



Arctic IEC-104 Gateway User's Manual

Arctic IEC-104 Gateway (2205)



Firmware Version 5.0.9
Document Version 1.5
September 2010

Copyright and Trademark

Copyright © 2008-2010, Viola Systems Ltd. All rights to this manual are owned solely by Viola Systems Ltd. (referred elsewhere in this User's Manual as Viola Systems). All rights reserved. No part of this manual may be transmitted or reproduced in any form or by any means without a prior written permission from Viola Systems.

Ethernet™ is a trademark of XEROX Corporation. Windows™ and Internet Explorer™ are trademarks of Microsoft Corporation. Netscape™ is a trademark of Netscape Communications Corporation. All other product names mentioned in this manual are the property of their respective owners, whose rights regarding the trademarks are acknowledged.

Viola Systems Ltd.

Lemminkäisenkatu 14-18 A

FI-20520 Turku

Finland

E-mail: info@violasystems.com

Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: <http://www.violasystems.com>

Disclaimer

Viola Systems reserves the right to change the technical specifications or functions of its products or to discontinue the manufacture of any of its products or to discontinue the support of any of its products without any written announcement and urges its customers to ensure that the information at their disposal is valid.

Viola software and programs are delivered "as is". The manufacturer does not grant any kind of warranty including guarantees on suitability and applicability to a certain application. Under no circumstance is the manufacturer or the developer of a program responsible for any damage possibly caused by the use of a program. The names of the programs as well as all copyrights relating to the programs are the sole property of Viola Systems. Any transfer, licensing to a third party, leasing, renting, transportation, copying, editing, translating, modifying into another programming language or reverse engineering for any intent is forbidden without the written consent of Viola Systems.

Viola Systems has attempted to verify that the information in this manual is correct with regard to the state of products and software on the publication date of the manual. We assume no responsibility for possible errors which may appear in this manual. Information in this manual may change without prior notice from Viola Systems.

Declaration of Conformity

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name: Viola Systems Ltd.

Manufacturer's Address:

Lemminkäisenkatu 14-18 A

FI-20520 Turku

Finland

declares that this product:

Product Name:

Arctic IEC-104 Gateway

conforms to the following standards:

EMC:

EN 55022 Emission Test (Class A)

1. Radiated Emissions (30-1000MHz)
2. Conducted Emissions (0.15-30MHz)

EN 50082-1 Immunity Test

1. IEC 801-3: Radio Frequency Electromagnetic Field
2. IEC 801-2: Electrostatic Discharge
3. IEC 801-4: Fast Transients, AC Power Ports and Signal cables

Supplementary Information:

"The product complies with the requirements of the Low Voltage Directive 73/23/EEC and EMC directive 89/336/EEC."



Warning!

This is a Class A product. In a domestic environment this product may cause radio Interference which may make it necessary for the user to take adequate measures.

Manufacturer's Contact Information:

Viola Systems Ltd.

Lemminkäisenkatu 14-18 A

FI-20520 Turku

Finland

Phone: +358 20 1226 226

Fax: +358 20 1226 220

Warranty and Safety Instructions

Read these safety instructions carefully before using the products mentioned in this manual:

Warranty will be void if the product is used in any way in contradiction with the instructions given in this manual or if the product has been tampered with.

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.

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. Before connecting any power cables the output voltage of the power supply should be checked.

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 Viola Systems manufactured hardware or software could lead directly to death, personal injury, or severe physical or environmental damage.

Revisions

Date	Document Version	Firmware Version	Description of changes
09/2010	1.5	5.0.9	New manual and lay-out.

Contents

COPYRIGHT AND TRADEMARK	2
DISCLAIMER.....	3
DECLARATION OF CONFORMITY.....	4
WARRANTY AND SAFETY INSTRUCTIONS.....	5
REVISIONS.....	6
1. INTRODUCTION.....	9
1.1 About this User's Manual.....	9
1.2 The Arctic Platform.....	9
2. PHYSICAL INTERFACES.....	11
2.1 Front Panel Description.....	11
2.2 Back Panel Description.....	14
2.3 Side Panel Description.....	15
2.4 Product Information Label	16
2.5 Firmware Version.....	17
3. GETTING STARTED.....	18
3.1 Unpacking the Arctic	18
3.2 Installation of the Arctic.....	18
3.3 Setting of the IP Address Using an HTML Browser.....	18
3.4 Setting of the IP Address Using a Console.....	20
4. ARCTIC CONFIGURATOR TOOL.....	23
4.1 Login to Arctic Configurator.....	23
4.2 General Usage of the Arctic Configurator.....	24
5. ARCTIC SOFTWARE CONFIGURATION.....	25
5.1 System Menu.....	25
5.2 Network Menu.....	25
5.2.1 Ethernet.....	26
5.2.2 GPRS.....	27
5.2.3 Dial-in.....	28
5.2.4 SSH-VPN.....	28
5.2.5 L2TP-VPN.....	30
5.2.6 GRE.....	31
5.2.7 Monitor.....	32
5.2.8 Routing.....	33
5.2.9 S-NAT.....	33
5.2.10 D-NAT.....	33
5.2.11 DNS Update.....	33
5.2.12 DynDNS Client.....	34
5.2.13 NTP Client.....	35
5.2.14 SMS Config.....	35
5.3 Firewall Menu.....	36
5.4 Service Menu.....	38
5.4.1 WWW.....	38
5.4.2 SSH.....	38

5.4.3	Telnet.....	38
5.4.4	DHCP	39
5.5	Application Menu.....	40
5.6	Tools Menu.....	41
6.	GPRS.....	42
6.1	Placing Arctic.....	42
6.2	GPRS Antenna.....	42
6.3	SIM Card and Card Holder.....	43
6.4	Configuring Arctic's GPRS Settings.....	43
6.5	Useful GSM/GPRS Information.....	44
7.	IEC-104 APPLICATION SETTINGS.....	46
7.1	General settings.....	46
7.2	Serial settings.....	47
7.3	Network settings.....	48
7.4	IEC-104 Settings.....	50
7.5	IEC-101 settings.....	53
7.6	ASDU Converter.....	56
7.7	Packet collector.....	57
7.8	IO extension.....	59
7.9	Other settings.....	59
8.	IEC-104 IO APPLICATION SETTINGS.....	60
9.	TROUBLESHOOTING.....	61
9.1	Common Problems.....	61
	SPECIFICATIONS	62
	LIMITED WARRANTY.....	64
	TECHNICAL SUPPORT	65

1 Introduction

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

1.1 About this User's Manual

This User's Manual describes the operation of the Arctic IEC-104 Gateway products. All devices in this User's Manual are referred to as Arctic, unless otherwise mentioned. This manual provides introductory information as well as detailed instructions on how to set up and manage the Arctic as part of a network environment. It is intended for anyone involved in installing and managing Arctic devices. It is assumed that the reader of this manual is familiar with basic working principles of Internet technology.

