
Wireless Gateway

ARG600 ANSI Single SIM Variants

User Manual





Document ID: 1MRS758865
Issued: 2021-12-10
Revision: E
Product version: 3.4.7

© Copyright 2021 ABB. All rights reserved

Copyright

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party, nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB is a registered trademark of the ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Warranty

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

abb.com/mediumvoltage

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. In case of discrepancies between the English and any other language version, the wording of the English version shall prevail.

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

Section 1	Introduction.....	3
	This manual.....	3
	Intended audience.....	3
	Product documentation.....	3
	Product documentation set.....	3
	Document revision history.....	3
	Related documentation.....	4
	Symbols and conventions.....	4
	Symbols.....	4
	Document conventions.....	5
Section 2	ARG600 overview.....	7
	Overview.....	7
	Physical interfaces.....	8
	Front panel.....	8
	Back panel.....	10
	Side panel.....	11
	DIN rail mounting.....	13
	Product information label	13
	Firmware version.....	13
Section 3	Getting started.....	15
	Connecting cables.....	15
	Connection principle.....	15
	Logging in.....	15
	User interface.....	16
	Setting Ethernet port function to LAN.....	16
	Configuring mobile WAN.....	17
	Configuring the default route.....	17
Section 4	Network configuration.....	19
	Defining host and domain names.....	19
	Configuring communication interfaces.....	19
	Configuring Ethernet LAN.....	19
	Configuring Ethernet WAN.....	19
	Configuring the mobile WAN interface.....	20
	Setting WAN failover and backup routing.....	20

Table of contents

	Routing parameters.....	21
	Configuring the network monitor.....	22
	Configuring DNS proxy.....	23
	Checking network status.....	23
Section 5	Serial port configuration.....	25
	Configuring serial ports.....	25
	Serial gateway.....	25
Section 6	Additional system configuration.....	27
	Changing passwords.....	27
	Setting date and time.....	27
	Restoring factory default settings.....	28
	Updating the firmware.....	28
	Saving configuration profiles.....	28
Section 7	Service configuration.....	31
	Configuring services.....	31
	Service parameters.....	31
Section 8	Troubleshooting.....	35
	Common troubleshooting issues.....	35
	Viewing the system log.....	36
Section 9	Technical data.....	37
Section 10	Glossary.....	41

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 abb.com/mediumvoltage.

1.3.2 Document revision history

Document revision/date	Product version	History
A/2017-09-22	3.4	First release
B/2019-04-24	3.4.7	Content updated to correspond to the product version
C/2020-07-09	3.4.7	Content updated
D/2021-05-31	3.4.7	Content updated
E/2021-12-10	3.4.7	Content updated



Download the latest documents from the ABB Web site
abb.com/mediumvoltage.

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 abb.com/mediumvoltage.

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

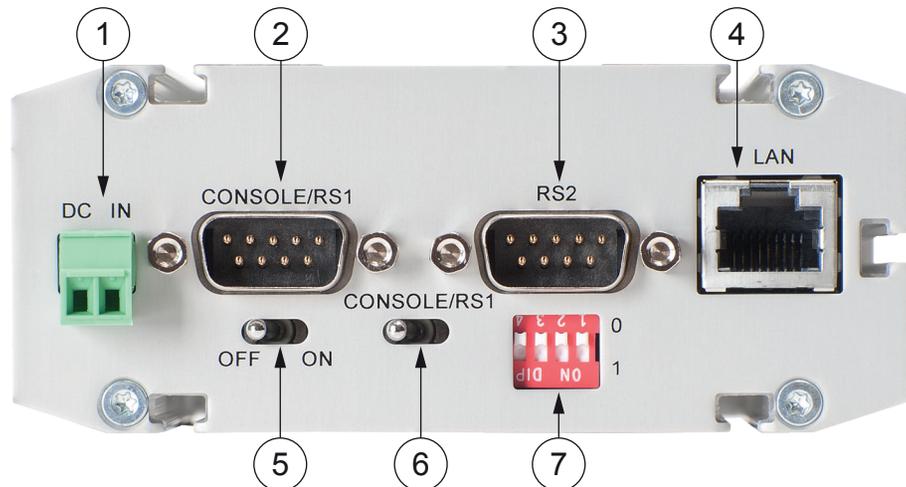


Figure 1: Front panel

- 1 Power supply 12...48 VDC, limited (<240 VA) power source that fulfills the requirements of standard IEC 60950-1
- 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.

