5-101 standard. The communication is carried out between the device and the IEC 60870-5-101 slave. Only unbalanced IEC 60870-5-101 communication is supported.



IEC-101 settings

Setting	Value
Slave link address	10
Link address field length	2
Event poll interval (x0.1 s)	1
Link test interval (x0.1 s)	200
Keep link open	Yes
Reply header timeout (msecs)	1000
Reply end timeout (secs)	2
Retry limit	3
Cause of transmission length	1
Common address length	2
Info object address length	2

Figure 34: IEC-101 settings

Slave link address defines the link-level address of the IEC 60870-5-101 slave.

Table 27: IEC 60870-5-101 slave link address

Description	Value
Type	Link address
Units	N/A
Value range	1...65000
Note	The link-level address of the IEC 60870-5-101 slave

Link address field length defines the length of the IEC 60870-5-101 link-level address field in bytes.

Table 28: IEC 60870-5-101 slave link address field length

Description	Value
Type	Field length
Units	Bytes
Value range	1, 2
Note	The link-level address of the IEC 60870-5-101 slave

Event poll interval defines the IEC 60870-5-101 event-polling interval in 0.1-second increments (class 1 or 2 poll).

Table 29: IEC 60870-5-101 event poll interval

Description	Value
Type	Interval
Units	0.1 seconds
Value range	1...65000
Note	The events are polled only when the IEC 60870-5-104 connection is active

Link test interval defines the IEC 60870-5-101 link test interval in 0.1-second increments. The link test is performed if there is no other activity.

Table 30: IEC 60870-5-101 link test interval

Description	Value
Type	Interval
Units	0.1 seconds
Value range	1...65000
Note	The link test is performed if there is no other activity during the defined interval

Keep link open defines that the IEC 60870-5-101 link is always kept open even when there is no active IEC 60870-5-104 connection. If this parameter is enabled, the device sends link test frames and restarts the IEC 60870-5-101 link if the test fails. The events are still not polled before the IEC 60870-5-104 connection is active.

Table 31: IEC 60870-5-101 keep link open

Description	Value
Type	Boolean
Units	N/A
Value range	No, Yes
Note	Some IEC 60870-5-101 slaves require the link to be continuously open to operate

Reply header timeout defines the time-out the device waits for the reply to start from the IEC 60870-5-101 slave after a command or request.

Table 32: IEC 60870-5-101 reply start time-out

Description	Value
Type	Timeout
Units	Milliseconds
Value range	1...65000
Note	-

Reply end timeout defines the maximum duration of the IEC 60870-5-101 slave response.

Table 33: IEC 60870-5-101 reply end time-out

Description	Value
Type	Timeout
Units	Seconds
Value range	1...65000
Note	-

Retry limit defines the number of retries sent to an IEC 60870-5-101 slave in case of no reply. If no reply is received after this limit, the device closes the IEC 60870-5-101 and IEC 60870-5-104 connections.

Table 34: IEC 60870-5-101 retry limit

Description	Value
Type	Retry limit
Units	Retries
Value range	0...65000
Note	-

Cause of transmission length defines the length of the IEC 60870-5-101 Cause of transmission ASDU header field in bytes.

Table 35: IEC 60870-5-101 ASDU cause of transmission length

Description	Value
Type	Field length
Units	Bytes
Value range	1...3
Note	The IEC 60870-5-101 standard defines the value “1”

Common address length defines the length of the IEC 60870-5-101 Common address ASDU header field in bytes.

Table 36: IEC 60870-5-101 ASDU common address length

Description	Value
Type	Field length
Units	Bytes
Value range	1...3
Note	The IEC 60870-5-101 standard defines the value “2”

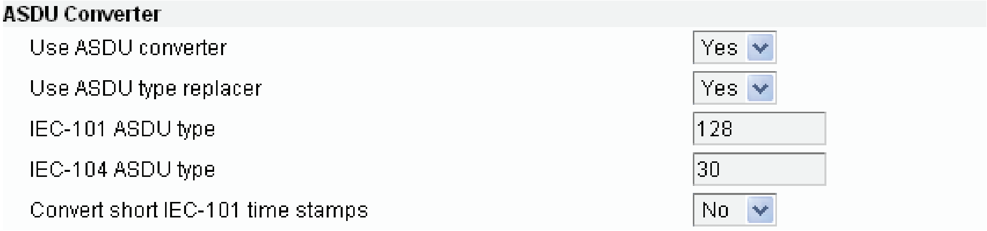
Info object address length defines the length of the IEC 60870-5-101 Information object address ASDU header field in bytes.

Table 37: IEC 60870-5-101 ASDU information object address length

Description	Value
Type	Field length
Units	Bytes
Value range	1...3
Note	The IEC 60870-5-101 standard defines the value “2”

5.9.6 ASDU converter

The ASDU converter can be used to convert the ASDU header field lengths between the IEC 60870-5-101 and IEC 60870-5-104 protocols.



ASDU Converter

Use ASDU converter: Yes

Use ASDU type replacer: Yes

IEC-101 ASDU type: 128

IEC-104 ASDU type: 30

Convert short IEC-101 time stamps: No

Figure 35: ASDU Converter

Use ASDU converter defines if the ASDU header field length conversion is in use. This parameter must be enabled if the ASDU header field lengths differ between IEC 60870-5-101 and IEC 60870-5-104.

Table 38: Use ASDU converter

Description	Value
Type	Boolean
Units	N/A
Value range	No, Yes
Note	The information in the field must fit in the shorter one of the two. It is not possible to convert, for example, the value “12000” to a one byte field.

Use ASDU type replacer can be used to convert an ASDU type (original type) to another type (applied type), for example, in cases when the IEC implementation differs between the master and the slaves.

Table 39: Use ASDU type replacer

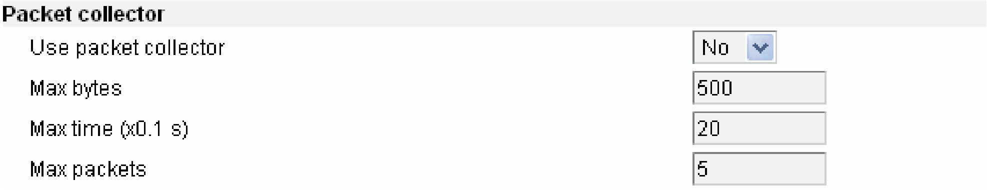
Description	Value
Type	Boolean
Units	N/A
Value range	No, Yes
Note	-

Original type defines the original ASDU type searched by the ASDU type replacer.

Applied type defines the new ASDU that replaces the original type.

5.9.7 Packet collector

The packet collector can be used to collect a number of IEC 60870-5-101 messages or events to a single network packet instead of sending every message separately. This is useful in a slow packet-switched communication network for speeding up the general interrogation response.



Packet collector

Use packet collector: No

Max bytes: 500

Max time (x0.1 s): 20

Max packets: 5

Figure 36: Packet collector

Use packet collector defines if the packet collector is in use.

Table 40: Use packet collector

Description	Value
Type	Boolean
Units	N/A
Value range	No, Yes
Note	-

Max bytes defines the number of maximum bytes for the packet collector. Before a new packet is inserted into the packet collector buffer, the amount of bytes is checked. If the number of bytes in the new packet exceeds the value defined by this parameter, the old content is sent to the network before inserting the new one.

Table 41: Maximum collected bytes

Description	Value
Type	Packet size
Units	Bytes
Value range	1...1500
Note	The value should be smaller than the MTU/MRU of the network used

Max time defines the maximum time collected for the packet collector in 0.1 second increments. If there has been data in the packet collector for longer than the value defined by this parameter, the data is sent to the network.

Table 42: Maximum collected time

Description	Value
Type	Timeout
Units	0.1 seconds
Value range	1...255
Note	The value must be smaller than t1

Max packets defines the maximum amount of IEC 60870-5-101 packets stored into the packet collector before sending the data to the network.

Table 43: Maximum collected packets

Description	Value
Type	Packet count
Units	Packets
Value range	1...255
Note	-

5.9.8 Other settings

Write syslog defines if error messages are stored to the system log file.