Figure 1. Arctic IEC-104 Gateway



1.2 The Arctic Platform

The Arctic platform utilizes a number of wireless or fixed line interfaces depending on your specific requirements. Arctic is a customizable technology allowing users to develop solutions for their own applications. Arctic devices have been designed to withstand the requirements of extreme environments and industrial use.

Technical Features Summary

The following are the functional components in the Arctic IEC-104 Gateway device.

Details of the each components are listed below:

HARDWARE

CPU Platform:

- 32-bit RISC microcontroller
- 32 MB RAM
- 8 MB Solid state FLASH memory

Network Interface:

- 10/100 Base-T Ethernet (RJ45)

Device Interface:

- 2 Serial ports (RS-232, RS-485)

Mechanics:

- Aluminum frame
- Attachment rail for optional and custom mounting tools

SOFTWARE

Operating System:

- Multitasking embedded μ CLinux

Supported Protocols:

- PPP, IP, ICMP, UDP, TCP, ARP, DNS, DHCP, FTP, TFTP, HTTP

Application Services:

- HTTP server, CGI
- FTP client
- Telnet server
- SSH server and client
- Temperature sensor
- Real Time Clock
- Syslog
- DHCP server and client
- Status querying using SMS
- Serial connection (Serial GW)
- IEC-104 communications

Management and Configuration:

- Web user interface
- Console port
- Telnet

2 Physical Interfaces

The Arctic unit contains three panels for interface connections and status indication. These panels are:

1. Front panel:

The front panel configuration is shown in figure 2. This panel includes all connectors and switches for the device operation, optional input/output connectors and the connectors for network and serial interface.

2. Back panel:

The GPRS antenna connector and SIM card holder are shown in figure 6.

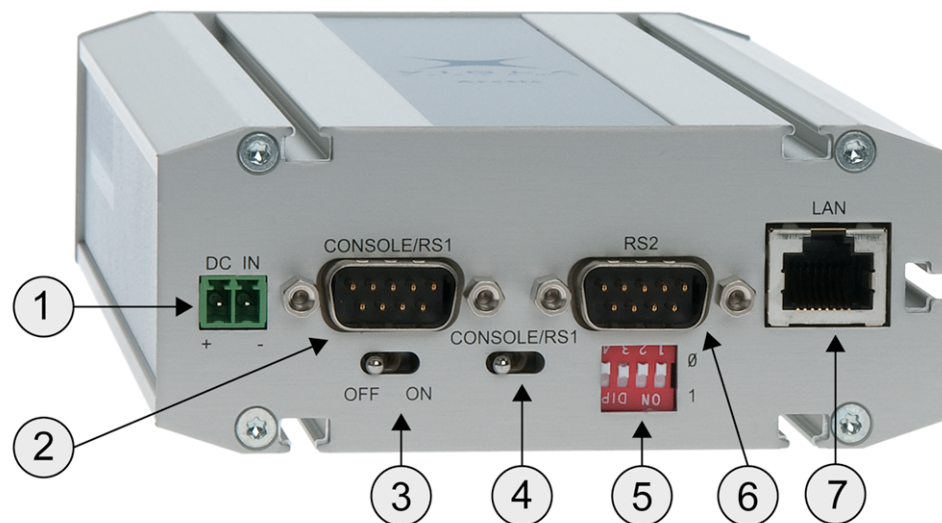
3. Side panel:

The side panel as shown in figure 7 contains all LEDs which indicate the status of the device.

2.1 Front Panel Description

The front panel of the Arctic GPRS consists of the following connectors and switches:

Figure 2. Front Panel Description



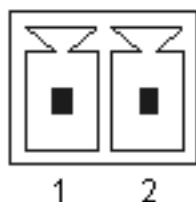
1. Power supply connector
2. Console serial port (RS1)
3. Power switch
4. Console switch
5. DIP switches
6. Application serial port (RS2)
7. Ethernet connector

The Arctic has rails to enable wall or rack mounting. The front panel contains slots for nuts or other mounting accessories (optional) in order to gain access to these rails.

Power Supply Connector

The Arctic has a 10 – 26 VDC power supply connector as shown in Figure 3.

Figure 3. Power supply connector



- Pin 1 is positive (+)
- Pin 2 is negative (-)

The unit is protected against reversed polarity.

Power Switch

Enables or disables the operation of the Arctic.

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

It selects 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

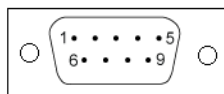
Number	Function	State	Explanation
1	RS-232/RS-485	"0" = RS-232 "1" = RS-485	Selects RS-port operation
2	HALF/FULL	"0" = full "1" = half	Selects between half-duplex (2-wire) and full-duplex (4-wire)
3	BIAS	"0" = OFF "1" = ON	RS-485 biasing
4	TERMINATION	"0" = OFF "1" = ON	RS-485 termination

Serial Ports (RS-232, RS-422/485 -connectors)

Arctic has two serial port connectors. These are 9-pin male connectors (DB9). A null modem cable may be used to connect the Arctic to a serial device or

a PC. The Arctic supports CTS/RTS flow control. The figure of Arctic's DB9 (DTE) Male connector is shown in Figure 4:

Figure 4. DB9 male connector



The serial port 1 (RS1) is a full RS-232 port. The pin description of this port is as follows:

Table 2: RS-232 Port PIN Description

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

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

Table 3: RS-485 Port PIN Description

Pin Number	RS-485,Full duplex (4-wire)	RS-485 Half duplex (2-wire)
1	NC	NC
2	RXD+ (in)	NC
3	TXD-(out)	TXD/RXD- (out/in)
4	NC	NC
5	GND	GND
6	NC	NC
7	TXD+ (out)	TXD/RXD+ (out/in)
8	RXD-(in)	NC
9	NC	NC

Note!