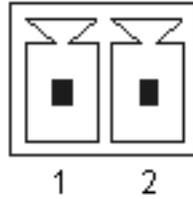


Figure 2: Power supply connector

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 (RS2) mode and settings (RS-232 or RS-485). By default, all DIP switches are set to the 0 position (RS-232 mode). DIP switches 2...4 apply only when DIP switch 1 is set to differential mode (RS-485/RS-422).

Table 1: *DIP switches*

DIP switch	Mode	State	Description
1	RS-232 or differential	0 = RS-232, 1 = RS-485 and RS-422	Selects the serial port operation mode
2	DUPLEX	0 = FULL, 1 = HALF	Selects between RS-422 full-duplex (4-wire) and RS-485 half-duplex (2-wire) differential modes
3	BIASING	0 = OFF, 1 = ON	Enables RS-422 biasing on pins 2 and 8
4	TERMINATION	0 = OFF, 1 = ON	Enables RS-422 termination on pins 2 and 8



If biasing and/or termination is required for the RS-485 half-duplex (2-wire) mode, enable RS-422 biasing/termination with DIP switches and manually connect pins 2-7 and 3-8 together at the application port (RS-2).

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.

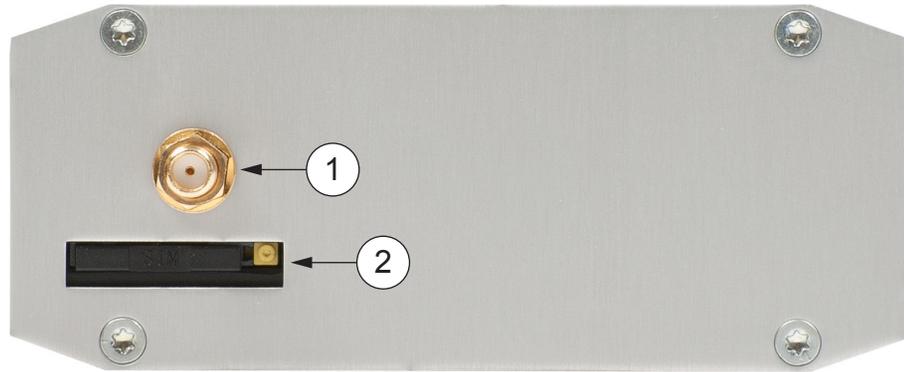


Figure 3: Back panel

- 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.

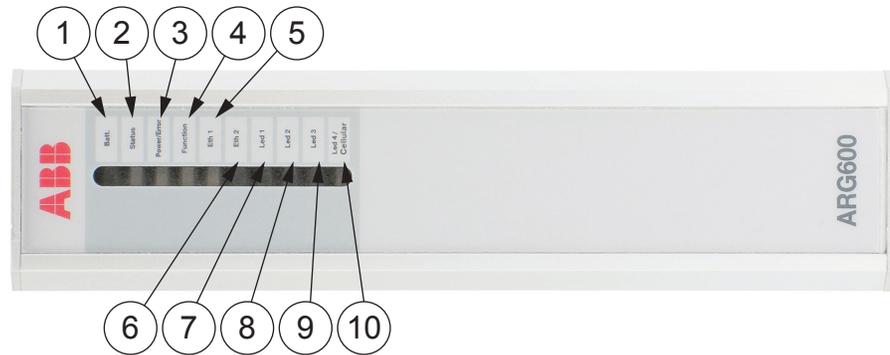


Figure 4: LEDs

- 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

Table continues on next page

LED	Label	State	Description
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
9	Led 2	-	LED reserved for future use
10	Cellular	On	This LED is controlled by the internal communication module logic. For more information, see Tools/Modem info on the Web HMI.
		Flashing	This LED is controlled by the internal communication module logic. For more information, see Tools/Modem info on the Web HMI.
		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 Getting started

3.1 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.

3.1.1 Connection principle

The device has configurable network interfaces.

- Ethernet LAN/WAN port
- Mobile WAN cellular interface

The device supports cellular connectivity (2G, 3G, LTE) allowing the use of wireless applications. 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.