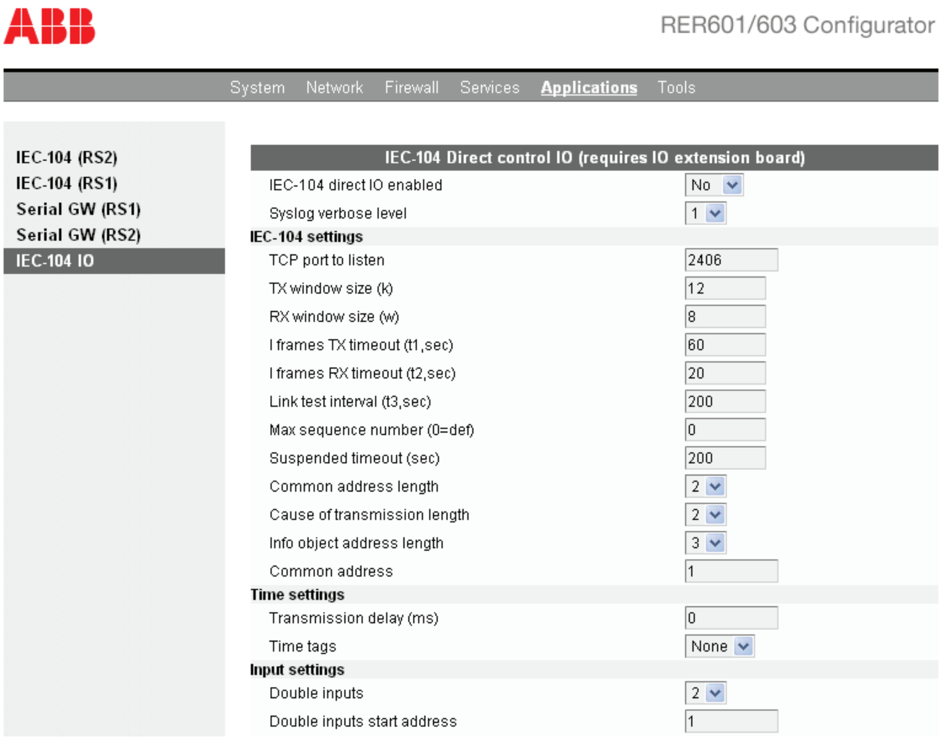
Table 44: Write system log

Description	Value
Type	Boolean
Units	N/A
Value range	No, Yes
Note	The system log is available by using the WHMI

5.10 IEC-104 I/O application settings

These settings can be used to enable or disable the IEC 60870-5-104 direct control I/O.

The I/O extension board (8BI/2BO) is only available in Wireless Gateway RER603.



IEC-104 Direct control IO (requires IO extension board)

IEC-104 direct IO enabled	No
Syslog verbose level	1
IEC-104 settings	
TCP port to listen	2406
TX window size (k)	12
RX window size (w)	8
I frames TX timeout (t1,sec)	60
I frames RX timeout (t2,sec)	20
Link test interval (t3,sec)	200
Max sequence number (0=def)	0
Suspended timeout (sec)	200
Common address length	2
Cause of transmission length	2
Info object address length	3
Common address	1
Time settings	
Transmission delay (ms)	0
Time tags	None
Input settings	
Double inputs	2
Double inputs start address	1

Figure 37: IEC-104 I/O application settings

5.11 Support for remote monitoring

The device has a Patrol client to communicate with Viola Systems M2M server to send communication diagnostics. Viola Patrol is an application within the M2M gateway solution. Patrol functionality offers a graphical user interface for monitoring the remote devices. The Patrol can be used to see the connection quality or locate faults. For more information on configuring the Patrol functionality, see M2M gateway documentation.

Section 6 Troubleshooting

This chapter lists the common problems encountered while installing, configuring or administering the device.

If the problem cannot be resolved, contact the nearest ABB office or representative.

6.1 Setting up the routing mode

When setting up the routing mode "Tunnel the following network", the routing to the M2M Gateway may not work.

- Check that the IP forwarding is enabled
- Check that the internal firewall does not block the packets

6.2 Restoring Ethernet connection

The connection to M2M Gateway Ethernet may not be working.

- Check if the IP forwarding has been enabled in the device.

6.3 Using the M2M Gateway with one public IP

Only one public IP may be available.

- Ensure that the firewall connected to the public IP can forward the incoming SSH connections to the M2M Gateway to be able to use the gateway with only one public IP.

6.4 Receiving characters from the console

The console may not receive the characters.

- Disable the hardware and software handshaking from the terminal software like Hyperterm or Minicom.

6.5 Setting up the GPRS communication

The GPRS interface may be set up but there is no communication.

- Set the default gateway in the Ethernet settings submenu to "0".
- Enable the default gateway from **Network/GPRS** if the GPRS interface is used as a default gateway.

6.6 Establishing GPRS connection

The GPRS connection may not be established.

- Check that the SIM card has the correct PIN number settings and that it has not been locked due to entering the wrong number three times successively.
- Check the PIN status from **Tools/Modem Info**.

6.7 Restoring the GPRS connection

The GPRS connection fails approximately after two minutes if the connection checking has been enabled in **Network/Monitor** but the correct IP has not been set to GPRS in ICMP Echo settings.

- Set the correct IP to GPRS in **Network/GPRS/ICMP Echo**.

Section 7 Technical data

Table 45: Dimensions

Description	Value
Width x Height x Depth	45 x 175 x 108 mm (without antenna)

Table 46: Hardware

Description		Value
Processor environment	Processor	32 bit RISC
	Memory	8 MB FLASH
		32 MB SDRAM
Power	Power supply	6...26 VDC nominal voltage input
	Power consumption	1...5 W
	Fuse	Automatic resettable
	Input protection	ESD
Other	Sensor	Temperature
	Internal clock	Real time
Approvals		CE
Environmental conditions	Temperature ranges	-40...+70 °C (operation)
		-40...+85 °C (transport and storage)
	Relative humidity	5...85 % RH

Table 47: Software

Description	Value
Network protocols	PPP, IP, ICMP, UDP, TCP, ARP, DNS, DHCP, FTP, TFTP, HTTP, POP3, SMTP
Tunneling (VPN)	SSH-VPN client (requires M2M Gateway)
	L2TP-VPN client (requires M2M Gateway)
	SSH client
Management	WWW, SSH, Telnet and console FTP, TFTP and HTTP software update
Routing and firewall	Static routing, proxy ARP, port forwarding, IP masquerading/NAT, firewall

Table continues on next page

Description	Value
Serial device connectivity	Device server application (IEC 60870-5-104 GW)
	Simultaneous GPRS, CSD and SMS
	SMS configuration and status reporting
IEC 60870-5-104 and IEC 60870-5-101	IEC 60870-5-104 over TCP or UDP
	IEC 60870-5-101 FT 1.2 framing
	Local IEC 60870-5-101 polling
	ASDU replacer
	Packet compressor

Table 48: Physical interfaces

Description	Value
I/O interfaces (for Wireless Gateway RER603 only)	8 binary inputs
	2 binary outputs

Table 49: Network interfaces

Description	Value	
Ethernet	10/100 Base-T. Shielded RJ-45	
	1.5 kV isolation transformer	
	Ethernet IEEE 802-3, 802-2	
GPRS	Bandwidth	Quad band (850/900/1800/1900 MHz)
	Module	Internal module and SIM card socket
	Class	Multi-slot class 12
		Mobile station class B
	Downlink speed	Max. 85.6 kbps
	Uplink speed	Max. 85.6 kbps
	Coding schemes	CS1...4
	Antenna connector	FME (50 Ω)
	Security	Via encrypted VPN
CSD (GSM data)	Up to 14.4 kbps	
	V.110	
	Non-transparent mode	
	USSD support	
	FME external antenna connector (50Ω) (Stub antenna included)	