Make sure that you DO NOT connect RS-422 or RS-485 devices to a port which has been configured to operate as an RS-232 port.

Ethernet Connector

Arctic has an RJ45 connector for 10/100 Mbps Ethernet connection. Maximum length of the Ethernet cable is 100m.

Note!

The cross-connected cable is only for connecting the Arctic to the PC's network interface card. When connecting to a local network (e.g. hub or switch), a direct Ethernet cable must be used.

The figure and pin description of the Arctic's RJ45 Ethernet connector is as follows:

Figure 5. RJ45 Ethernet connector

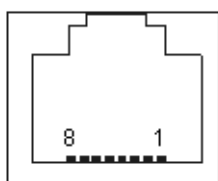


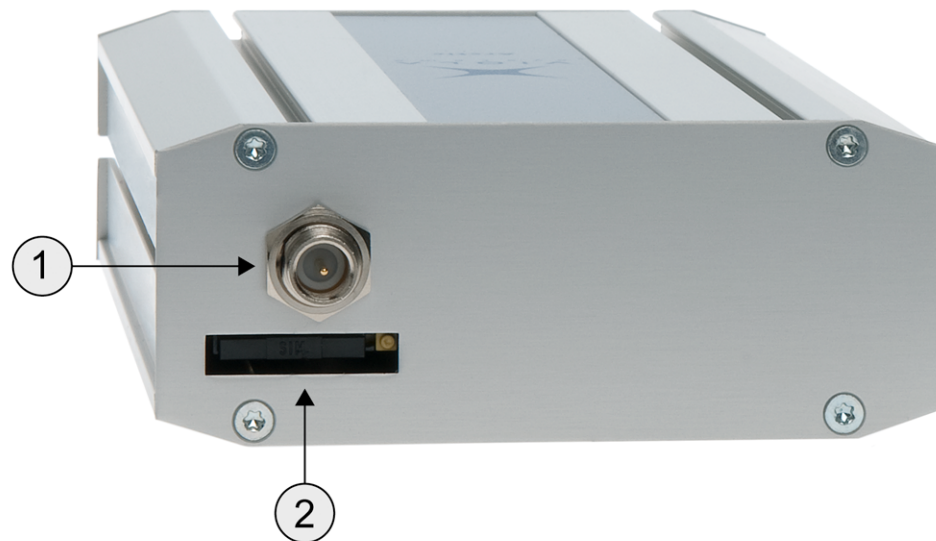
Table 4: RJ45 Ethernet connector PIN Description

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

2.2 Back Panel Description

The Arctic IEC-104 Gateway has an antenna connector and a slot for a SIM card on the back panel.

Figure 6. Back Panel



1. FME connector for an antenna.
2. SIM Card slot.

Note!

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

2.3 Side Panel Description

The side panel of the device contains ten LEDs which are used to indicate the status of the Arctic and only five of them are connected. The LEDs are numbered from 1 to 10 starting from the rear panel side. A detailed description of each LED is listed below:

Figure 7. LED Description

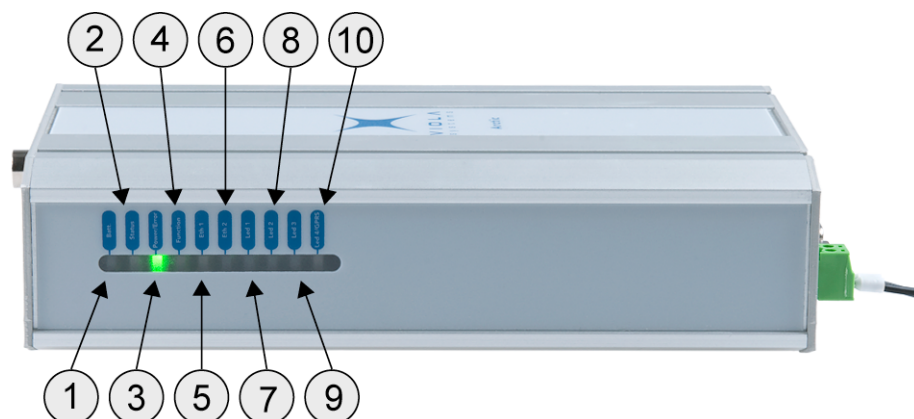


Table 5: LED Description

LED Number	LED	State	Description
1	Battery		Not connected
2	VPN	ON Blinking OFF	VPN connection is up VPN onnection is starting VPN connection is disabled
3	Power/Error	ON OFF	Operating power is turned on Operating power is turned off
4	System Function	ON Blinking	Device is starting Device is operating normally
5	Eth 1	ON Blinking OFF	Ethernet link is up Ethernet link is transferring data Ethernet link is down
6	Eth 2		Not connected
7	LED 1		Not connected
8	LED 2		Not connected
9	LED 3		Not connected
10	LED 4/GPRS	Blinking OFF	GPRS is starting or transferring data GPRS is inactive

2.4 Product Information Label

The product information label on the underside of the Arctic contains the following information:

1. Product type
2. Serial number
3. MAC address

The Ethernet address (MAC address) of the unit is printed on the product label (Figure 7). Each address code starts with the digits "00:06:70", but the remaining six digits are unique for each unit.

