Wireless Gateway
ARG600 Single SIM Variant
User Manual

Power and productivity
for a better world™

Document ID: 1MRS758456
Issued: 2017-09-22
Revision: B
Product version: 3.4

Copyright

Trademarks

Warranty

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

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.

Safety information

Dangerous voltages can occur on the connectors, even though the auxiliary voltage has been disconnected.

Non-observance can result in death, personal injury or substantial property damage.

Only a competent electrician is allowed to carry out the electrical installation.

National and local electrical safety regulations must always be followed.

This product is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment or as part of such equipment in any hazardous environment requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the hardware or software described in this manual could lead directly to death, personal injury, or severe physical or environmental damage.

To prevent damage both the product and any terminal devices must always be switched off before connecting or disconnecting any cables. It should be ascertained that different devices used have the same ground potential. The output voltage of the power supply should be checked before connecting any power cables.

The devices mentioned in this manual are to be used only according to the instructions described in this manual. Faultless and safe operation of the devices can be guaranteed only if the transport, storage, operation and handling of the devices is appropriate. This also applies to the maintenance of the products.

Table of contents

Table of contents

Section 1 Introduction

1.1 This manual

The user manual provides introductory information as well as detailed instructions on how to set up and manage the device as part of a network environment.

1.2 Intended audience

This manual addresses the personnel involved in installing and managing the devices.

The personnel is expected to be familiar with basic working principles of Internet technology.

1.3 Product documentation

1.3.1 Product documentation set

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

1.3.2 Document revision history

Document revision/date	Product version	History
A/2015-12-18	A	First release
B/2017-09-22	3.4	Content updated to correspond to the product version

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

1.3.3 Related documentation

Name of the document	Description	Document ID
Arctic Cyber Security Deployment Guideline		1MRS758860
3G/LTE configuration guide Technical Note	Configuring Wireless Gateways, Controllers and M2M Gateway	1MRS758449
OpenVPN server in Wireless Gateway/ Controller Technical Note	Configuring and using a static key OpenVPN server/client in Wireless Gateway and Controller products	1MRS758450
3G/LTE Wireless Gateway firmware update Technical Note	Updating firmware of Wireless Gateway devices	1MRS758451

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 Document conventions

A particular convention may not be used in this manual.

- Abbreviations and acronyms are spelled out in the glossary. The glossary also contains definitions of important terms.
- Menu paths are presented in bold.
  Select **Main menu/Settings**.
- 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 ARG600 overview

2.1 Overview

Wireless Gateway ARG600 provides wireless monitoring and control of field devices via cellular network from a central site or a control center. The devices offer industrial quality connectivity for the TCP/IP and serial port based protocols. Wireless Gateway ARG600 exhibits integrated communication capability and seamless integration to the SCADA systems.

Wireless Gateway ARG600 is a member of ABB’s Arctic product family and part of its 600 Wireless Gateway product series.

By using Wireless Gateway ARG600, Ethernet and serial devices can be attached to a TCP/IP based control system. With Wireless Gateway ARG600, conventional IEC60870-101 devices can be attached to a modern TCP/IP based IEC 60870-5-104 control system. This is made possible by the protocol conversion from IEC 60870-5-101 to IEC 60870-104. ARG600 also supports Modbus RTU to Modbus TCP protocol conversion.DNP3 serial devices can be attached to a DNP3 TCP SCADA system. In this case, the DNP3 protocol is transferred over TCP/IP communication (transparent serial gateway mode).

Wireless Gateway ARG600 can be utilized for various industrial and utility applications to maximize the benefits.

- Industrial grade TCP/IP router: several serial and TCP/IP based field devices can be integrated into a central supervisory and control system (SCADA)
- Integrated protocol conversion enables connecting the legacy serial-based devices into a TCP/IP-based supervisory control system (SCADA)
- Ideal for retrofitting by allowing the user to extend the life cycle of existing serial-based substation devices
- Remote access to field devices means less site visits for operations and maintenance
- Optimizing the cost of communication by using public cellular networks
- Possibility to upgrade from the existing legacy's private radio system to a higher bandwidth cellular network based solution. This enables to fully maximize the usage of the existing application. For example, the video surveillance of traffic can now be integrated into the same system.

2.2 Physical interfaces

2.2.1 Front panel

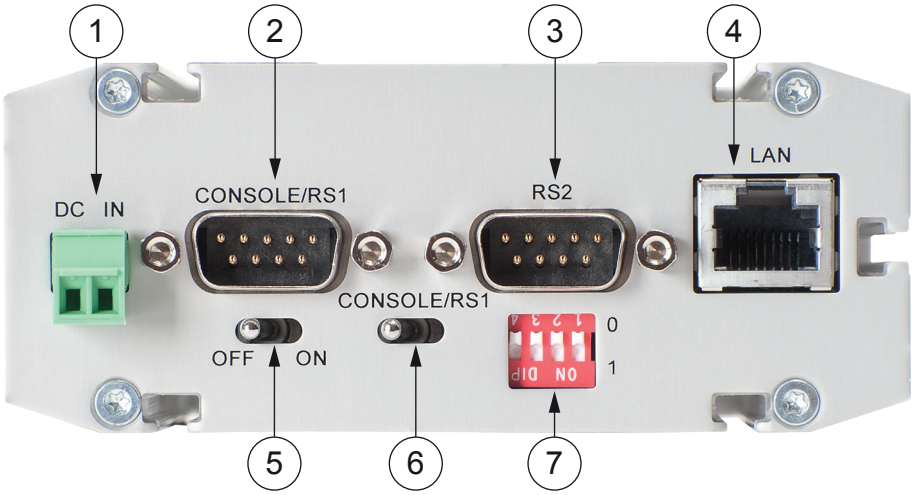

Figure 1: Front panel

1 Power supply 12...48 VDC
2 Console/serial port
3 Application serial ports
4 LAN/WAN port
5 Power switch
6 Console/serial port switch
7 DIP switches

Power supply connector

The device has a VDC power supply connector.

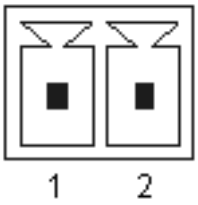

Figure 2: Power supply connector

Pin 1 Positive (+)
Pin 2 Negative (-)

The unit is protected against reversed polarity in specified voltage range.

Power switch

The power switch enables or disables the operation of the device.

Console enable switch

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

DIP switches

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

Table 1: DIP switches

DIP switch	Mode	Value	Description
1	RS-232/RS-485	“0” = RS-232 ”1” = RS-485	Selects 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	RS-485 biasing
4	TERMINATION	“0” = OFF “1” = ON	RS-485 termination

Ethernet connector

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

2.2.2 Back panel

The device has an antenna connector and a slot for a SIM card on the back panel.