Table continues on next page

Description	Value	
Serial Ports	Serial 1 / Console	RS-232 DTE
		Male DB-9 connector
		IEC 60870-5-101 protocol support
		Full serial and modem signals
		300...460 800 bps.
		Data bits – 7 or 8
		Stop bits - 1 or 2
		Parity - None, Even, Odd
		Flow control – None, RTS/CTS
		Protection – 15 kV ESD and short circuit
		Console – RS-232, 19200 bps, 8 data bits, 1 stop bit, no parity (8N1)
	Serial 2 / IEC 60870-5-101	RS-232 DTE, RS-422, RS-485 (selectable)
		Male DB-9 connector
		Full serial and modem signals
		Biasing and termination selectable
		300...460 800 bps
		Data bits - 7 or 8
		Stop bits - 1 or 2
		Parity - None, Even, Odd
		Flow control – None, RTS/CTS
		Protection – 15 kV ESD and short circuit
		IEC 60870-5-101 protocol support

Table 50: Electromagnetic compatibility tests

Description	Type test value	Reference
Electrostatic discharge test: • Contact discharge • Indirect contact discharge	 4 kV 4 kV	EN 61000-4-2
Conducted RF Immunity test: • 150 kHz...80 MHz	 10 V (rms)	EN 61000-4-6
Table continues on next page		

Description	Type test value	Reference
Radiated RF Immunity test: • 80...1000 MHz • 1400...2000 MHz • 2000...2700 MHz	 10 V/m (rms) 3 V/m (rms) 1V/m (rms)	EN 61000-4-3
Fast transient disturbance tests: • Communication ports • AC power input ports	 1 kV 2 kV	EN 61000-4-4
Surge immunity test: • AC power input ports	 2 kV, line-to-earth 1 kV, line-to-line	EN 61000-4-5
Voltage dips and short interruptions	0 % / 1 cycle 40 % / 10 cycles 70 % / 25 cycles	EN 61000-4-11
Emission tests: • Conducted 0.15...0.50 MHz 0.50...30 MHz • Radiated 30...230 Mhz 230...1000 MHz	 < 79 dB(μV) quasi peak < 66 dB(μV) average < 73 dB(μV) quasi peak < 60 dB(μV) average < 50 dB(μV/m) quasi peak, measured at 3 m distance < 58 dB(μV/m) quasi peak, measured at 3 m distance	CISPR 22 (EN 55022), Class B

Table 51: EMC compliance

Description	Reference
Standard	ETSI EN 301489-1 (V1.8.1 2008-04) IEC 61000-6-1 (Second edition 2005–01) IEC 61000-6-3 (2006–07)

Table 52: RoHS and REACH compliance

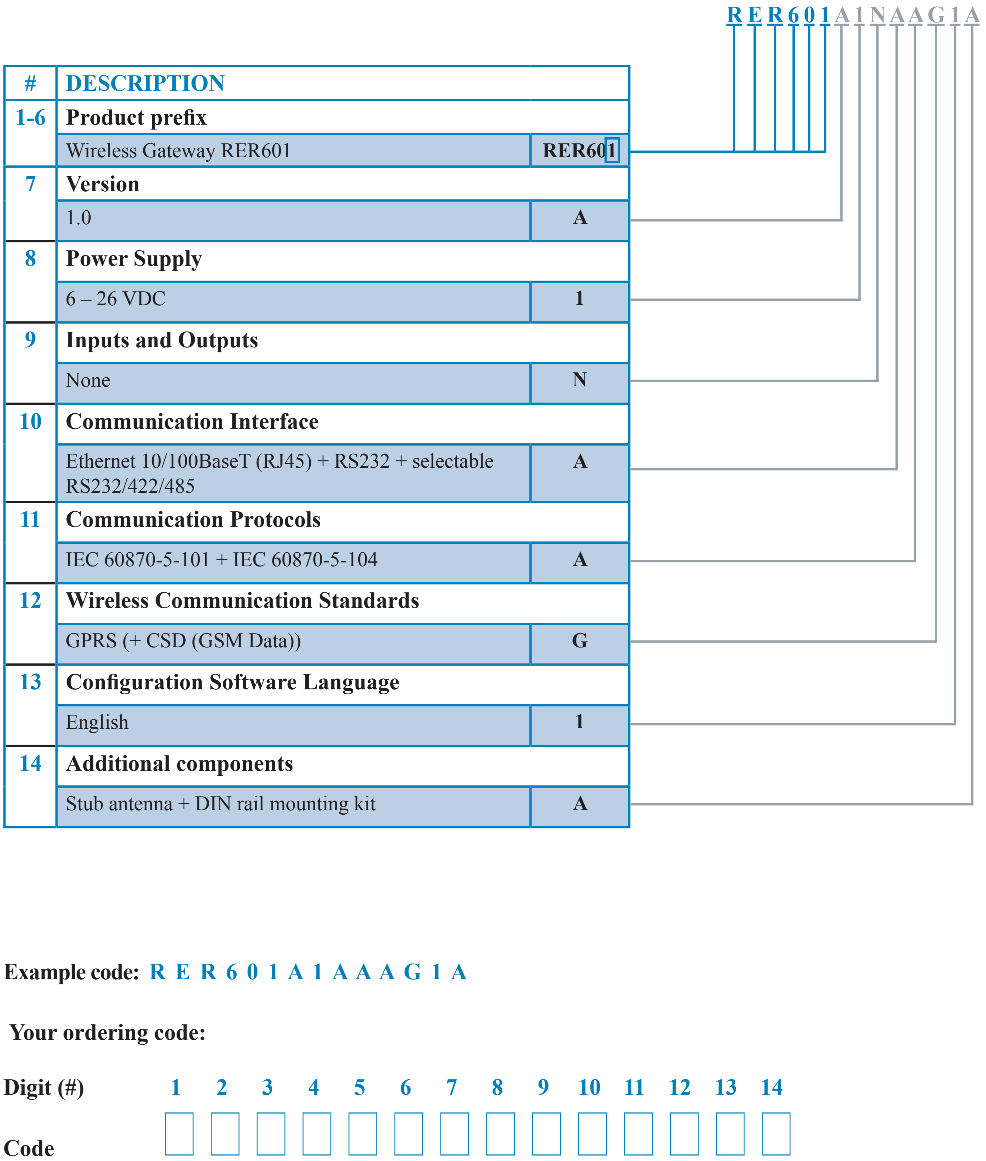
Description
Complies with RoHS directive 2002/95/EC
Complies with REACH directive 2006/1907/EC

Section 8 Ordering data

Product label is found on the bottom of the device and it contains the basic information about the unit such as product name, serial number and Ethernet MAC address.

The order number consists of a string of codes generated from the device’s hardware and software modules. Use the ordering key information to generate the order number when ordering complete devices.

As an example of how the ordering code is generated the following schematics are shown.



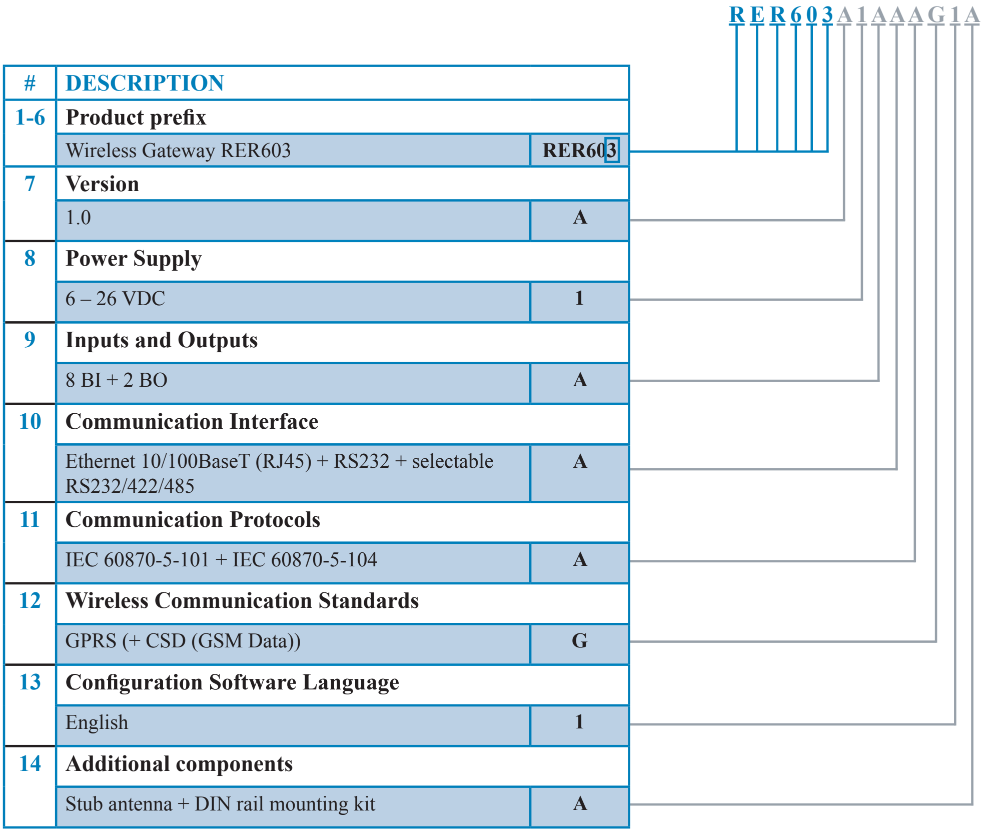
#	DESCRIPTION	
1-6	**Product prefix**	
	Wireless Gateway RER601	**RER601**
7	**Version**	
	1.0	**A**
8	**Power Supply**	
	6 – 26 VDC	**1**
9	**Inputs and Outputs**	
	None	**N**
10	**Communication Interface**	
	Ethernet 10/100BaseT (RJ45) + RS232 + selectable RS232/422/485	**A**
11	**Communication Protocols**	
	IEC 60870-5-101 + IEC 60870-5-104	**A**
12	**Wireless Communication Standards**	
	GPRS (+ CSD (GSM Data))	**G**
13	**Configuration Software Language**	
	English	**1**
14	**Additional components**	
	Stub antenna + DIN rail mounting kit	**A**