3.2 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 **Home Page** opens.

3.2.1 User interface

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

3.3 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.

If the functional mode of the Ethernet port is set to "WAN" or "VLAN", the following details must be noted. Before changing the Ethernet port mode to "WAN", the firewall

configuration needs to allow Web UI and SSH access from WAN (**Firewall/General** and enable both *Allow WebUI access from WAN* and *Allow SSH access from WAN*). The VLAN functional mode of the Ethernet port requires an external VLAN switch.

3.4 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.

3.5 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 4 Network configuration

4.1 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.

4.2 Configuring communication interfaces

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.3 Routing parameters

The device has multiple configuration options that define routing.

Table 3: *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.

4.4 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.

4.5 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.

4.6 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 5 Serial port configuration

5.1 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

5.2 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 6 Additional system configuration

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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 7 Service configuration

7.1 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.

7.2 Service parameters

Table 4: 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 machines on LAN to find the device using its hostname. By default, the device uses its hostname (for example, 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 5: *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 6: *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 7: *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 8: *Arctic Patrol*

Name	Description	Value range
Basic Information		
Enabled	Enables Viola Patrol	No, Yes
Name	Free-text field for the unique name of the Patrol connection	
Registration password	Password needed to register to server with HTTPS protocol. This password should not be entered after registration unless re-registering is necessary.	
Protocol	Patrol communication protocol	HTTPS, SSH
Connection interval	Defines how often to report to server	Seconds
Server Information		
Server address, server port	Server IP address and the port the server listens. If no value is given, the value is 10000.	
SSH Settings (Only needed for SSH protocol)		

Table continues on next page

Name	Description	Value range
SSH local identity	SSH private key to be used if the SSH connection protocol is selected.	
SSH public key	SSH public key to be used if the SSH connection protocol is selected. This key can be copied to Patrol server.	
Remote identity	SSH public key of the Patrol server	
Connection mode	The connection mode defines how the Patrol server polls the clients in the SSH protocol mode. In case of a large number of Patrol connections in the server, the polling mode is recommended.	Polling, continuous
Options		
Backup active configuration to server	When set to "Yes", copies encrypted version of the XML configuration file to the server.	No, Yes
Allow remote management	Enables remote management by Patrol server	No, Yes
Allow LAN device scan	Allows periodical local network scan for ABB devices. Currently, the supported device is RIO600.	No, Yes

Section 8 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.

8.1 Common troubleshooting issues

Table 9: 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: <ol style="list-style-type: none"> 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.

8.2 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 9 Technical data



Technical specifications can be changed without notification. For information on the supported mobile data speed, see the mobile data reference guide.

Table 10: *Dimensions*

Description	Value
Width × Height × Depth	108 × 45 × 175 mm (without antenna)
Weight	510 g

Table 11: *Hardware*

Description		Value
Processor environment	Processor	32 bit RISC
	Memory	128 MB Flash 128 MB RAM
Power	Power supply	12...48 VDC, limited (<240 VA) power source that fulfills the requirements of standard IEC 60950-1
	Power consumption	1...5 W
Other	Internal clock	Real time
Approvals		CE and FCC
Environmental conditions	Temperature range	-30...+70°C (operating)
		-40...+85°C (storage)
	Humidity	5...85% RH (non condensing)
	Protection class	IP30

Table 12: *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 13: 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
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
	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 14: *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 15: *RoHS and REACH compliancy*

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

Table 16: *FCC compliancy*

Description	Reference
Standard	FCC 47 CFR FCC Part 15
	ANSI C63.4-2014

Section 10 Glossary

CHAP	Challenge handshake authentication protocol
CTS	Clear to send
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
DIP switch	A set of on-off switches arranged in a standard 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
DTE	Data Terminal Equipment
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
HTTPS	Hypertext Transfer Protocol Secure
LAN	Local area network
LED	Light-emitting diode
NTP	Network time protocol
PAP	Password authentication protocol
RAM	Random access memory
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
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
VPN	Virtual Private Network
WAN	Wide area network



ABB Distribution Solutions

P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11

ABB Inc.

305 Gregson Dr.
Cary, NC 27511, USA

abb.com/mediumvoltage
abb.com/contacts