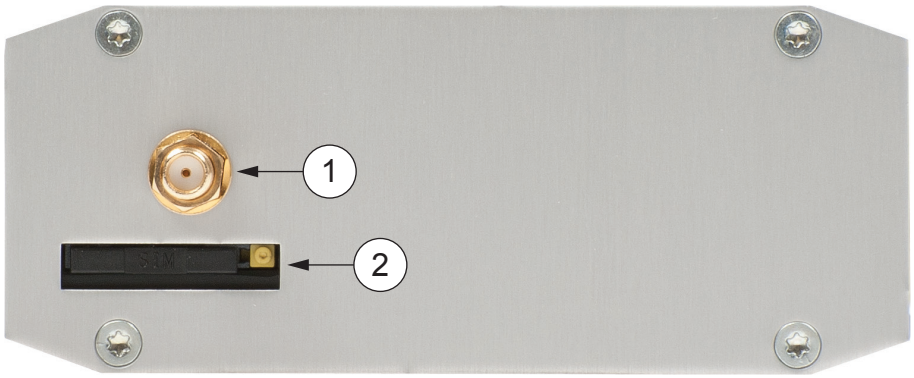

Figure 3: Back panel

1 Antenna connector SMA (female)
2 SIM card slot

2.2.3 Side panel

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

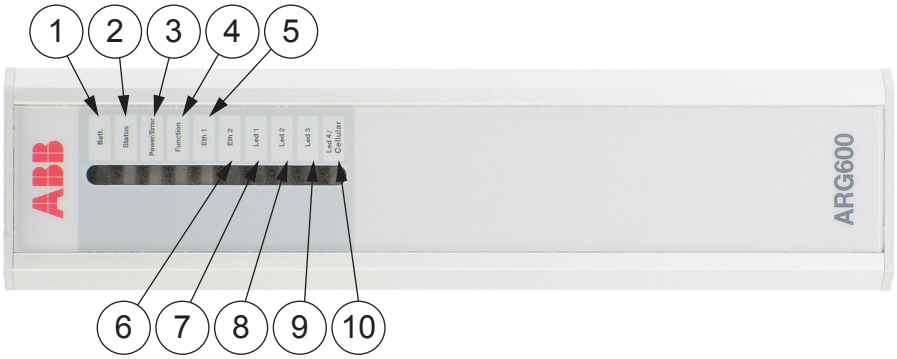

Figure 4: LEDs

1 Batt.
2 Status
3 Power/Error
4 Function
5 Eth 1
6 Eth 2
7 Led 1
8 Led 2
9 Led 3
10 Cellular

Table 2: Description of available LEDs

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

Table continues on next page

LED	Label	State	Description
9	Led 2	-	LED reserved for future use
10	Cellular	Flashing	Cellular connections up and active
		Off	Cellular connection is inactive

2.3 DIN rail mounting

The device has mounting holes for optional DIN rail mounting brackets. The order code for the DIN rail mounting kit is 2RCA028234 (DIN rail clips set consisting of a plastic clip and screws).

2.4 Product information label

The product label contains basic information about the unit such as product name, serial number and Ethernet MAC address.

2.5 Firmware version

The device's firmware version is visible on the welcome page (**System/Welcome Page**), which is displayed after logging in to the device.

For firmware updates, contact ABB's technical customer support.

Section 3 Physical connections

3.1 Communication connections

The device uses the serial ports for console or application communication, the Ethernet port for network communication and cellular connectivity for wireless applications.

3.1.1 Serial ports

The device has two application serial ports. Serial port 1 is configurable to either console or data mode and supports RS-232 only. Serial port 2 is configurable to multiple serial modes (RS-232/422/485). Serial port connectors are 9-pin D-sub male connectors. Serial ports function as DTE devices.

3.1.1.1 Console/serial port 1

The console switch enables or disables console access. When the switch is in the right position, serial port 1 is in the serial port mode, and when it is in the left position, serial port 1 is in the console mode.

The console switch is located below the serial port 1 connector. Turn off power from the device before toggling the console switch, as the switch position is read during the boot sequence only. The baud rate is fixed to 115200 bps when the port is configured in the serial console mode.

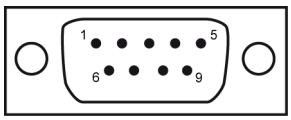

Figure 5: Console/RS1 port connector

Table 3: Console/RS1 port pinout

PIN	Function
1	DCD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR

Table continues on next page

PIN	Function
7	RTS
8	CTS
9	RI

Table 4: Console/RS1 port configuration

Parameter	Value
Baud rate	300...230400 (console 115200) bps
Data bits	8
Parity	No parity
Stop bits	1
Flow control	No flow control

3.1.1.2 Serial port 2

Serial port 2 can be configured to multiple serial formats (RS-232/422/485). The default is RS-232.

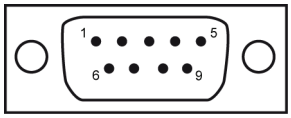

Figure 6: Application serial port

Table 5: Application serial port pinout (RS-232)

PIN	Function
1	DCD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI

Table 6: Application serial port configuration

Parameter	Value
Baud rate	300...460800 bps
Data bits	8
Parity	No parity
Stop bits	1
Flow control	CTS/RTS

By default, all DIP switches are set to the 0 position (RS-232 mode). DIP switches 2-4 apply only when the port is set in the RS-485 mode (DIP switch 1 in the 1 position).

Table 7: Application serial port DIP switches

DIP	Function	State	Description
1	RS-232 / RS-485	0 = RS-232, 1 = RS-485	Selects the serial port operation mode
2	DUPLEX	0 = FULL, 1 = HALF	Selects between half (2-wire) and full (4-wire) duplex
3	BIAS	0 = OFF, 1 = ON	RS-485 biasing
4	TERMINATION	0 = OFF, 1 = ON	RS-485 termination

Do not connect RS-422 or RS-485 cables to a serial port configured to the RS-232 mode. This could damage the port and the connected equipment.

Table 8: Application serial port pinouts in RS-422/485 modes

PIN	RS-422 full-duplex (4-wire)	RS-485 half-duplex (2-wire)
1	-	-
2	RXD positive (in)	-
3	TXD negative (out)	TXD/RXD negative (out/in)
4	-	-
5	GND	GND
6	-	-
7	TXD positive (out)	TXD/RXD positive (out/in)
8	RXD negative (in)	-
9	-	-

3.1.2 Ethernet

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

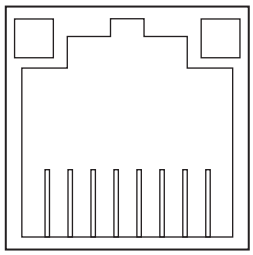

Figure 7: Ethernet connector

Table 9: Ethernet port configuration

Description	Value
Number of ports	1
Speed	10Base-T, 100Base-TX
Duplex	Half and full duplex
Auto-negotiation	No
Recommended cabling	Cat5e or better

The cross-connected cable is only used for connecting the device to the PC network interface. When connecting to a local network like a hub or switch, a direct Ethernet cable must be used.

3.1.3 Wireless network

The device supports cellular connectivity (GPRS, 3G, LTE) allowing the use of wireless applications. The device supports wireless data speed up to 100 Mbit/s. The practical data transfer rates depend on the subscription details and wireless network capacity.

The device with wireless interface includes an SMA female type connector for an external antenna. Any kind of external 50 Ω wide band antenna can be used intended for GPRS, 3G or LTE 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 male type SMA connector.

If the PIN code query is enabled, check that the ARG600 configurator has the correct PIN code entered in the wireless WAN submenu.

Section 4 Getting started

4.1 Connecting cables

1. Check that the power switch is in the OFF position.
2. Connect the Ethernet cable between the device’s Ethernet LAN connector and the computer used for the configuration.
3. Connect the power supply to the device.
4. Toggle the power switch to ON position.
   The power/error LED and function LED should turn on immediately after the power switch is turned on.

After the system has initialized, the function LED starts to flash.

4.1.1 Connection principle

The device has configurable network interfaces.

- Ethernet LAN/WAN port
- Mobile WAN cellular interface

The device can use a GPRS (2G), UMTS (3G) or LTE (4G) cellular network connection. The Mobile WAN interface is used for connecting the device to the cellular network. The Ethernet LAN is used for connecting other Ethernet devices to the device's local network.

The WAN interfaces can be configured to create a redundant system where one WAN automatically receives traffic if the other one goes down. For example, if the primary Ethernet connection goes down, the traffic is automatically switched to mobile WAN (secondary connection) and back when the Ethernet interface comes up again.

4.2 Logging in

1. Configure the computer to use the same IP address space as the device.
   Example: Laptop IP is 10.10.10.11 with netmask 255.255.255.0.
2. Check the IP configuration with the ping command in the command line.
3. In a Web browser, connect to the device over the HTTPS protocol using the device’s IP address.
   Example: The default IP address of the device is 10.10.10.10. The corresponding address to enter in the browser is https://10.10.10.10/.