Example code: R E R 6 0 1 A 1 A A A G 1 A

Your ordering code:

Digit (#)	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Code	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 38: RER601 ordering code example



#	DESCRIPTION	
1-6	**Product prefix**	
	Wireless Gateway RER603	**RER603**
7	**Version**	
	1.0	**A**
8	**Power Supply**	
	6 – 26 VDC	**1**
9	**Inputs and Outputs**	
	8 BI + 2 BO	**A**
10	**Communication Interface**	
	Ethernet 10/100BaseT (RJ45) + RS232 + selectable RS232/422/485	**A**
11	**Communication Protocols**	
	IEC 60870-5-101 + IEC 60870-5-104	**A**
12	**Wireless Communication Standards**	
	GPRS (+ CSD (GSM Data))	**G**
13	**Configuration Software Language**	
	English	**1**
14	**Additional components**	
	Stub antenna + DIN rail mounting kit	**A**

Example code: R E R 6 0 3 A 1 A A A G 1 A

Your ordering code:

Digit (#)	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Code	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 39: RER603 ordering code example

Section 9 Appendix 1 Installation and mounting instructions

9.1 Unpacking the device

The device is delivered in a package containing the device itself, a short antenna, a connector for power input and an I/O extension connector (only available in RER603). Accessories such as null-modem cables and roof antennas can be ordered separately.

1. Remove the transport packing carefully without force.

   All packaging materials are recyclable. Follow the environmental regulations regarding the disposal of materials.

2. Examine the delivered products to ensure that they were not damaged during the transport. If any of the items is missing or damaged, inform the nearest ABB office or representative. ABB should be notified immediately if there are any discrepancies in relation to the delivery documents.

   Handle the device carefully before installation on site.

9.2 Installing the device

- Install the device horizontally on a flat surface on a desk or on a rack.
- As the device has the GPRS option, consider the high-frequency radio waves it uses for data transmission and choose the installation site accordingly.
  - If the device with antenna is mounted directly to the antenna connector, avoid placing the device where nearby obstacles might disturb the radio signal.
  - In case of metal racks or surfaces, use an external antenna with an appropriate cable.

Walls with metallic structures, such as cabling or concrete iron, may degrade the antenna performance.

- Use mounting tools to mount the device on a wall. Select the optimum mounting direction using the rails on the device's aluminium casing.

The protective earth screw terminal is located next to the DIN-rail mounting clips. The earth lead must always be properly connected, at least 6.0 mm^2 and as short as possible.

9.3 Installing the SIM card

Standard 3 V SIM cards can be used with the device's IEC 60870-5-104 gateway. A SIM card holder is located on the back panel near the GPRS antenna connector.

If the PIN code query is enabled, check that the correct PIN code is entered in the RER601/603 configurator GPRS submenu.

1. Switch off power from the device.
2. Ensure that the GSM module is in the shutdown mode.

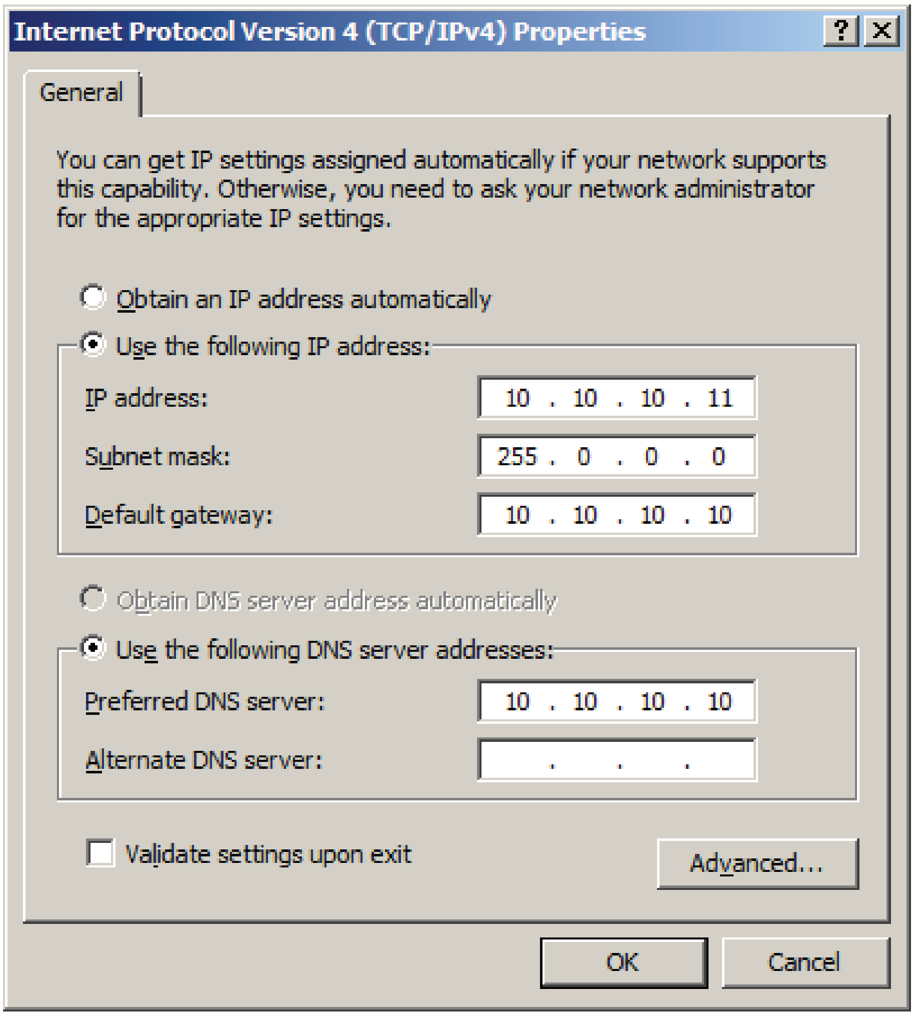
The SIM card holder has a card detection circuit that allows hot insertion and removal of the card. This is not recommended, as the SIM card content may become corrupted if the card is removed while the GSM module is writing data to it.

3. Eject the SIM card holder by pushing the **Eject** button.
4. Remove the tray from the holder and place the SIM card onto the tray.
5. Insert the tray carefully back to the holder and press the tray until it is locked.