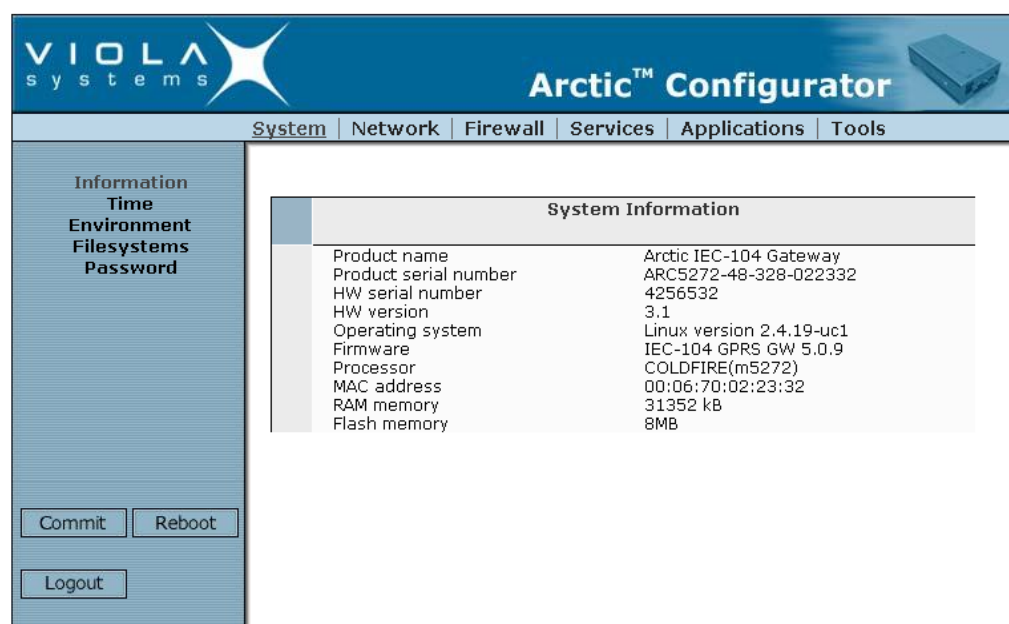
Figure 8. Product Information Label



2.5 Firmware Version

The Arctic firmware version may be checked from the Viola Configurator startup page (System -> Information). It is also possible to get the firmware version by issuing command *firmware* in console.

Figure 9. Firmware Version



This manual describes the series 5 firmware version IEC-104 GPRS GW 5.0.9.

3 Getting Started

3.1 Unpacking the Arctic

Arctic is delivered in a bulk package containing only the device itself.

A separate Arctic Accessory Kit (ordered separately) contains the following items:

- Power supply and cable
- Cross-over Ethernet Cable
- Null modem cable

If any of the items are missing or damaged, please contact Viola Systems Ltd. All packaging materials are recyclable. Viola Systems urges its customers to follow environmental regulations regarding the disposal of all the materials.

3.2 Installation of the Arctic

The Arctic can be installed horizontally on a flat surface e.g. on a desk or a rack.

When installing Arctic models with wireless connectivity options, it should be remembered that high-frequency radio waves need to be taken into account. The surrounding environment affects the range of radio signals. Therefore, if you are using an Arctic with antennas directly mounted to the antenna connector, try to avoid placing the Arctic where the radio signal might be disturbed ("shadowed") by nearby obstacles. Also large metallic surfaces (racks) may have a highly detrimental effect on the antenna performance. In case of metal racks or surfaces, it is recommended to use an external antenna with an appropriately selected cable. By following these precautions, the Arctic may be installed more freely.

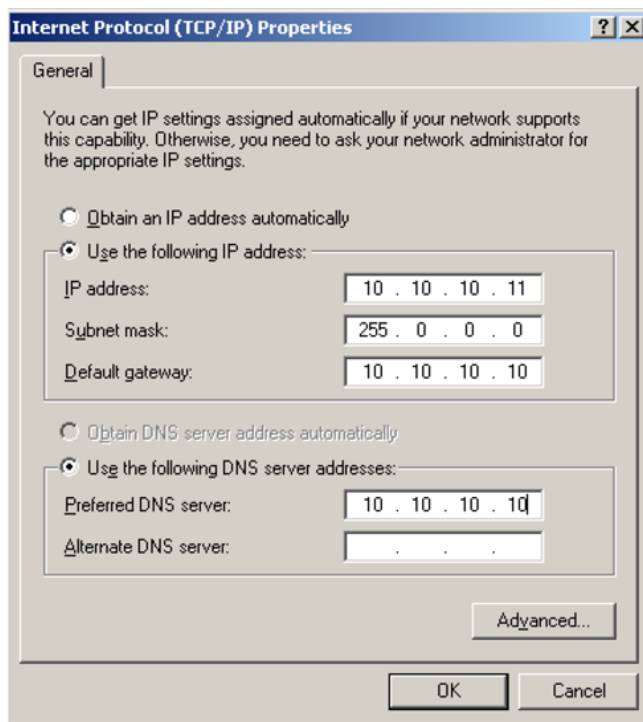
The aluminum case of the Arctic contains rails for wall mounting. Both broad sides contain two rails and the narrow side opposite to the LED panel contains one rail. These rails allow a flexible selection of the optimum mounting direction. To mount the Arctic on a wall using optionally available mounting tools can be used.

3.3 Setting of the IP Address Using an HTML Browser

This is the recommendable way to set up the network parameters. It is an easy-to-apply solution if the computer used for configuration has been properly configured. Follow the procedure listed below:

1. Connect to the Arctic using your HTML browser. The default IP address of the Arctic is "10.10.10.10" (netmask "255.0.0.0"). Computer connected to Viola Arctic device can use for example IP address 10.10.10.11.

Figure 10. IP Properties



2. From the initial page, click **Start Configurator** and enter login information in the following page. Username is *root* and by default no password is set (just leave the field empty).

3. Navigate to Network -> Ethernet page.

Figure 11. Ethernet Settings

The screenshot shows the 'Arctic Configurator' web interface. The top navigation bar includes 'System', 'Network', 'Firewall', 'Services', 'Applications', and 'Tools'. The 'Network' tab is selected. On the left, a sidebar lists various configuration options: Summary, Ethernet, GPRS, Dial-in, SSH-VPN, L2TP-VPN, GRE tunnel, Monitor, Routing, S-NAT, D-NAT, DNS Update, DynDNS client, NTP client, and SMS Config. The 'Ethernet' option is highlighted. The main content area is titled 'Ethernet Settings' and contains the following fields and values:

Field	Value
Override Ethernet configuration by DHCP?	<input checked="" type="radio"/> Enabled
Host name	ViolaArctic
Domain name	(none)
Ethernet IP address	10.10.10.10
Network mask	255.0.0.0
Use Ethernet as default route (usually No)	Yes
Default router IP address	10.10.10.1
MTU	1500
DNS servers (optional)	212.83.96.242 212.83.96.250
MAC address	00:06:70:02:1D:77

At the bottom of the form are 'Apply' and 'Reset' buttons.

4. Enter the Ethernet IP address (and other network settings) of your choice and click Apply and then Commit (on bottom of page) to store the settings.
5. Reboot the Arctic for the settings to take effect.

Note!

Arctic default password is *empty*. Remember to set the password before connecting the Arctic device to a public network (Chapter 5).