Ignore the browser's warning about a self-signed certificate.

4. Enter the username and password.

The default username is “arctic-adm“ and the default password is “arcticm2m”. Change the password before connecting the product to a public network.

5. Click **Login**.
   The **Welcome Page** opens.

4.2.1 User interface

The user interface consists of views that can be opened from the menu in the left pane.

4.3 Setting Ethernet port function to LAN

Changing *Port function* to “LAN” disables automatic IP address detection. If *Port function* is set to the default value “auto”, the Ethernet LAN port tries to automatically obtain the IP address using DHCP when the device boots. If the DHCP discovery fails, the device automatically uses IP address 10.10.10.10.

Change the following setting before changing any other Ethernet settings.

1. In the left pane, under **Network**, click **Ethernet Port**.
2. Set **Port function** to **LAN**.
3. Click **Submit** to save the settings.

4.4 Configuring mobile WAN

Install the SIM card before configuring the mobile WAN.

1. In the left pane, under **Network**, click **Mobile WAN**.
2. Enter the preferred configuration in the configuration fields.
3. Click **Submit** to save the settings.

4.5 Configuring the default route

1. In the left pane, under **Network**, click **WAN Failover**.
2. Set **WAN Default Route** to **Yes**.
   This setting enables the use of the Ethernet WAN or the Mobile WAN as the default route interface.
3. If configuring Ethernet WAN as the default gateway, in the left pane under **Network**, click **Ethernet Port** and set **Port function** to **WAN**.
   If configuring Mobile WAN as the default gateway, skip this step.
4. Set the default route.
   - To select Ethernet WAN as the default gateway, under **Primary WAN**, set **Interface** to **Ethernet WAN**.
   - To select Mobile WAN as the default gateway, under **Primary WAN**, set **Interface** to **Mobile WAN**.
5. If both Ethernet WAN and Mobile WAN are configured, under **Backup WAN**, set **Interface** to **Mobile WAN** or **Ethernet WAN**, whichever is not selected as the default gateway.
   If the primary WAN interface comes down, the device automatically switches the default route to the backup WAN interface.
6. Click **Submit** to save the settings.
7. Restart the device.

Section 5 Network configuration

5.1 Defining host and domain names

1. In the left pane, under **Systems**, select **General Settings**.
2. In the **Hostname** field, enter the name of the device without the domain part.
3. In the **Domain** field, enter the domain name.

5.2 Configuring communication interfaces

5.2.1 Configuring Ethernet LAN

1. In the left pane, under **Network**, click **Ethernet LAN**.
2. Set **Enabled** to **Yes**.
3. Set **Interface**, **IP Address** and **Subnet mask**.
4. Click **Submit** to save the settings.

5.2.2 Configuring Ethernet WAN

1. In the left pane, under **Network**, click **Ethernet WAN**.
2. Set **Enable** to **Yes**.
3. Select a **WAN interface**.
4. Select a **Configuration Mode**.
   The “Manual (Static IP Address)” mode requires entering the values in the **Manual Settings** fields.
5. Click **Submit** to save the settings.

Use the Connectivity Monitor settings when WAN redundancy functionality is required. The Connectivity Monitor keeps checking the connection to the given remote host to determine the network status. If the ping does not get an answer within a given time window, it informs the WAN switch logic to try the secondary interface.

5.2.3 Configuring the mobile WAN interface

1. Set **Enable** to **Yes**.
2. If the SIM card is protected by a PIN code, enter the code in the **PIN Code** field.
   If necessary, change the SIM card’s PIN code by using a mobile phone.
3. If automatic APN discovery does not work, define the APN settings.

3.1. Set **APN Type** to **Manual**.
3.2. Type the cellular access point name in the **APN** field according to the network operator's instructions.

By default, the device uses automatic APN discovery with default APN values based on the network ID received from the cellular network. When *APN Type* is set to "Manual", the access point works as a gateway from the cellular network to the Internet. There are public and private access points. A public access point is usually defined. A private access point requires contract with a cellular operator. The device is compatible with both public and private access points.

4. If the cellular network's access point requires authentication, define the authentication settings according to the network operator's instructions.
   4.1. Set **Authentication** to **PAP** or **CHAP**.
   4.2. Type the access point's username in the **Username** field.
   4.3. Type the access point's password in the **Password** field.
5. If the device acts as a wireless router to Ethernet devices, and DNS is needed, enter the DNS settings.
   - Set **DNS Selection** to **From Network** to set up the device to receive DNS server IP addresses automatically from the cellular network.
   - Set **DNS Selection** to **Manual** to set up the device to use DNS servers manually defined in the **DNS Servers** field.
6. Click **Submit** to save the settings.
7. Restart the device to activate the configuration.

5.2.4 Setting WAN failover and backup routing

1. In the left pane, click **Network WAN Failover**.
2. Set **WAN Default Route** to **Yes**.
   This setting enables the use of the Ethernet WAN or the Mobile WAN as the default route interface.
3. Set the value of **Mobile WAN On Demand**.
   - If the backup WAN interface needs to come up only when the primary interface goes down, select **Yes**.
   - If both the wireless and Ethernet WAN interfaces have to be up all the time, select **No**.
4. Click **Submit** to save the settings.
5. Restart the device.

5.3 Routing parameters

The device has multiple configuration options that define routing.

Table 10: Routing parameters

Screen	Parameter	Value	Description
Ethernet WAN	Gateway (IP address)	(IP address)	IP address of router used to reach the internet. If not used, the field should be empty.
WAN Failover	WAN Default Route	Yes No	Usually "Yes" if the default route is defined by "static routes". “No” is required if the selection logic is done on VPN level.
	On Demand	Yes No	"Yes" activates the backup interfaces only when required. "No" makes all the WAN interfaces available simultaneously, for example, for VPNs.
	Primary WAN Interface	None Mobile WAN Ethernet WAN Ethernet WAN Secondary	These three settings configure the high-level default gateways. They must be configured to enable default route.
	Backup WAN Interface	None Mobile WAN Ethernet WAN	
	Secondary Backup WAN Interface	None Mobile WAN Ethernet WAN Ethernet WAN Secondary	
OpenVPN Client Settings	Interface	Any WAN Ethernet WAN Wireless WAN Ethernet LAN	This setting defines which interface to use for connection.
	Routing mode	None Host Net Default route	This setting defines how the routing is configured with OpenVPN. See OpenVPN application note.

5.4 Configuring the network monitor

The network monitor detects Internet connectivity drops by sending ping packets to designated targets. Its use is recommended.

1. In the left pane, under **Network**, click **Monitor**.
2. Set **Enable** to **Yes**.
3. Enter IP addresses for ping targets in **Target** and **Secondary target**.
4. Set the other values in the view.

The user interface contains information on the default values.

5. Click **Submit** to save the settings.

5.5 Configuring DNS proxy

The solution does not require name resolution because IP addresses are used directly in configuration. If name resolution is needed (for example, for browsing the Web), the device act as a DNS server for the devices connected to local LAN. When the DNS proxy is enabled, the device is defined as the DNS server for LAN devices (either manually or through DHCP) and the device forwards the name queries to the actual DNS server and back to the LAN devices.

1. In the left pane, under **Services**, click **Common**.
2. Set **Use DNS Proxy** to **Yes**.
3. Click **Submit** to save the settings.

5.6 Checking network status

The device has user interface views and LEDs that show network status and are useful in troubleshooting situations.

1. In the left pane, under **System**, click **Status** to view network status information.
2. In the left pane, under **Tools**, click **Modem Info** to view the status of the wireless modem.
3. Check if the cellular LED is flashing, indicating network traffic.