9.4 Setting the IP address via a Web browser

1. Connect to the device using the Web browser.

The default IP address is “10.10.10.10” (netmask “255.0.0.0”). A computer connected to the device may use, for example, the IP address “10.10.10.11”.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 11

Subnet mask: 255 . 0 . 0 . 0

Default gateway: 10 . 10 . 10 . 10

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

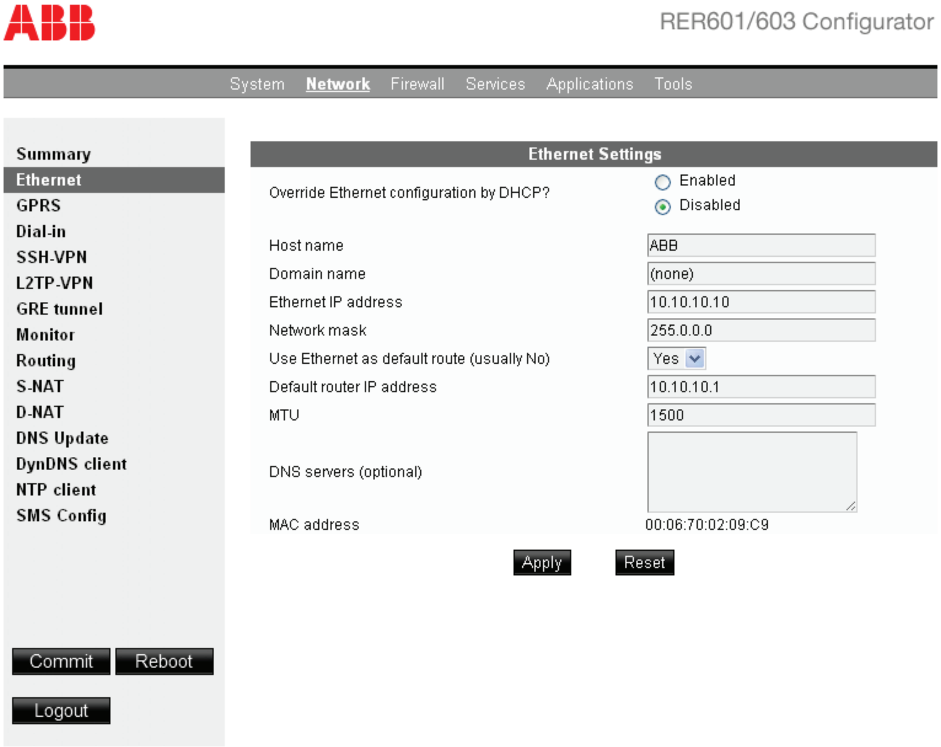
Preferred DNS server: 10 . 10 . 10 . 10

Alternate DNS server: . . .

□ Validate settings upon exit

Figure 40: IP Properties

2. On the start page, click the **Start Configurator** link.
3. Enter the login information.
   - 3.1. Type the user name as “root”.
   - 3.2. Leave the password box empty.
4. Select **Network/Ethernet**.



Ethernet Settings

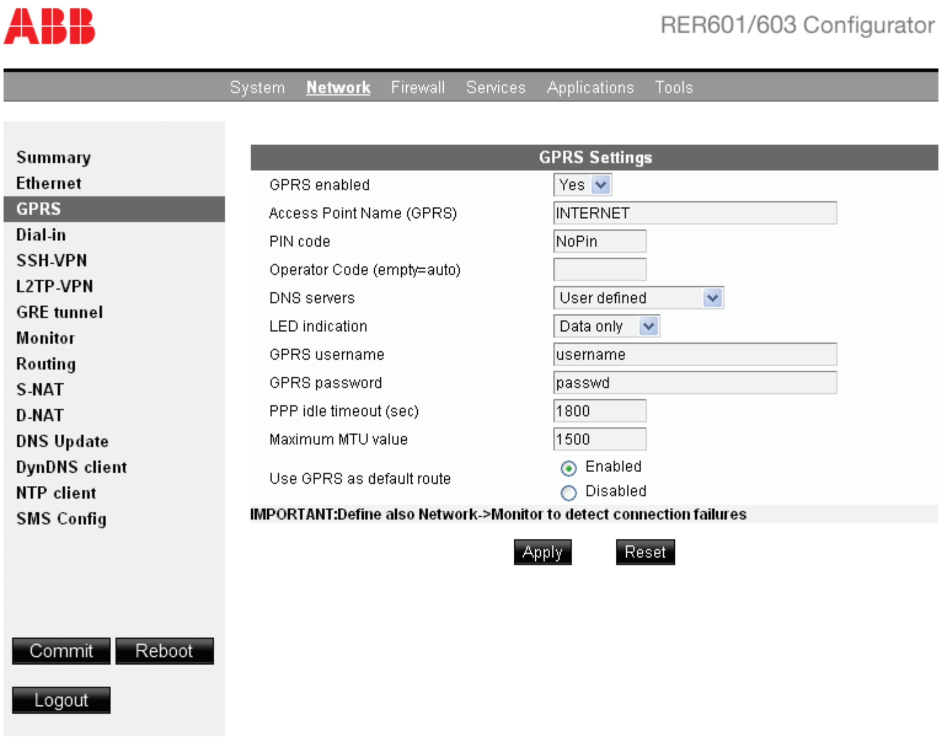
Override Ethernet configuration by DHCP?	○ Enabled ● Disabled
Host name	ABB
Domain name	(none)
Ethernet IP address	10.10.10.10
Network mask	255.0.0.0
Use Ethernet as default route (usually No)	Yes
Default router IP address	10.10.10.1
MTU	1500
DNS servers (optional)	
MAC address	00:06:70:02:09:C9

Figure 41: Ethernet Settings

5. Type the Ethernet IP address and the required network settings in the boxes. Click **Apply** and **Commit** at the bottom of the page to save the settings.
6. Restart the device for the settings to take effect.

The default password is empty. Set the password before connecting the device to a public network.

9.5 Configuring the GPRS settings



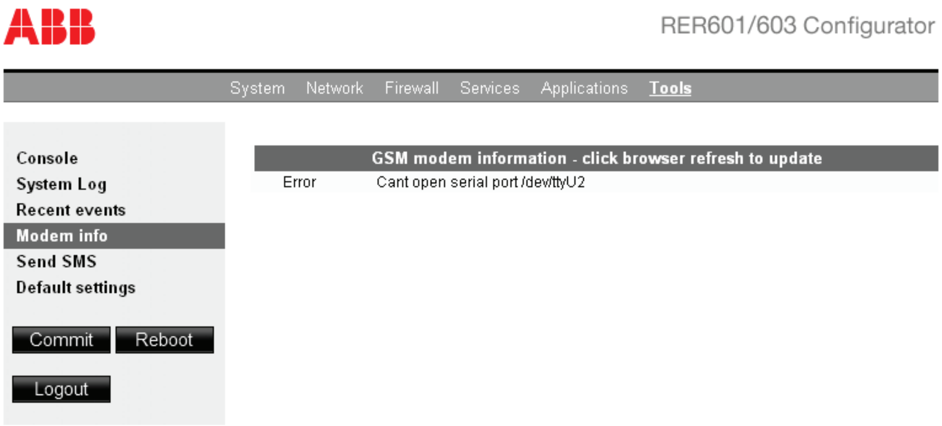
GPRS Settings

GPRS enabled	Yes
Access Point Name (GPRS)	INTERNET
PIN code	NoPin
Operator Code (empty=auto)	
DNS servers	User defined
LED indication	Data only
GPRS username	username
GPRS password	passwd
PPP idle timeout (sec)	1800
Maximum MTU value	1500
Use GPRS as default route	● Enabled ○ Disabled

IMPORTANT:Define also Network->Monitor to detect connection failures

Figure 42: GPRS settings

See **Tools/Modem info** for GSM/GPRS information.



GSM modem information - click browser refresh to update

Error Cant open serial port /dev/ttyU2

Figure 43: GSM modem information

1. If the SIM card has the PIN code querying enabled, configure the PIN code before inserting the card in the card holder.
2. Connect to the device and log in to the RER601/603 configurator.
3. Navigate to **Network/GPRS**.
4. Type the access point name in the **Access Point Name (GPRS)** box. Usually, the access point name is “INTERNET“
5. Set the GPRS network user name and password if the GPRS service requires authentication.
6. Set the default route to “Enabled”.
7. The parameters *PIN code* and *PPP idle timeout (sec)* are optional.
    - If the SIM card has the PIN code set, type the code in the **PIN code** box.