3.4 Setting of the IP Address Using a Console

Before installation, you need to find out the required network settings. These include the **IP Address**, **Netmask** and **Gateway Settings** used by the Arctic. The local network administrator can provide them to you or you can ask for them from your Internet Service Provider.

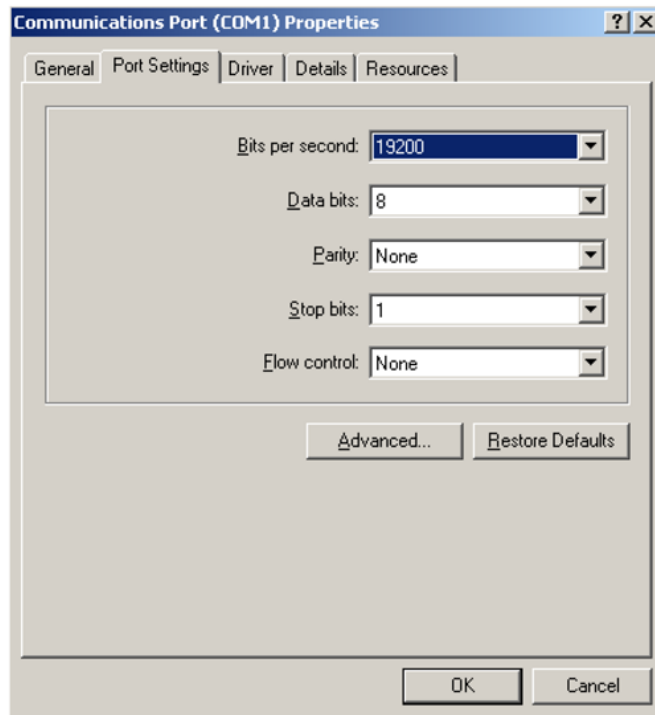
Note!

If possible, it is recommended to use an HTML browser to set up network settings as described in the next chapter. If using a console, please follow the procedure below:

1. Before you start, turn off the power from all devices and check that the power switch of the Arctic is in the "OFF" position.
2. Connect a serial cable (crossover) to the console serial port (RS1) and an Ethernet cable to the RJ45 connector.
3. Switch the Arctic on by toggling the power switch to "ON" position.

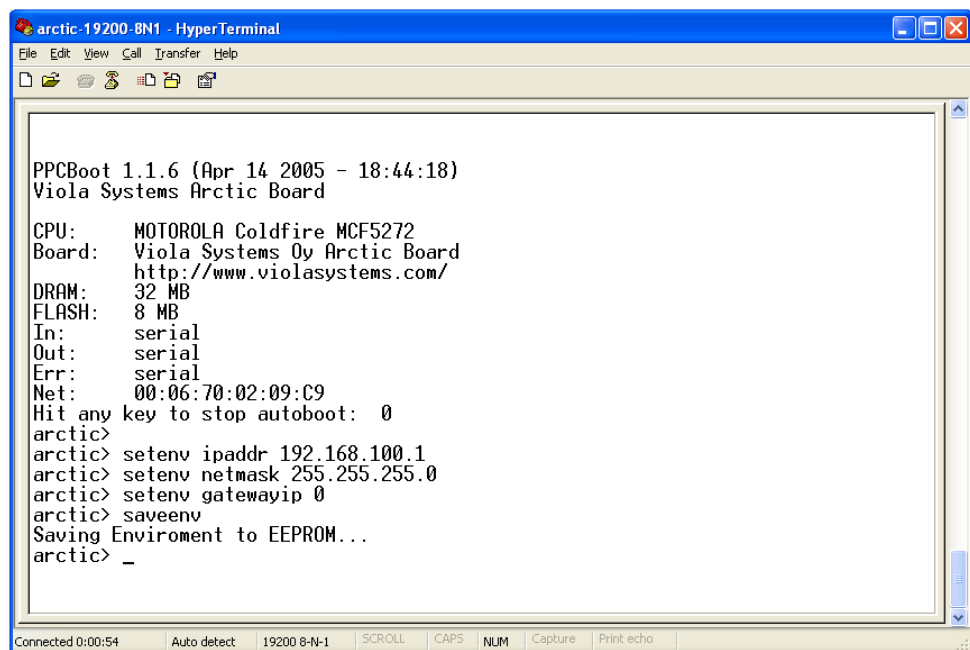
4. Connect to Arctic using COM port and terminal program (Hyperterminal). Serial settings for console (RS1) are 19200-8-N-1 and "Flow control set to none".

Figure 12. COM1 Properties



5. Stop the PPCboot to get the "Arctic>" command prompt. Set the IP address and netmask using command "setenv".

Figure 13. Arctic COM1 Hyperterminal



6. Save the setting with command “saveenv”.
7. Reboot the Arctic for the settings to take effect.

Note!

Default gateway value (gatewayip) is usually set to zero (0) because GPRS or VPN is used as default router.

4 Arctic Configurator Tool

The Arctic Configurator is a tool which allows the user to manage the properties of the Arctic device by using a user-friendly, www-based interface. You only need a computer with an HTML browser and a working connection to the Arctic to be able to use the web configurator.

With the Arctic Configurator, you can set important parameters, receive status information, and set variables that control which applications and processes run on the Arctic board.

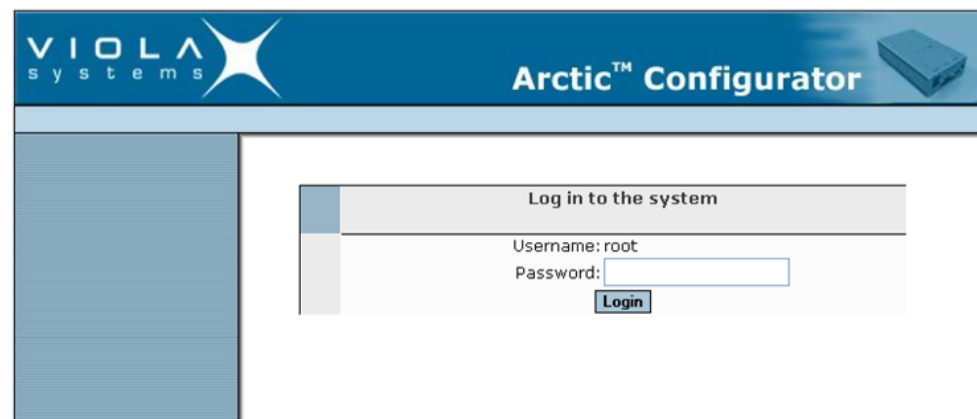
4.1 Login to Arctic Configurator

To start using the Arctic Configurator, open the URL where the Arctic is located and it has to be configured. On the Viola Arctic main page, select the **Start Configurator** link.