Section 6 Serial port configuration

6.1 Configuring serial ports

1. In the left pane, under **Serial Port and I/O**, click **General Configuration**.
2. Select an **Application Mode** for each serial port.
   - Serial Gateway: Transparent connection to any serial device
   - IEC-104: IEC-101 to IEC-104 conversion with IEC-101 serial device protocol
   - Modbus: Modbus conversion with Modbus/RTU or Modbus/ASCII serial device protocol

6.2 Serial gateway

The serial gateway feature enables data from the serial port attached device to be routed to Ethernet/mobile network (serial over IP) and vice versa. Serial gateway processes the transmitted data transparently and does not alter it any way except for buffering it for transmission. Because of the transparent communication, any protocols can be used in actual communication between nodes.Serial gateway configuration depends on used protocols.

Section 7 Additional system configuration

7.1 Changing passwords

1. In the left pane, under **Tools**, select **User Config**.
2. Type the old password in the **Old password** field.
3. Type the new password in the **New password** field and the **New password (confirm)** field.
4. Click **Submit** to save the settings.

See the cyber security deployment guideline for more information on password configuration.

7.2 Setting date and time

1. In the left pane, under **System**, click **Time**.
2. Set **Mode** to **Automatic (NTP)** or **Manual**.
   The “Automatic (NTP)” setting synchronizes the date and time with an remote NTP (or SNTP) server. The NTP server always defines the time in UTC time. The time zone can be set so that the device shows the time in a local format. There is also an NTP server in the device (NTP client and server), this enables the device to work as NTP server for the LAN devices.
3. Click **Submit** under the **Mode** setting.
   The lower part of the view is updated if the setting changed.
4. Check the time and date settings.
   - In the “Automatic (NTP)” mode, check the settings under **Current Time and Date (NTP mode)**, including **Time zone**, and click **Test NTP servers**.
   - In the “Manual” mode, enter the time and date in the **Time** and **Date** fields, respectively.

   Clicking **Copy PC** changes the device’s time and date settings to match the connected PC. This requires JavaScript support from the browser.
5. Click **Submit** to save the settings.

7.3 Restoring factory default settings

1. In the left pane, under **Tools**, click **Default settings**.
2. Select a configuration profile to overwrite with the factory default settings.
3. Click **Submit**.
4. In the confirmation dialog, click **OK**.
5. Restart the device.

7.4 Updating the firmware

Save a configuration profile as a backup of the current configuration before starting the firmware update.

Check that a valid firmware package is stored on the PC before attempting to update the firmware.

1. In the left pane, under **Tools**, select **Firmware Update**.
   The current firmware version is shown in the **Firmware Update** view.
2. Click **Browse** to open the file selection dialog.
3. Select the new firmware file.
4. Click **Update**.
   A confirmation dialog opens.
5. Click **OK** to confirm firmware.
   The update takes a few minutes.
6. Once the update is finished, restart the device.

7.5 Saving configuration profiles

It is possible to save the device's configuration in a profile for use in other devices or as a backup when updating the firmware. The configuration can be exported as an XML file.

1. In the left pane, under **Tools**, select **Configuration profiles**.
2. Click **Create a new profile**.
3. Select a profile to clone.
   Selecting **Last Boot** allows saving the configuration in use when the device was booted the previous time.
4. Type a name for the profile.
5. Click **Submit** to save the profile.

It is possible to clone, export, and import profiles in the same view.

Section 8 Service configuration

8.1 Configuring services

1. In the left pane, click **Services**.
   The service categories are listed under **Services**.
2. Click a service category.
3. Configure the service with the service parameters listed in the view.
4. Click **Submit** to save the settings.

8.2 Service parameters

Table 11: Common

Name	Description	Value range
Common Services		
Use DNS Proxy	Determines if the device acts as a DNS server for LAN devices.	No, Yes
LLMNR responder	The link-local multicast name resolution is a protocol that enables Windows™ machines on LAN to find the device using its hostname. This is currently supported in Windows™ Vista, Windows™ Server 2008, Windows™ 7 and Windows™ 8.x. By default, the device uses it's hostname (eg. arctic-02xxyy).	No, Yes
mDNS responder	The multicast domain name system is a protocol that enables Mac® OS X® machines on LAN to find the device using its hostname (for example, arctic-02xxyy).	No, Yes
SSH Server	The SSH (secure shell) is an encrypted network protocol for safe remote command line connections. It is replacing the Telnet protocol.	
SSH Server	Determines if logging into the device using SSH is allowed. The device has internal SSH server, which allows incoming SSH connections when enabled. By default, the SSH service is enabled for LAN connections.	No, Yes
SSH protocol version	Selects which SSH protocol versions are enabled in SSH Server. It is recommended to allow only SSH protocol version 2 (SSH2) to be used.	SSH1, SSH2
SSH public keys	SSH Public keys can be added for remote logins with SSHkeys.	

Table 12: DHCP server

Name	Description	Value range
DHCP Server Settings		
Enabled	Determines if the device acts as a DHCP server in LAN.	No, Yes
Required Settings		
Subnet	Defines the address of the subnet to listen to.	
Subnet mask	Defines the subnet mask of the subnet to listen to.	
Range low IP address	Defines the lowest IP address to share.	
Range high IP address	Defines the highest IP address to share.	
Optional Settings		
Domain name	DNS domain name given to clients.	
DNS Servers	List of DNS servers (comma separated).	
Gateway IP address	IP address of the default gateway. This must usually be defined as Arctic's own IP address.	
Broadcast IP address	Usually the last IP address of the subnet.	
Default lease time	Given to clients that don't request a specific lease length (empty: 10800).	
Maximum lease time	The maximum lease time given to clients (empty:10800).	
NTP Servers	List of NTP servers (comma separated).	
LPR Servers	List of line printer (LPR) servers (comma separated).	
WINS Servers	List of WINS servers (comma separated).	

Table 13: DynDNS client

Name	Description	Value range
DynDNS client settings		
DynDNS service client enabled		No, Yes
DynDNS service provider	Selects the supported dyndns service provider.	
DynDNS client update interval	Defines how often (in seconds) the device's IP is checked.	
DynDNS hostname	Arctic name reported to service, for example, host name.	

Table continues on next page

Name	Description	Value range
DynDNS username	User name for dyndns service.	
DynDNS password	Service password.	
DynDNS logging enabled	Logs dyndns update to system log.	No, Yes

Table 14: SNMP agent

Name	Description	Value range
SNMP Agent		
Enable SNMP	Enables SNMP	No, Yes
Read only SNMP community	Defines read only SNMP community.	
Read and write SNMP community	Defines read and write SNMP community.	
Server port	The default server port is 161.	

Table 15: Arctic Patrol

Name	Description	Value range
Basic Information		
Enabled	Enables Viola Patrol.	No, Yes
Server IP, Port	Server IP address and the port server listens. If no value is given, the value is 10000.	
Connection interval	Defines how often to report to server.	
Backup active configuration to server	When set to “Yes”, copies encrypted version of XML configuration file to server.	No, Yes
Registration password	Password needed to register to server. This password should not be entered after registration unless re-registering is necessary.	

Section 9 IEC-104 application settings

9.1 The use of the IEC-104 protocol

The IEC-104 and IEC-101 protocols share the same ASDU level messaging but differ on the link level. IEC-104 is intended for packet-switched TCP/ IP communication whereas IEC-101 is intended for serial communication. By using the device, the IEC-101 slaves (for example RTUs) can be connected to a IEC-104 master (for example SCADA). The device requests an event from the IEC-101 slave locally and sends them to the IEC-104 master. This eliminates the need to continuously poll the data remotely and therefore reduces the communication costs on pay-per-use wireless network.

9.2 Configuring IEC-104 application settings

1. In the left pane, select **Serial Port and I/O/IEC-104 Gateway (RSx)**.
2. View and change settings in the view that opens.
3. Click **Submit** to save the settings.