      Set the correct PIN code with the RER601/603 configurator before plugging in the SIM card. If an incorrect PIN code is set and the PIN code is required by the SIM card, the device does not retry with the wrong PIN code, thus avoiding a SIM card lock-up. In such a case, insert the SIM card to a mobile phone and enter the correct PIN code before continuing.

    - **PPP idle timeout (sec)** defines the interval in seconds when the device resets the GPRS connection if the connection is idle.
    - **ICMP Echo** is used to monitor the GPRS connection between the device and the remote host. If the host cannot be reached, the GPRS connection is reset. This feature should always be enabled from **Network/Monitor**.
8. Click **Apply**. After confirmation, click **Commit** to save the settings.
9. Restart the device for the settings to take effect. Check the GPRS status from **Network/Summary**.

Section 10 Appendix 2 IEC 60870-5-104 interoperability

10.1 Interoperability

The document describes the interoperability of the IEC-104 IO application used to control the device internal I/O board signals. This document does not describe the interoperability of the IEC 60870-5-101 to IEC 60870-5-104 gateway application.

This companion standard presents sets of parameters and alternatives from which subsets must be selected to implement particular telecontrol systems. Certain parameter values, such as the choice of “structured“ or “unstructured“ fields of the INFORMATION OBJECT ADDRESS of ASDUs represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturers, it is necessary that all partners agree on the selected parameters.

The interoperability list is defined as in IEC 60870-5-101 and extended with parameters used in this standard. The text descriptions of parameters which are not applicable to this companion standard are strike-through (corresponding check box is marked black).

The full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

The selected parameters should be marked in the white boxes.

□ Function or ASDU is not used

☒ Function or ASDU is used as standardized (default)

R Function or ASDU is used in reverse mode

B Function or ASDU is used in standard and reverse mode

The possible selection (blank, X, R, or B) is specified for each specific clause or parameter.

A black check box indicates that the option cannot be selected in this companion standard.

? Function or ASDU is planned, contact the product management

10.1.1 System or device

(System-specific parameter, select one definition of a system or a device by marking with an “X“.)

□ System definition

□ Controlling station definition (Master)

☒ Controlled station definition (Slave)

10.1.2 Network configuration

(Network-specific parameter, all configurations that are used are to be marked with “X“.)

■ ~~Point-to-point~~

■ ~~Multiple point-to-point~~

■ ~~Multipoint~~

■ ~~Multipoint-star~~

10.1.3 Physical layer

(Network-specific parameter, all interfaces and data rates that are used are to be marked with “X“.)

Transmission speed (control direction)

Unbalanced interchange Circuit V. 24/V.28 Standard	Unbalanced interchange Circuit V. 24/V.28 Recommended if >1200 bit/s	Balanced interchange Circuit X. 24/X.27	
■ ~~100 bit/s~~	■ ~~2400 bit/s~~	■ ~~2400 bit/s~~	■ ~~56000 bit/s~~
■ ~~200 bit/s~~	■ ~~4800 bit/s~~	■ ~~4800 bit/s~~	■ ~~64000 bit/s~~
■ ~~300 bit/s~~	■ ~~9600 bit/s~~	■ ~~9600 bit/s~~	
■ ~~600 bit/s~~		■ ~~19200 bit/s~~	
■ ~~1200 bit/s~~		■ ~~38400 bit/s~~	

Transmission speed (monitor direction)

Unbalanced interchange Circuit V. 24/V.28 Standard	Unbalanced interchange Circuit V. 24/V.28 Recommended if >1 200 bit/s	Balanced interchange Circuit X. 24/X.27	
■ ~~100 bit/s~~	■ ~~2400 bit/s~~	■ ~~2400 bit/s~~	■ ~~56000 bit/s~~
■ ~~200 bit/s~~	■ ~~4800 bit/s~~	■ ~~4800 bit/s~~	■ ~~64000 bit/s~~
■ ~~300 bit/s~~	■ ~~9600 bit/s~~	■ ~~9600 bit/s~~	
■ ~~600 bit/s~~		■ ~~19200 bit/s~~	
■ ~~1200 bit/s~~		■ ~~38400 bit/s~~	

10.1.4 Link layer

(Network-specific parameter, all options that are used are to be marked with “X“). Specify the maximum frame length. If a non-standard assignment of class 2 messages are implemented for unbalanced transmission, indicate the Type ID and COT of all messages assigned to class 2.)

~~Frame format FT 1.2, single character 1 and the fixed time out interval are used exclusively in this companion standard.~~

Link transmission	Address field of the link
■ ~~Balanced transmission~~	■ ~~not present (balanced transmission only)~~
■ ~~Unbalanced transmission~~	■ ~~One octet~~

Table continues on next page

■ ~~Two octets~~

Frame length

■ ~~Maximum length L (number of octets)~~

■ ~~Structured~~

■ ~~Unstructured~~

When using an unbalanced link layer, the following ASDU types are returned in class 2 messages (low priority) with the indicated causes of transmission:

■ ~~The standard assignment of ASDUs to class 2 messages is used as follows:~~

Type identification	Cause of transmission
9, 11, 13, 21	<1>

■ ~~A special assignment of ASDUs to class 2 messages is used as follows:~~

Type identification	Cause of transmission

~~(In response to a class 2 poll, a controlled station may respond with class 1 data when there is no class 2 data available).~~

10.1.5 Application layer

Transmission mode for application data

Mode 1 (Least significant octet first), as defined in 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Common address of ASDU

(System-specific parameter, all configurations that are used are to be marked with “X“.)

☒ One octet

☒ Two octets

Information object address

(System-specific parameter, all configurations that are used are to be marked with “X“).

☒ One octet

☒ Two octets

☒ Three octets

□ Structured

☒ Unstructured

Cause of transmission

(System-specific parameter, all configurations that are used are to be marked with “X“.)

☒ One octet

☒ Two octets (with originator address). Originator address is set to zero if not used

Length of APDU

(System-specific parameter, specify the maximum length of the APDUper system.)

The maximum length of the APDU is 253 (default). The maximum length may be reduced by the system.

253 Maximum length of APDU per system

Selection of standard ASDUs

Process information in monitor direction

(Station-specific parameter, mark each Type ID “X“ if it is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒	<1>:= Single-point information	M_SP_NA_1
☒	<2>:= Single-point information with time tag	M_SP_TA_1
☒	<3>:= Double-point information	M_DP_NA_1
☒	<4>:= Double-point information with time tag	M_DP_TA_1
□	<5>:= Step position information	M_ST_NA_1
■	~~<6>:= Step position information with time tag~~	M_ST_TA_1

Table continues on next page

□	<7>Bitstring of 32 bit	M_BO_NA_1
■	~~<8>:= Bitstring of 32 bit with time tag~~	M_BO_TA_1
□	<9>:= Measured value, normalized value	M_ME_NA_1
■	~~<10>:= Measured value, normalized value with time tag~~	M_ME_TA_1
□	<11>:= Measured value, scaled value	M_ME_NB_1
■	~~<12>:= Measured value, scaled value with time tag~~	M_ME_TB_1
☒	<13>:= Measured value, short floating point value	M_ME_NC_1
■	~~<14> := Measured value, short floating point value with time tag~~	M_ME_TC_1
□	<15>:= Integrated totals	M_IT_NA_1
■	~~<16>:= Integrated totals with time tag~~	M_IT_TA_1
■	~~<17>:= Event of protection equipment with time tag~~	M_EP_TA_1
■	~~<18>:= Packed start events of protection equipment with time tag~~	M_EP_TB_1
■	~~<19>:= Packed output circuit information of protection equipment with time tag~~	M_EP_TC_1
□	<20>:= Packed single-point information with status change detection	M_SP_NA_1
□	<21>:= Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30>:= Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31>:= Double-point information with time tag CP56Time2a	M_DP_TB_1
□	<32>:= Step position information with time tag CP56Time2a	M_ST_TB_1
□	<33>:= Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
□	<34>:= Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
□	<35>:= Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
□	<36>:= Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
□	<37>:= Integrated totals with time tag CP56Time2a	M_IT_TB_1
□	<38>:= Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
□	<39>:= Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
□	<40>:= Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

Either the ASDUs of the set <2>, <4>, <6>, <8>, <10>, <12>, <14>, <16>, <17>, <18>, <19> or of the set <30> – <40> are used.