Figure 14. Start Configurator



Figure 15. System Log-in



Initially, the Arctic Configurator will ask you for the password for the Arctic device root-account. Enter the correct password in the box provided and press the login-button to start the Arctic Configurator.

Note!

Default password for root is empty. Remember to set the password before connecting the device to a public network. Password can be changed from System -> Password menu (Chapter 5).

4.2 General Usage of the Arctic Configurator

After a successful login, the Arctic Configurator will display the main screen. This consists of the main navigation menu on the top, the secondary navigation bar on the left, and the main screen containing the currently active content and controls.

When the program starts for the first time, the System/Information screen will be shown in the main content area. The main navigation-menu on the top of the screen is used to navigate between the different subsets of settings available. Selecting an item from the main menu will display the available items related to this subset in the secondary navigation bar, selecting the first of these to be shown in the main content area.

The secondary navigation-bar on the left contains the groups of parameters in this subset. Selecting an item from this menu will display the content related to the selected group in the main content area. In the bottom of the secondary navigation-bar is a group of three buttons which are always visible: **Commit**, **Reboot** and **Logout**. The Commit-button is used to save the memory-resident data for "soft" parameters permanently to non-volatile memory. Note that the values for the previous parameters are not saved to non-volatile memory unless the Commit-button is pressed. The Reboot-button, as the name suggests, will reboot the Arctic. The Logout button will end the current session and return to the login-screen.

5 Arctic Software Configuration

5.1 System Menu

The System-menu contains items that are relevant to the Arctic board itself. It allows the user to view information about the system or the current executing environment and to set the date and time.

Information – submenu contains general information about the Arctic device. Information on this submenu should be provided if possible when contacting Viola Systems technical support.

Time – submenu contains time information. Arctic has a real time clock with battery backup and time information may be adjusted here.

Note!

Updated time data is not saved permanently until the **Commit** button is pressed. Until then, it will be stored only in RAM memory.

Environment – submenu contains information about the Arctic device memory usage, uptime and inside temperature.

Password – submenu contains password changing. The default password is blank. When changing the password for the first time, the same password has to be written in all three boxes.

5.2 Network Menu

Through the Network-menu you can access sub items to control the various network interface properties. The menu contains items for Ethernet, VPN and GPRS interfaces. Also Email, Proxy and firewall settings are located in this submenu. The **Network Interface Summary page** shows which interfaces are up and also routing information:

Figure 16. Network Interface Summary

Arctic™ Configurator

System | **Network** | Firewall | Services | Applications | Tools

Summary
Ethernet
GPRS
Dial-in
SSH-VPN
L2TP-VPN
GRE tunnel
Monitor
Routing
S-NAT
D-NAT
DNS Update
DynDNS client
NTP client
SMS Config

Network Interface Summary

Ethernet (eth0)

HW address	00:06:70:02:1D:77
Internet address	10.10.10.10
Status	UP BROADCAST RUNNING MULTICAST
Rx packets	116
Tx packets	105

Loopback (lo)

Internet address	127.0.0.1
Status	UP LOOPBACK RUNNING
Rx packets	0
Tx packets	0

Running Routes

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

Running ARP cache

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

Commit Reboot

Logout

5.2.1 Ethernet

Configuration for the Arctic Ethernet Interface:

Figure 17. Ethernet Settings

Arctic™ Configurator

System | **Network** | Firewall | Services | Applications | Tools

Summary
Ethernet
GPRS
Dial-in
SSH-VPN
L2TP-VPN
GRE tunnel
Monitor
Routing
S-NAT
D-NAT
DNS Update
DynDNS client
NTP client
SMS Config

Ethernet Settings

Override Ethernet configuration by DHCP? ☐ Enabled ☒ Disabled

Host name: ViolaArctic

Domain name: (none)

Ethernet IP address: 10.10.10.10

Network mask: 255.0.0.0

Use Ethernet as default route (usually No): Yes

Default router IP address: 10.10.10.1

MTU: 1500

DNS servers (optional): 212.83.96.242, 212.83.96.250

MAC address: 00:06:70:02:1D:77

Apply Reset

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

Host name – Sets the Arctic device hostname. This is important to set up correctly when using a Viola M2M Gateway and VPN.

Every Arctic connected to Viola M2M Gateway must have unique hostname.

Domain name – Domain name for name resolution (optional).

Ethernet IP address – IP address used by *eth0* interface.

Network mask – Network mask used by *eth0* interface.

Use Ethernet as default route – Set this to “Yes” only when using Ethernet as default gateway/router. This parameter overrides next parameter “Default Route IP Address”, so as long this parameter is set to no, next parameter has no affect. Usually this is set to “No”, because either GPRS or VPN is used as default route.

Default Router IP address – Default router (or default gateway) used when the direct route to host or network is not known. This parameter applies to *eth0* interface only. When GPRS or VPN is used as default gateway this parameter has to be set to 0.

MTU – MTU for Ethernet interface (usually 1500).

DNS servers (optional) – Name server IP (DSN) address for resolving host names to IP address and vice versa.

Applicable when GPRS parameter “DNS servers” is set to “User defined”.

5.2.2 GPRS

GPRS settings include APN and other settings for GPRS network connectivity. More details of GPRS connectivity is in Chapter *GPRS*.

GPRS enabled – When set to yes, GPRS interface is automatically attached to GPRS network.

Access Point Name (GPRS) – GPRS Access Point (APN) name where the connection is made.

PIN code – SIM card pin code.

Operator Code (empty=auto) – A manually selected operator code. Leave empty for automatic network selection. The default value is empty.

DNS servers – When set to “User defined”, DNS servers from Ethernet page are used. If the parameter is set to “From GPRS network” Arctic receives DNS server IPs automatically from GPRS network.

Led indication – In Data only mode, GPRS LED blinks green when transmitting data. In Informative mode, LED blinks also when connected to GPRS network without data transfer (GPRS context is active).