9.3 IEC-104 application settings

Table 16: IEC-104 application settings

Name	Description	Value range
Basic settings		
Enable IEC-104 gateway	Enables or disables IEC-104 to IEC-101 gateway functionality.	No, Yes
Serial settings	The serial settings define the properties of physical serial communication between the device and an IEC-101 slave. The selection between RS-232/422/485 is made with physical DIP switches located below the RS2 serial port.	
Serial port	Indicates the serial port to which the settings apply.	RS1, RS2
Speed	IEC-101 serial communication speed (bits per second)	1200, 2400, 4800, 9600, 19200, 38400, 57600
Data bits	Number of data bits used on IEC-101 serial communication	5, 6, 7, 8
Parity	Parity method used on IEC-101 serial communication	None, Even, Odd

Table continues on next page

Name	Description	Value range
Stop bits	Number of stop bits used on IEC-101 serial communication	1, 2
Use HW flow control	HW flow control mechanism (RTS/CTS) on IEC-101 serial communication. Note: The HW handshaking is available only on RS-232 mode.	No, Yes
Network settings	The Network settings define the general TCP/IP networking properties between the device and the IEC-104 master.	
Network protocol	Network protocol defines the network transmission layer protocol (either TCP or UDP) used on IEC-104 network communication. The IEC-104 standard protocol uses TCP, but for reliable slow speed packet switched networks (for example Mobitex), the UDP protocol can be used to minimize the packets transmitted over network. Note: The IEC-104 standard specifies only TCP protocol.	UDP, TCP
Network protocol to listen	TCP or UDP port number to listen for incoming IEC-104 connections	0...65000
Network idle timeout	Network idle timeout defines the idle timeout of the network connection in seconds. If there is no network data received during the specified interval, the connection is closed by the device. This parameter is required in order to detect partially closed connections and release the resources for new connections especially if the *New connection priority* parameter is disabled. Value “0” disables the network idle timeout detection. The network idle timeout must be longer than IEC-104 link test interval (t3).	0...65000
New connection priority	It 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. It is recommendable to set this value to “Yes” in normal configurations having only one IEC-104 master.	No, Yes
Max clients	Max clients defines the maximun number of connections (redundancy group).	1...3
IEC-104 settings	The IEC-104 settings define the properties of IEC-104 link layer and application layer parameters as described in the IEC 60870-5-104 standard. The IEC-104 communication is carried out between the device and the IEC-104 master over the TCP/IP network.	
TX window size (k)	TX window size defines the maximum number of I format APDU packets the device may send before requiring the IEC-104 master to acknowledge them. If there are *k* unacknowledged frames sent the device stops polling IEC-101 slave for events until acknowledgement is received. The *k* must be always less than the maximum sequence number defined below. The IEC-104 standard suggests *k* to be 12.	1...20
RX window size (w)	RX window size defines the maximum number of I format APDU packets the device may receive before sending acknowledgement to the IEC-104 master. The *w* should not exceed two-thirds of TX window size *k*. The IEC-104 standard suggests *w* to be 8.	1...20
I frames TX timeout (t1)	It defines the timeout in seconds the device waits for acknowledgement from IEC-104 master after sending last I format APDU or control frame (e.g. link test). If no acknowledgement is received during the defined time the device will close the network connection and the IEC-101 link. The t1 must be longer than the network round-trip-time. The IEC-104 standard suggests 15 seconds.	1...255
I frames RX timeout (t2)	This defines the timeout in seconds from the last received I format APDU before sending acknowledgement. The t2 must be smaller than t1. The IEC-104 standard suggests 10.	1...255

Table continues on next page

Name	Description	Value range
Link test interval (t3)	This defines the interval in seconds how often the IEC-104 link is tested if there is no other activity. The recommended value depends on the criticality of the link. The IEC-104 standard suggests 20 seconds but for pay-per-use GPRS connections the practical value may be substantially longer.	1...65000
Test link on suspended state	Answer to test frame activation if the 101 link is in the suspended state.	No, Yes
Suspended timeout	This defines the time in seconds how long a connected IEC-104 link can be in suspended state (STOPD) before the device closes the connection. Using this parameter increases the probability of detecting partially closed network connections especially in UDP mode.	1...65000
Max sequence number	These are the maximum sequence number used in IEC-104 communication. The default value “0” equals to 32767 as suggested by the IEC-104 standard.	0...32767
Flush buffered events on connection	Defines if buffered events are flushed on new a IEC-104 connection.	No, Yes
Cause of transmission length	It defines the length of IEC-104 Cause of transmission ASDU header field in bytes. The IEC-104 standard defines value “2”.	1, 2, 3
Common address length	This defines the length of IEC-104 Common address ASDU header field in bytes. The IEC-104 standard defines value “2”.	1, 2, 3
Info object address length	This defines the length of IEC-104 Information object address ASDU header field in bytes.	1, 2, 3
IEC-101 settings	The IEC-101 settings define the properties of IEC-101 link layer and application layer parameters as described in the IEC 60870-5-101 standard. The IEC-101 communication is carried out between the device and a IEC-101.	
Slave link address	The link-level address of IEC-101 slave.	1...65000
Link address field length	Defines the length of the IEC-101 link-level address field in bytes. The link-level address of IEC-101 slave.	1, 2
Event poll interval	Event poll interval defines the IEC-101 event polling interval in 0.1 second increments (class 1 or 2 poll). The events are polled only when the IEC-104 connection is active.	1...65000
Link test interval	Link test interval defines the IEC-101 link test interval in 0.1 second increments. Link test is performed if there is no other activity. The link test is performed if there is no other activity during defined interval.	1...65000
Keep link open	Defines that the IEC-101 link is kept always open even when there is no active IEC-104 connection. If the functionality is enabled the device sends link test frames and restarts the IEC-101 link if the test fails. The events are still not polled before the IEC-104 connection is active. Some IEC-101 slaves require the link to be continuously open in order to operate.	No, Yes
Reply header timeout	Defines the timeout in milliseconds that the device waits the reply to start from IEC-101 slave after command or request.	1...65000
Reply end timeout	Defines the maximum duration of IEC-101 slave response in seconds.	1...65000
Retry limit	Defines the number of retries sent to a IEC-101 slave in case of no reply. If no reply is still received the device closes the IEC-101 and IEC-104 connections.	0...65000

Table continues on next page

Name	Description	Value range
Cause of transmission length	Defines the length of IEC-101 cause of transmission ASDU header field in bytes. The IEC-101 standard defines value 1.	1, 2, 3
Common address length	Defines the length of the IEC-101 common address ASDU header field in bytes. The IEC-101 standard defines value 2.	1, 2, 3
Info object address length	Defines the length of IEC-101 information object address ASDU header field in bytes. The IEC-101 standard defines value 2.	1, 2, 3
ASDU Converter	The ASDU converter can be used to convert ASDU header field lengths between IEC-101 and IEC-104 protocols.	
Use ASDU converter	This defines if the ASDU header level conversion between IEC-101 and IEC-104 is performed. If enabled the ASDU header field lengths are converted between IEC-104 and IEC-101. This parameter must be enabled if the ASDU header lengths differ between the IEC-104 and the IEC-101. The information on the field must fit in the shorter one of the two. It's not possible to convert e.g. value 12000 to a one byte field.	No, Yes
Use ASDU type replacer	The ASDU type replace function can be used to convert an ASDU type (Original type) to another (Applied type) type e.g. in cases when the IEC implementation differs between master and slaves.	No, Yes
IEC-101 ASDU type	The original ASDU type searched by ASDU type replacer.	0...255
IEC-104 ASDU type	The new ASDU type is replaced by the original type.	0...255
Convert short IEC-101 time stamps	Defines if 56-bit timestamps are converted to 24-bit.	No, Yes
Packet collector	The packet collector can be used to collect many IEC-101 messages and events to a single network packet instead of sending every message separately. This function is useful for slow packet switched communication network (for example Mobitex) for speeding up especially the general interrogation response.	
Use packet collector	Determines if the packet collector is in use.	No, Yes
Max bytes	Max bytes defines the maximum bytes trigger for packet collector. Before a new packet is inserted into the packet collector buffer the amount of bytes is checked. If the insertion of the new packet would cause the number of bytes in the packet collector to exceed MAX BYTES, the old content is sent to the network before inserting the new one. The value should be smaller than the MTU/MRU of network used.	1...1500
Max time	Max time defines the maximum collect time trigger for packet collector in 0.1 second increments for packet collector. If there has been data on packet collector over MAX TIME, the data is sent to network. The value must be smaller than t1.	1...255
Max packets	Max packets defines the maximum amount of IEC-101 packets stored into the packet collector before sending the data to the network.	1...255
Other settings		
Write syslog	Write syslog defines if the error messages are stored to system log file or not. The system log is available by using Web user interface.	No, Yes

Section 10 Modbus application settings

10.1 Modbus Gateway properties

The Modbus Gateway is an adapter application enabling conversions between serial and network Modbus protocols. The gateway can operate on two modes; either connecting serial masters to slaves behind the network or connecting network master to serial slaves.