Process information in control direction

(Station-specific parameter, mark each Type ID “X“ if it is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒	<45>:= Single command	C_SC_NA_1
☒	<46>:= Double command	C_DC_NA_1
□	<47>:= Regulating step command	C_RC_NA_1
□	<48>:= Set point command, normalized value	C_SE_NA_1
□	<49>:= Set point command, scaled value	C_SE_NB_1
□	<50>:= Set point command, short floating point value	C_SE_NC_1
□	<51> := Bitstring of 32 bit	C_BO_NA_1
□	<58> := Single command with time tag CP56Time2a	C_SC_TA_1
□	<59>:= Double command with time tag CP56Time2a	C_DC_TA_1
□	<60>:= Regulating step command with time tag CP56Time2a	C_RC_TA_1
□	<61>:= Set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
□	<62>:= Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
□	<63> := Set point command, short floating point value with time tag CP56Time2a	C_SE_TC_1
□	<64> := Bitstring of 32 bit with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set <45> – <51> or of the set <58> – <64> are used.

System information in monitor direction

(Station-specific parameter, mark with “X" if used.)

☒	<70> := End of initialization	M_EI_NA_1

System information in control direction

(Station-specific parameter, mark each Type ID “X“ if it is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒	<100>:= Interrogation command	C_IC_NA_1
□	<101>:= Counter interrogation command	C_CI_NA_1
☒	<102>:= Read command	C_RD_NA_1
☒	<103>:= Clock synchronization command (option see 7.6)	C_CS_NA_1
☒	<104>:= Clock synchronization command (option see 7.6)	C_TS_NA_1
☒	<105>:= Reset process command	C_RP_NA_1
■	~~<106>:= Delay acquisition command~~	C_CD_NA_1
☒	<107>:= Test command with time tag CP56Time2a	C_TS_TA_1

Parameter in control direction

(Station-specific parameter, mark each Type ID “X“ if it is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

□	<110>:= Parameter of measured value, normalized value	P_ME_NA_1
□	<111>:= Parameter of measured value, scaled value	P_ME_NB_1
□	<112>:= Parameter of measured value, short floating point value	P_ME_NC_1
□	<113>:= Parameter activation	P_AC_NA_1

File transfer

(Station-specific parameter, mark each Type ID “X“ if it is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

□	<120>:= File ready	F_FR_NA_1
□	<121>:= Section ready	F_SR_NA_1
□	<122>:= Call directory, select file, call file, call section	F_SC_NA_1
□	<123>:= Last section, last segment	F_LS_NA_1
□	<124>:= Ack file, ack section	F_AF_NA_1
□	<125>:= Segment	F_SG_NA_1
□	<126>:= Directory {blank or X, only available in monitor (standard) direction}	F_DR_TA_1

Type identifier and cause of transmission assignments

(Station-specific parameters.)

Shaded boxes: option not required.

Black boxes: option not permitted in this companion standard

Blank: functions or ASDU not used.

Mark the Type Identification/Cause of transmission combinations.

“X“ if only used in the standard direction

“R“ if only used in the reverse direction

“B“ if used in both directions

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1	▨		X	▨		▨	▨	▨	▨	▨	X		▨	X	▨	▨	▨	▨	▨
<2>	M_SP_TA_1	▨	▨	X	▨	■	▨	▨	▨	▨	▨		■	▨	▨	▨	▨	▨	▨	▨
<3>	M_DP_NA_1	▨		X	▨		▨	▨	▨	▨	▨	X		▨	X	▨	▨	▨	▨	▨
<4>	M_DP_TA_1	▨	▨	X	▨	■	▨	▨	▨	▨	▨	■	■	▨	▨	▨	▨	▨	▨	▨
<5>	M_ST_NA_1	▨			▨		▨	▨	▨	▨	▨			▨		▨	▨	▨	▨	▨
~~<6>~~	~~M_ST_TA_1~~	▨	▨	■	▨	■	▨	▨	▨	▨	▨	■	■	▨	▨	▨	▨	▨	▨	▨
<7>	M_BO_NA_1	▨			▨		▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨	▨
~~<8>~~	~~M_BO_TA_1~~	▨	▨	■	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<9>	M_ME_NA_1				▨		▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨	▨
~~<10>~~	~~M_ME_TA_1~~	▨	▨	■	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<11>	M_ME_NB_1				▨		▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨	▨
~~<12>~~	~~M_ME_TB_1~~	▨	▨	■	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<13>	M_ME_NC_1				▨		▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨	▨
~~<14>~~	~~M_ME_TC_1~~	▨	▨	■	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<15>	M_IT_NA_1	▨	▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨
~~<16>~~	~~M_IT_TA_1~~	▨	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	■	▨	▨	▨	▨
~~<17>~~	~~M_EP_TA_1~~	▨	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
~~<18>~~	~~M_EP_TB_1~~	▨	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
~~<19>~~	~~M_EP_TC_1~~	▨	▨	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<20>	M_PS_NA_1	▨			▨		▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨	▨
<21>	M_ME_ND_1				▨		▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨	▨
<30>	M_SP_TB_1	▨	▨	X	▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<31>	M_DP_TB_1	▨	▨	X	▨		▨	▨	▨	▨	▨			▨	▨	▨	▨	▨	▨	▨
<32>	M_ST_TB_1	▨	▨		▨		▨	▨	▨	▨	▨			▨	▨	▨	▨	▨	▨	▨

Table continues on next page

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<33>	M_BO_TB_1	▨	▨		▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<34>	M_ME_TD_1	▨	▨		▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<35>	M_ME_TE_1	▨	▨		▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<36>	M_ME_TF_1	▨	▨		▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<37>	M_IT_TB_1	▨	▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨
<38>	M_EP_TD_1	▨	▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<39>	M_EP_TE_1	▨	▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<40>	M_EP_TF_1	▨	▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<45>	C_SC_NA_1	▨	▨	▨	▨	▨	X	X	X	X	X	▨	▨	▨	▨	▨				
<46>	C_DC_NA_1	▨	▨	▨	▨	▨	X	X	X	X	X	▨	▨	▨	▨	▨				
<47>	C_RC_NA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<48>	C_SE_NA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<49>	C_SE_NB_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<50>	C_SE_NC_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<51>	C_BO_NA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<58>	C_SC_TA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<59>	C_DC_TA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<60>	C_RC_TA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<61>	C_SE_TA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<62>	C_SE_TB_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<63>	C_SE_TC_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<64>	C_BO_TA_1	▨	▨	▨	▨	▨						▨	▨	▨	▨	▨				
<70>	M_EI_NA_1*	▨	▨	▨	X	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
<100>	C_IC_NA_1	▨	▨	▨	▨	▨	X	X			X									
<101>	C_CI_NA_1	▨	▨	▨	▨	▨			▨	▨		▨	▨	▨	▨	▨				
<102>	C_RD_NA_1	▨	▨	▨	▨	X	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨				
<103>	C_CS_NA_1	▨	▨		▨	▨	X	X	▨	▨	▨	▨	▨	▨	▨	▨				
<104>	C_TS_NA_1	▨	▨	▨	▨	▨	X	X	▨	▨	▨	▨	▨	▨	▨	▨	■	■	■	■
<105>	C_RP_NA_1	▨	▨	▨	▨	▨	X	X	▨	▨	▨	▨	▨	▨	▨	▨				
~~<106>~~	~~C_CD_NA_1~~	▨	▨	■	▨	▨	■	■	▨	▨	▨	▨	▨	▨	▨	▨	■	■	■	■
<107>	C_TS_TA_1	▨	▨	▨	▨	▨			▨	▨	▨	▨	▨	▨	▨	▨				
<110>	P_ME_NA_1	▨	▨	▨	▨	▨			▨	▨	▨	▨	▨	▨		▨				
<111>	P_ME_NB_1	▨	▨	▨	▨	▨			▨	▨	▨	▨	▨	▨		▨				
<112>	P_ME_NC_1	▨	▨	▨	▨	▨			▨	▨	▨	▨	▨	▨		▨				
<113>	P_AC_NA_1	▨	▨	▨	▨	▨					▨	▨	▨	▨	▨	▨				
<120>	F_FR_NA_1	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨				
<121>	F_SR_NA_1	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨				
<122>	F_SC_NA_1	▨	▨	▨	▨		▨	▨	▨	▨	▨	▨	▨		▨	▨				

Table continues on next page

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<123>	F_LS_NA_1	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨				
<124>	F_AF_NA_1	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨				
<125>	F_SG_NA_1	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨				
<126>	F_DR_TA_1*	▨	▨		▨		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
* Blank or X only																				

10.1.6 Basic application functions

Station initialization

(Station-specific parameter, mark with an “X“ if the function is used.)