GPRS username – Username used for authentication if APN requires it.

GPRS password – Password used for authentication if APN requires it.

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

Maximum MTU value – MTU (Maximum transfer unit) for GPRS.

Use GPRS as default route – If enabled, GPRS is used as default route. Ethernet default gateway has to be disabled (Parameter “Use Ethernet as default route” set to “No” in Network -> Ethernet).

Figure 18. GPRS Settings

VIOLA
systems

Arctic™ Configurator

System | **Network** | Firewall | Services | Applications | Tools

GPRS Settings

GPRS enabled	No
Access Point Name (GPRS)	INTERNET
PIN code	NoPin
Operator Code (empty=auto)	
DNS servers	User defined
LED indication	Data only
GPRS username	username
GPRS password	passwd
PPP idle timeout (sec)	1800
Maximum MTU value	1500
Use GPRS as default route	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

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

Apply Reset

Commit Reboot

Logout

5.2.3 Dial-in

Configuration for the Arctic PPP dial-in Interface.

Dial-in enabled – When enabled, PPP connections can be made to Arctic (GSM data).

Require authentication (PAP) – When set to yes password authentication is used for incoming data calls.

Required username – PAP username allowed login.

Required password – PAP password used for authentication.

Idle timeout – Idle time before PPP connection is terminated.

Local IP address – IP address used in PPP peer.

Peer's IP address – IP address used in PPP peer.

Maximum MTU value – MTU (Maximum transfer unit) for Dial-in connections.

5.2.4 SSH-VPN

Arctic has a VPN client that can be used with the Viola M2M Gateway. For VPN configuration, please refer to the Viola M2M Gateway User's Manual.

Figure 19. SSH-VPN Settings

SSH-VPN Settings	
Use SSH-VPN?	No
Primary server	
Primary interface	GPRS
Primary server IP	127.0.0.1
Primary server port	22
Primary server GW	0
Max duration (0=unlimited)	0
Backup server (optional)	
Use backup SSH-VPN?	No
Backup interface	GPRS
Backup server IP	127.0.0.1
Backup server port	22
Backup server GW	0
Max duration (0=unlimited)	7200
Routing	
Routing mode	None
Remote network IP	0.0.0.0
Remote network mask	255.255.0.0
Link management	
MTU	1420
Idle timeout (sec)	3600
Hello interval (sec)	200
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Primary server

Use SSH-VPN? – When set to "Yes" Arctic automatically establishes SSH-VPN connection to primary Viola M2M Gateway.

Primary interface – Interface used to reach the Viola M2M Gateway server.

Primary server IP – IP address of Viola M2M Gateway SSH-VPN server.

Primary server port – SSH-VPN TCP port on primary server (default 22).

Primary server GW – If other gateway than default route is needed to reach the Viola M2M Gateway.

Max duration (0=unlimited) – Maximum duration of the VPN connection. On primary server, should be set to zero. With backup server, after this timeout, the primary server is tried again.

Connection start timeout (sec) – Time to wait for the connection establishment.

Connection retry interval (sec) – How often retry the connection.

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

Hello interval (sec) – Hello packet interval for the VPN. This can be used as a keepalive message on very critical links.

Hello failure limit – How many hello-packets can be lost before restarting the connection.

Backup server (optional)

Use backup SSH-VPN? – When set to "Yes", Arctic will try to establish VPN connection to backup Viola M2M Gateway, if the primary cannot be reached.

Primary failure limit – How many times primary must not be reached, before changing to secondary.

Other parameters are same as in primary server. The duration of the connection can be set for example to 3600 seconds, so after one hour connection time to backup server the secondary is tried to be reached.

Routing

Routing mode – Routing mode has three modes:

1. "Tunnel the following network" - This adds the "Remote network IP" to be reached via the SSH-VPN. Parameters "Remote network IP" and "Remote network mask" must be set.
2. "Default route" -> VPN interface is used as default route.
3. "None" -> No routing is added when the VPN is established. The VPN peer IPs can be used for communications.

Remote network IP – Remote network IP behind the VPN (on Viola M2M Gateway side) what is needed to be reached by Arctic.

Remote network mask – Netmask for remote network IP.

Link management

MTU – MTU for SSH-VPN interface.

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

5.2.5 L2TP-VPN

Arctic has a L2TP client that can be used with L2TP server.

Figure 20. L2TP-VPN Settings

L2TP-VPN Settings	
Use L2TP-VPN?	No <input type="button" value="v"/>
Primary server	
Primary interface	GPRS <input type="button" value="v"/>
Primary server IP	0.0.0.0
Primary server port	1701
Primary server gateway	0
Max duration (0=unlimited)	0
Hello interval (secs)	20
MTU	1420
L2TP username (usually hostname)	primary_user
L2TP password	pass
Backup server (optional)	
Use backup L2TP-VPN?	No <input type="button" value="v"/>
Backup interface	GPRS <input type="button" value="v"/>
Backup server IP	0.0.0.0
Backup server port	1701
Backup server gateway	0
Max duration (0=unlimited)	7200
Hello interval (secs)	20
MTU	1420
L2TP username (usually hostname)	backup_user
L2TP password	passwd
Routing	
Routing mode	None <input type="button" value="v"/>
Remote network IP	0.0.0.0
Remote network mask	255.255.0.0
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Use L2TP-VPN? – When set to "Yes", Arctic established L2TP VPN connection with primary Viola M2M Gateway.

Primary server

Primary interface – Interface used to reach the Viola M2M Gateway server.

Primary server IP – IP address of Viola M2M Gateway L2TP server.

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

Primary server gateway – If other gateway than default route is needed to reach the Viola M2M Gateway

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

Hello interval (secs) – Hello interval for connection keepalive (default 20 seconds).

MTU – MTU for L2TP interface

L2TP username – (usually hostname) - Username for authentication.

L2TP password – L2TP password for authentication.

Backup server

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

Routing mode

It is used if routing is needed with L2TP interface. Configuration parameters are same as in SSH-VPN.

5.2.6 GRE

GRE tunnel enabled – When set to "Yes", Arctic establish automatically GRE connection

Interface – Interface used to reach the GRE server

GRE server IP – IP address of GRE server

Gw to GRE server* – (ethernet mode) If other gateway than default route is needed to reach the GRE server.