The gateway offers a number of core properties.

- Supports Modbus RTU and Modbus ASCII serial protocols
- Supports Modbus TCP, Modbus RTU over TCP, Modbus RTU over UDP, Modbus ASCII over TCP and Modbus ASCII over UDP network protocols
- Generates and filters out gateway exceptions
- Routes traffic on the network, based on Modbus addressing, enabling intelligent use of network resources
- Makes automatic connection management
- Enables multiple server sessions over network
- Offers unlimited amount of Masters on serial or Network side
- Offers 30 routes over network to slaves

10.2 Modbus modes

Serial master to network slaves

When the Modbus master supports serial based Modbus, communication needs to control slaves over a TCP/IP network. The device on the master side must be in the “Serial master to network slaves” mode.

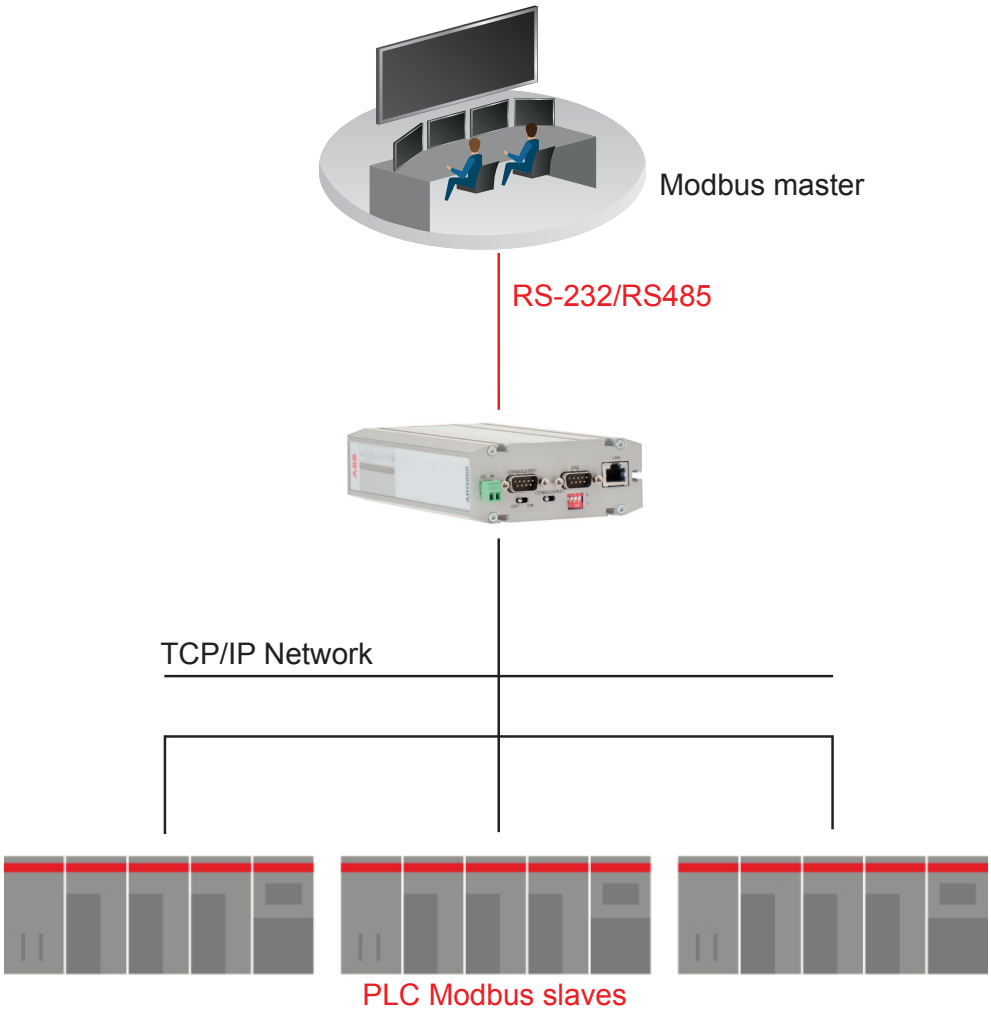

Figure 8: Serial master to network slaves mode

In that mode, the device routes serial Modbus packets to network and performs conversions between serial and network protocols. The routing based on Modbus addressing allows intelligent use of network resources, which is especially useful for pay-per-use networks like GPRS. The settings consist of two parts, common settings and settings for each route.

Network master to serial slaves

When the PLC/RTU slaves supporting serial based Modbus communication are required to be controlled over TCP/IP networks, the device on the slave side must be in the “Network master to serial slaves” mode.