☒ Remote initialization

Cyclic data transmission

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒ Cyclic data transmission

Read procedure

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

□ Read procedure

Spontaneous transmission

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒ Spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous

(Station-specific parameter, mark each information type with an “X“ where both a Type ID without time and a corresponding Type ID with time are issued in response to a single spontaneous change of a monitored object.)

The following type identifications may be transmitted in succession caused by a single status change of an information object. The particular information object addresses for which double transmission is enabled are defined in a project-specific list.

☒ Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1

☒ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1

□ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1

□ Bitstring of 32 bit M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1 (if defined for a specific project)

□ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1

□ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1

☒ Measured value, short floating point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

Station interrogation

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒ global

☒ group 1

■ group 2

☒ group 3

☒ group 4

☒ group 5

☒ group 6

☒ group 7

☒ group 8

☒ group 9

☒ group 10

☒ group 11

☒ group 12

☒ group 13

☒ group 14

☒ group 15

☒ group 16

Information object addresses assigned to each group must be shown in a separate table.

Clock synchronization

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒ Clock synchronization

□ Day of week used

□ RES1, GEN (time tag substituted/ not substituted) used

□ SU-bit (summertime) used

Command transmission

(Object-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒ Direct command transmission

□ Direct set point command transmission

☒ Select and execute command

□ Select and execute set point command

□ C_SE ACTTERM used

□ No additional definition

☒ Short-pulse duration (duration determined by a system parameter in the outstation)

☒ Long-pulse duration (duration determined by a system parameter in the outstation)

☒ Persistent output

□ Supervision of maximum delay in command direction of commands and set point commands

[configurable] Maximum allowable delay of commands and set point commands

Transmission of integrated totals

(Station- or object-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

□ Mode A: Local freeze with spontaneous transmission

□ Mode B: Local freeze with counter interrogation

□ Mode C: Freeze and transmit by counter-interrogation commands

□ Mode D: Freeze by counter-interrogation command, frozen values reported

Table continues on next page

□ Counter read

□ Counter freeze without reset

□ Counter freeze with reset

□ Counter reset

□ General request

□ Request counter group 1

□ Request counter group

□ Request counter group 3

□ Request counter group 4

Parameter loading

(Object-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

□ Threshold value

□ Smoothing factor

□ Low limit for transmission of measured values

□ High limit for transmission of measured values

Parameter activation

(Object-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

□ Act/deact of persistent cyclic or periodic transmission of the addressed object

Test procedure

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

☒ Test procedure

File transfer

(Station-specific parameter, mark with an “X“ if the function is used.)

Compare with "File transfer in monitor direction".

□ Transparent file

□ Transmission of disturbance data of protection equipment

□ Transmission of sequences of events

□ Transmission of sequences of recorded analogue values

File transfer in control direction

□ Transparent file

Background scan

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

□ Background scan

Acquisition of transmission delay

(Station-specific parameter, mark with an “X“ if the function is only used in the standard direction, “R“ if only used in the reverse direction, and “B“ if used in both directions.)

■ ~~Acquisition of transmission delay~~

Definition of time-outs

Parameter	Default value	Remarks	Selected value
t_0	30 s	Time-out of connection establishment	Configurable
t_1	15 s	Time-out of send or test APDUs	Configurable
t_2	10 s	Time-out for acknowledges in case of no data messages $t_2 < t_1$	Configurable
t_3	20 s	Time-out for sending test frames in case of a long idle state	Configurable (up to 65535 s)

Maximum range for time-outs: 1 s to 255 s, accuracy 1 s.

Maximum number of outstanding I format APDUs k and latest acknowledge APDUs (w)

Parameter	Default value	Remarks	Selected value
k	12 APDUs	Maximum difference receive sequence number to send state variable	Configurable
w	8 APDUs	Latest acknowledge after receiving w I format APDUs	Configurable

Maximum range of values *k*: 1 to 32767 (2^{15} –1) APDUs, accuracy 1 APDU

Maximum range of values *w*: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: w should not exceed two-thirds of *k*).

Portnumber

Parameter	Value	Remarks
Portnumber	2406	Configurable. The IEC-104 standard port is 2404 but in Arctic this port is reserved for IEC-101↔IEC-104 gateway application by default. The Direct I/O and Gateway applications must have unique ports when used simultaneously.

RFC 2200 suite

RFC 2200 is an official Internet Standard which describes the state of standardization of protocols used in the Internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

☒ Ethernet 802.3

□ Serial X.21 interface

□ Other selection from RFC 2200:

List of valid documents from RFC 2200

1. ....
2. ....
3. ....
4. ....
5. ....
6. ....
7. etc.

Section 11 Glossary

AC	Alternating current
APDU	Application protocol data unit
APN	Access Point Name
ARP	Address Resolution Protocol
ASDU	Application-layer service data unit
BIND	Berkeley Internet Name Domain
CTS	Clear to send
D-NAT	Destination network address translation
DC	1. Direct current 2. Disconnector 3. Double command
DCD	Data carrier detect
DHCP	Dynamic Host Configuration Protocol
DIN rail	A standardized 35 mm wide metal rail with a hat-shaped cross section
DIP	Dual in-line package
DNS	Domain Name System
DSR	Data set ready
DTE	Data Terminal Equipment
DTR	Data terminal ready
EMC	Electromagnetic compatibility
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
FME	For Mobile Equipment
FTP	File transfer protocol
GND	Ground/earth
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation. Network tunneling protocol.
GSM	Global system for mobile communications
HTML	Hypertext markup language

HW	Hardware
I/O	Input/output
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEC 60870-5-101	Companion standard for basic telecontrol tasks
IEC 60870-5-104	Network access for IEC 60870-5-101
IEC 60870-5-4	
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet protocol
IP address	A set of four numbers between 0 and 255, separated by periods. Each server connected to the Internet is assigned a unique IP address that specifies the location for the TCP/IP protocol.
LAN	Local area network
LED	Light-emitting diode
MAC	Media access control
MRU	Maximum Receive Unit
MTU	Maximum Transfer Unit
NC	Normally closed
NTP	Network time protocol
PC	1. Personal computer 2. Polycarbonate
PIN	Personal Identification Number
PPP	Point-to-point protocol
RF	Radio frequency
RFC 2200	Internet Standard which describes the state of standardization of protocols used in the Internet as determined by the Internet Architecture Board
RI	Ring Indicator
RISC	Reduced Instruction Set Computer
RJ-45	Galvanic connector type
RoHS	Restriction of the use of certain hazardous substances in electrical and electronic equipment
RS-232	Serial interface standard
RS-422	Serial communication standard (EIA–422)

RS-485	Serial link according to EIA standard RS485
RTS	Ready to send
RTU	Remote terminal unit
Rx	Receive/Received
RXD	Received exchange data
S-NAT	Source network address translation
SCADA	Supervision, control and data acquisition
SIM	Subscriber Identity Module
SMS	1. Short Message Service 2. Station monitoring system
SNMP	Simple Network Management Protocol
SSH	Secure shell
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	An Internet protocol that allows logging on to a remote computer using a user name and password
TSIG	Transaction signature
Tx	Transmit/Transmitted
TXD	Transmit exchange data
UDP	User datagram protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WHMI	Web human-machine interface
WWW	World Wide Web

Contact us

ABB Oy
Medium Voltage Products,
Distribution Automation
P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11
Fax +358 10 22 41094

www.abb.com/substationautomation

Power and productivity
for a better world™