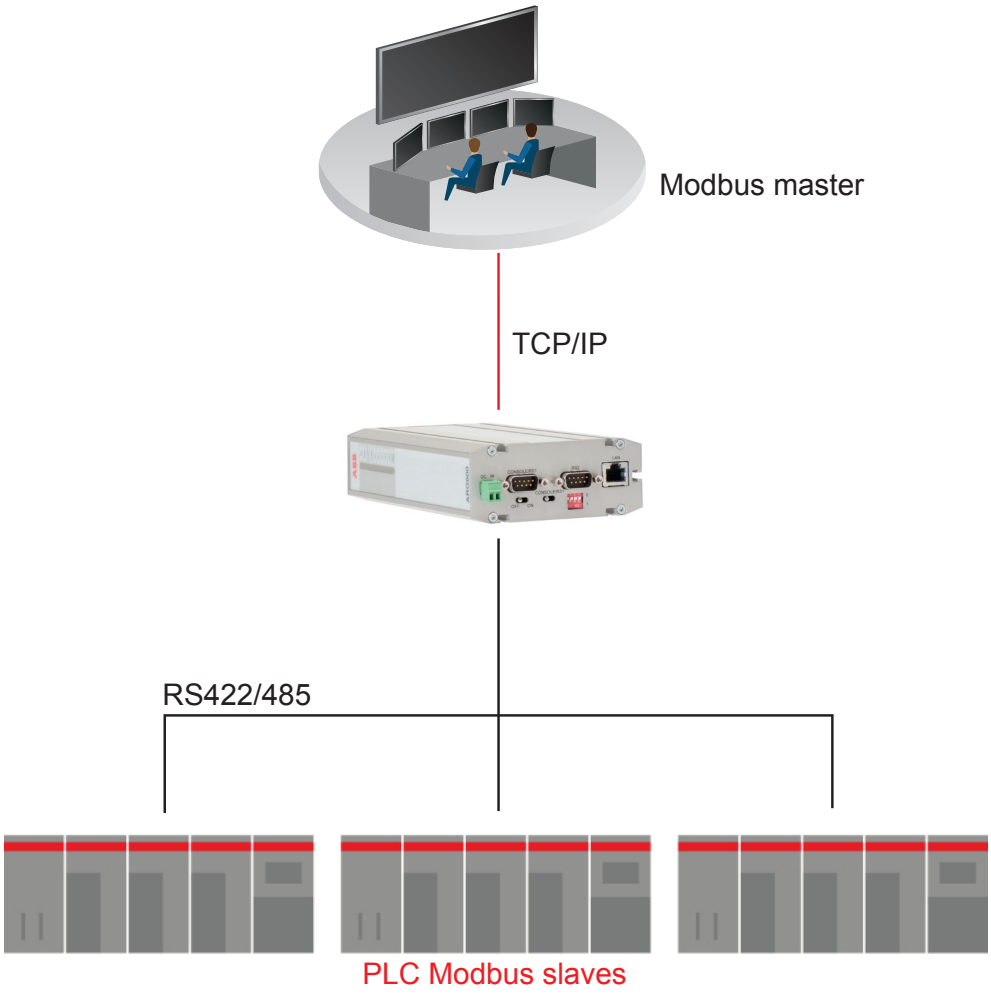

Figure 9: Network master to serial slaves mode

In that mode, the device acts like network server where masters (clients) can connect (the default port being 502) and transmit Modbus requests. The device makes conversions between network and serial protocols. If the slave does not reply during defined timeout or if the reply is corrupted, the device sends “gateway exception message” back to the master if the exception generation is enabled. Otherwise, the reply is returned. Multiple masters can connect simultaneously to the Gateway, which handles the multiplexing between masters.

10.3 Configuring Modbus modes

10.3.1 Configuring the serial master to network slaves mode

1. In the left pane, under **Serial Port and I/O**, click **Modbus Gateway (RSx)**.
2. Set **Enable Modbus gateway** to **Yes**.
3. Set **Gateway mode** to **Serial master to network slaves**.

4. Set the parameters under **Serial settings**, **Protocols**, **Framing**, **Exceptions**, as the network and the Modbus master and slaves require.
   See Chapter Common parameters for additional information and recommendations.

   The parameters under **Network server settings** are not used in the “Serial master to network slaves” mode.

5. In the **Routes to client/slaves** tab, set the route parameters.
   See Chapter Route parameters for additional information and recommendations.
6. Click **Submit** to save the settings.
7. Restart the device.

10.3.2 Configuring the network master to serial slaves mode

1. In the left pane, under **Serial Port and I/O**, click **Modbus Gateway (RSx)**.
2. Set **Enable Modbus gateway** to **Yes**.
3. Set **Gateway mode** to **Network master to serial slaves**.
4. Set the parameters under **Serial settings**, **Protocols**, **Framing**, **Exceptions** and **Network server settings** as the network and the Modbus master and slaves require.
   See Chapter Common parameters for additional information and recommendations.
5. Click **Submit** to save the settings.
6. Restart the device.

10.4 Parameter settings

10.4.1 Parameter types

The parameters are divided into two groups.

- Common parameters
- Route parameters

Common parameters define for example the protocols used in serial and network communications, serial port settings and protocol specific timeouts. Route parameters are only required in the "Serial master to network slaves" mode defining the IP and Modbus addresses of slaves behind the network.

10.4.2 Common parameters

Table 17: Common parameters

Name	Description	Value range
Basic settings		
Enable Modbus gateway	If set to “Yes”, the Modbus gateway functionality is enabled for the serial port. Each serial port of the device has its own Modbus gateway definitions.	No, Yes
Serial settings		
Serial port	Defines the serial port that the device uses for Modbus serial communication. The possible settings are “RS1”, which selects serial port 1 (RS-232 console/application port) and “RS2”, which selects serial port 2 (RS-232/422/485 application port). If a single serial port or RS-422/485 is required, port 2 is recommended. If Port 1 is used, the console switch of the device must be in the Application position. DIP switches below the DB-9 serial connector specify the RS-232/422/485 settings of Port 2.	RS1, RS2
Serial settings		
Speed	Defines the serial port speed for Modbus communication in bps. The optimal speed depends on the connected Modbus equipment.	300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Data bits	Defines the number of data bits used in Modbus serial communication. The required number depends on how many data bits the connected Modbus equipment supports. Generally Modbus RTU communication uses 8 data bits and Modbus ASCII communication uses 7 data bits.	5, 6, 7, 8, Auto
Parity	Defines the parity method used in Modbus serial communication. If set to “None”, no parity method is used. If set to “Even”, an even parity bit is generated and inspected. If set to “Odd”, odd parity bits are generated and inspected.	None, Even, Odd
Stop bits	Defines the number of stop bits used in Modbus serial communication.	1, 2
Use HW handshaking (CTS/RTS)	Enables CTS/RTS handshaking if set to “Yes”.	No, Yes
Gateway mode		
Gateway mode	If set to “Network master to serial slaves”, the slaves are on the serial side. If set to “Serial master to network slaves”, the slaves are on the network side. If the slaves are on the network side, the routes also need to be defined.	Network master to serial slaves, Serial master to network slaves
Protocols		
Serial protocol	Defines the Modbus protocol that serial devices use in serial communication. The possible settings are Modbus RTU protocol and Modbus ASCII protocol. ModbusRTU is recommended because it is more efficient.	ModbusRTU, ModbusASCII

Table continues on next page

Name	Description	Value range
Network protocol	Defines the TCP/IP and Modbus protocol used on network communication. Possible protocols are Modbus TCP protocol over TCP, Modbus RTU protocol over TCP, Modbus RTU protocol over UDP, and Modbus ASCII protocol over UDP.	ModbusTCP, ModbusRTU over TCP, ModbusRTU over UDP, ModbusASCII over TCP, ModbusASCII over UDP
Framing		
Slave response timeout	Defines the time in microseconds (millionths of a second) how long the device waits for the response from a Modbus slave. If the response is not received, the device can generate and return a Modbus gateway exception. The reply timeout of the Modbus master must be greater than the gateway device timeout. Otherwise, the flow of request-reply communication is violated. The device does not accept a new request before the reply from the slave is received or the reply timeout is elapsed. The delays in network communication can vary especially in wireless networks. When the slaves are located on the network side, ping or another method should be used to estimate the delay packets spend on network.	0...90 000 000 (0...90 seconds)
Inter-frame timeout	Defines the idle time in microseconds (millionths of a second) that marks the end of Modbus frame in serial communication. If the value is zero, the device uses the standard 4 character time. The recommendation is to use a value as small as possible to speed up communication and increase the value if problems arise. Some PC programs can insert unexpected delays between serial characters.	0...2 000 000 (0...2 seconds)
Exceptions		
Generate gateway exceptions	Defines if the device generates and returns a Modbus gateway exception message to the master if no valid reply is not received from the slave. If set to “Yes”, the generation of exceptions is enabled. This functionality is useful for debugging.	No, Yes
Pass gateway exceptions	If set to “Yes”, gateway exception replies from the slave side are passed to the master. If set to “No”, the replies are filtered away.	No, Yes
Network server settings		
Server TCP/UDP - port	Defines the TCP or UDP port that masters can form connections to. Default Modbus TCP/IP communication port is 502. If multiple Modbus gateways are running on same device (for both serial ports) the TCP/UDP communication ports must not be same. For example, ports 502 and 504 can be used. The network and the device's firewalls must enable TCP or UDP communication for that port.	1...32500

Table continues on next page

Name	Description	Value range
Max. number of clients	Defines how many network masters can be connected to the device simultaneously. The recommended value is at least 2 when using TCP communication. Otherwise if the device does not recognize a partially closed connection, forming new connections is not accepted by the device the time set in parameter “Connection idle timeout” is elapsed.	0...20
Connection idle timeout	If there has not been communication on this route during given amount of seconds, the device automatically closes the TCP connection to slave and therefore frees the slave’s communication resources. This is especially useful when multiple masters access the same slave. The recommended setting is about two times the polling interval of the master.	0...32500
Enable keepalive	Defines if connection testing is performed by sending TCP keepalive packets at certain intervals. enabled for TCP network communication. If set to “Yes”, testing the TCP connection with slave is enabled.	No, Yes

10.4.3 Route parameters

Table 18: Route parameters

Name	Description	Value range
Route information		
Route in use?	Each IP address and TCP/UDP port of slaves needs to be defined on separate route entries.	No, Yes
Host (name or IP-address)	The IP address or host name of a device where packets are routed by that entry. If host names are used, the DNS server IP address is required to be defined in the network settings. The Network Protocol setting on “Common parameters” defines the network and Modbus protocol used on network communication.	IP address or host name
TCP or UDP destination port	Defines the UDP or TCP destination port where this route entry sends Modbus requests. The port must be same as used on the network slave device or gateway behind network. The default Modbus port is 502.	0...32500
Filter slave addresses?	Defines if the routing based on Modbus addresses is used for that entry. If set to “No”, every Modbus request is routed to this entry. If set to “Yes”, only Modbus requests that have destination addresses matching the address list of entry are routed. It’s recommended to use routing based on Modbus address filtering in order to avoid unnecessary network traffic.	No, Yes
Table continues on next page		

Name	Description	Value range
Slave addresses behind this route	A list of Modbus slave addresses behind this route entry. The *Filter slave addresses?* parameter must be set to “Yes” for these addresses to be enabled.	A comma-separated list of addresses with up to 20 addresses
Connection idle timeout (TCP)	This parameter defines the timeout in seconds before the device automatically closes the TCP connection to a slave if there has not been communication. This frees up the slave's communication resources and is useful when multiple masters access the same slave. The recommended timeout is two times the polling interval of the master. If the polling interval is very long (over an hour), the recommended timeout is 200 seconds longer than the polling interval.	0...32500
Enable TCP keepalive	If set to “Yes”, connection testing with TCP keepalive packets between the master and slave devices is enabled for TCP network communication. The recommended setting is “Yes” if the polling interval or idle timeout is very long.	No, Yes

10.4.3.1 Modbus route settings

The route entries define how Modbus packets are routed on network from the serial master to network slaves. Up to 30 routes can be specified, and each route can have up to 20 specified slaves. If the routing is based on Modbus addressing or there are more than 20 slaves behind the route, the address filtering for that entry can be disabled by setting *Filter* to “No”.

- The Create new button opens the Route information view, in which it is possible define settings for the new route.
- The edit button allows changing the settings for an existing route.
- The trashcan button allows removing an existing route.

Section 11 Troubleshooting

If a troubleshooting issue persists, download a support log in **Tools/Support Log** and send it to the technical support. The log shows status information and the device's current configuration. The network test functionality in **Tools/Network Test** performs different network tasks, which help determine if the device's configuration and connections function properly.

11.1 Common troubleshooting issues

Table 19: Common troubleshooting issues

Problem	Suggested solution
Wireless WAN does not work.	Check mobile WAN settings, SIM card and signal level.
OpenVPN does not work.	For more information, see the OpenVPN server in Wireless Gateway/Controller technical note.
Serial ports do not work.	For more information, see serial port chapter notes. Verify DIP switch configuration if RS-422 or 485 modes are being used.
Access to web user interface does not work.	Web user interface uses HTTPS for secure web access and it must be specified on the web browser address field like in this example: https://10.10.10.10.
Access to the Internet with a laptop connected to the device does not work.	Test the wireless connection: 1. Configure wireless connection and verify if it is connected to the network. 2. Connect a laptop to Ethernet LAN. 3. Check that S-NAT rule on the firewall is set as **Action** is "Masquerade" and **Destination Interface** is "Mobile WAN". 4. Check that **Use DNS Proxy** is set to “Yes” in the **Services/Common** screen. 5. Configure network settings on laptop to use the device's Ethernet LAN address as gateway and DNS server. With these settings, the Internet should be accessible on the laptop.

11.2 Viewing the system log

1. In the left pane, under **Tools**, select **System Log**.
2. If necessary, refresh the system log with the Web browser’s reload or refresh button.

Section 12 Technical data

Technical specifications can be changed without notification.

Table 20: Dimensions

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

Table 21: Hardware

Description		Value
Processor environment	Processor	32 bit RISC
	Memory	128 MB Flash
		128 MB RAM
Power	Power supply	12...48 VDC (nominal)
	Power consumption	1...5 W
Other	Internal clock	Real time
Approvals		CE
Environmental conditions	Temperature range	-30...+70°C (operating)
		-40...+85°C (storage)
	Humidity	5...85% RH (non condensing)
	Protection class	IP30

Table 22: Supported protocols

Master protocol	Slave protocol
IEC 60870-5-104	IEC 60870-5-101
Modbus TCP	Modbus RTU/ASCII
TCP/IP, UDP/IP (DNP3)	Serial gateway - serial port data stream (such as DNP3)

Table 23: Network interfaces

Description		Value
Ethernet ports	Ethernet/LAN	10/100 Base-T. Shielded RJ-45
		1.5 kV isolation transformer
		Ethernet IEEE 802-3, 802-2

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	RS-232 DTE, RS-422, RS-485 (selectable)
		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

Table 24: Wireless network interfaces (WAN)

Product	Air interface	Frequency	Maximum data rate
ARG600A1260NA	GPRS/EDGE	1900/1800/900/850 MHz	85.2 Kbps/236.8 kbps
	WCDMA/HSPA+	2100/1900/900/850 MHz	21 Mbit/s
	LTE	2600 (band 7)/2100 (band 1)/1800 (band 3)/ 900 (band 8)/800 (band 20) MHz	100 Mbit/s

Table 25: Antenna connector and SIM card types

Description	Type
Antenna connector	SMA (female, 50 Ω)
SIM card type	2FF (Mini SIM)

Table 26: Electromagnetic compatibility tests

Description		Reference
Emission tests according to the test specification IEC 61850-3 (Edition 2.0 2013-12)	Radiated disturbance	CISPR 16-2-3
	Conducted disturbance	CISPR 16-2-1
Immunity tests according to the test specification IEC 61850-3 (Edition 2.0 2013-12)	Electrostatic discharge (ESD)	EN 61000-4-2 (2008-12)
	Radiated radiofrequency electromagnetic field	EN 61000-4-3 (2006-02)
	Electrical fast transient (EFT)	EN 61000-4-4 (2012-04)
	Surge	EN 61000-4-5 (2005-11)
	Conducted radiofrequency electromagnetic field	EN 61000-4-6 (2008-10)
	Power frequency magnetic field	EN 61000-4-8 (2009-09)

Table 27: RoHS and REACH compliancy

Description	Reference
Directive	RoHS directive 2002/95/EC
	REACH directive 2006/1907/EC

Section 13 Glossary

CHAP	Challenge handshake authentication protocol
CTS	Clear to send
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
DNP3	A distributed network protocol originally developed by Westronic. The DNP3 Users Group has the ownership of the protocol and assumes responsibility for its evolution.
DNS	Domain Name System
DSR	Data set ready
DTE	Data Terminal Equipment
DTR	Data terminal ready
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
GND	Ground/earth
GPRS	General Packet Radio Service
LAN	Local area network
LED	Light-emitting diode
NTP	Network time protocol
PAP	Password authentication protocol
PC	1. Personal computer 2. Polycarbonate
RAM	Random access memory
RI	Ring Indicator
RISC	Reduced Instruction Set Computer
RJ-45	Galvanic connector type
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
RXD	Received exchange data
SCADA	Supervision, control and data acquisition
SIM	Subscriber identity module
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TXD	Transmit exchange data
VPN	Virtual Private Network
WAN	Wide area network

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/mediumvoltage
www.abb.com/substationautomation

Power and productivity
for a better world™