Local GRE interface IP – (usually eth0 IP) - Local IP used in GRE tunnel

Remote GRE interface IP* – Remote IP used in GRE tunnel

TTL value – Time-to-live value for the interface

Checksum* – checksum value.

Incoming key* – authentication key.

Outgoing key* – Outgoing key for the server

Routing

Routing mode – same as in SSH-VPN and L2TP

Remote network* – same as in SSH-VPN and L2TP

Remote network mask* – same as in SSH-VPN and L2TP

*These are optional, please refer to your GRE server documentation

5.2.7 Monitor

Monitor is used for GPRS and VPN connection checking. If connection to the selected IP address is lost, the connection is restarted. Monitor uses ICMP echo (ping) packets to check the connection. The monitor also keeps the connection alive, so that idle timeout do not drop the connections.

ICMP Echo sending – Selects if the monitor is enabled.

This should be always enabled to correct IP.

Interval (sec) – Determines how often the connection is checked by sending ICMP echo packets. The interval should be smaller than GPRS idle timeout (typically max. 2/3 of GPRS idle timeout) in order to have uninterrupted communication.

Reply timeout (secs) – The waiting time for reply packets.

Retries – The number of tries before connections are restarted.

Target IP address – The host IP address to which echo packets are sent to.

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

Figure 21. Monitor Settings

The screenshot shows the 'Arctic™ Configurator' web interface. The top navigation bar includes 'System', 'Network', 'Firewall', 'Services', and 'Tools'. The left sidebar lists various configuration sections: Summary, Ethernet, GPRS, Dial-in, SSH-VPN, L2TP-VPN, GRE tunnel, Monitor (selected), Routing, S-NAT, D-NAT, DNS Update, DynDNS client, NTP client, and SMS Config. The main content area is titled 'Connection monitor settings' and contains the following fields:

Connection monitor settings	
ICMP Echo sending	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Interval (sec)	300
Reply timeout (secs)	20
Retries	3
Target IP address	0.0.0.0
Secondary target IP address (0=none)	0

At the bottom of the settings area are 'Apply' and 'Reset' buttons. The left sidebar also features 'Commit', 'Reboot', and 'Logout' buttons.

Note!

Monitor must be always enabled. When VPN is used, remote VPN peer IP (or other IP reached only via VPN) must be used for connection checking

5.2.8 Routing

5.2.9 S-NAT

These parameters are used to configure S-NAT (source network address translation) settings. When enabled, private IP address used in local LAN is changed to GPRS interface IP address.

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

5.2.10 D-NAT

These parameters are used to configure D-NAT (destination network address translation) settings. When enabled, packets coming to define GPRS interface port are forwarded to local IP address.

Source IP – D-NAT only connections coming from IP. Wildcard 0/0 means all IP addresses are D-NATted.

Protocol – Chooses which protocol is port forwarded. If “ANY” is chosen, other parameters are disregarded.

Dest.port – Chooses which GPRS interface is port forwarded to local Ethernet.

Redirect to IP – Chooses where port forwarding is done to.

Redir. port – Chooses which port forwarding goes to.

5.2.11 DNS Update

These parameters are used to configure dynamic DNS. Arctic can report its dynamic IP address to a DNS server.

The DNS Update settings are RFC2136 compliant, for example BIND DNS server.

Figure 22. DNS Update settings

The screenshot displays the 'Arctic Configurator' web interface. At the top, there is a navigation bar with tabs for 'System', 'Network', 'Firewall', 'Services', 'Applications', and 'Tools'. The 'Network' tab is selected. On the left side, a sidebar menu lists various configuration options: Summary, Ethernet, GPRS, Dial-in, SSH-VPN, L2TP-VPN, GRE tunnel, Monitor, Routing, S-NAT, D-NAT, DNS Update (which is highlighted), DynDNS client, NTP client, and SMS Config. Below this menu are buttons for 'Commit', 'Reboot', and 'Logout'. The main content area is titled 'DNS Update settings (RFC2136 compliant, e.g. BIND DNS server)'. It contains several configuration fields: 'Enable' (a dropdown menu set to 'No'), 'Record TTL (seconds)' (a text box with '1200'), 'Record refresh interval(seconds)' (a text box with '1000'), 'Zone' (a text box with 'exampledomain.com'), 'Authoritative name server address' (a text box with '0.0.0.0'), 'Our domain name' (a text box with 'arctic.exampledomain.com'), 'Use Transaction Signatures (TSIG)' (a dropdown menu set to 'No'), 'TSIG key name' (a text box with 'key.exampledomain.com'), and 'TSIG key value' (an empty text box). At the bottom of this section are 'Apply' and 'Reset' buttons.

The server pointed by parameter “Authoritative names server” (eg. company’s own DNS server, for example ISC BIND) must be configured to accept incoming DNS update messages. TSIG keys can be used for better security in DNS updates.

5.2.12 DynDNS Client

This feature can be used with DynDNS service available at <http://www.dyndns.org>.

Note!

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

Figure 23. DynDNS Client Settings

The screenshot shows the 'Arctic™ Configurator' web interface. The top navigation bar includes 'System', 'Network', 'Firewall', 'Services', 'Applications', and 'Tools'. The left sidebar lists various configuration options: Summary, Ethernet, GPRS, Dial-in, SSH-VPN, L2TP-VPN, GRE tunnel, Monitor, Routing, S-NAT, D-NAT, DNS Update, DynDNS client, NTP client, and SMS Config. The main content area is titled 'DynDNS client settings - requires registration to service. GPRS must have public IP address to use DynDNS.' It contains the following fields: 'DynDNS service client enabled' (a dropdown menu set to 'No'), 'DynDNS service provider' (a dropdown menu set to 'dyndns.org'), 'DynDNS Hostname' (a text input field), 'DynDNS Username' (a text input field), and 'DynDNS Password' (a text input field). Below these fields are 'Apply' and 'Reset' buttons. At the bottom of the sidebar are 'Commit', 'Reboot', and 'Logout' buttons.

DynDNS service client enabled – Disables or enables dynDNS DNS name update.

DynDNS service provider – Only dyndns.org currently supported.

DynDNS Hostname – Service provider account hostname.

DynDNS Username – Service provider username.

DynDNS Password – service provider password.

5.2.13 NTP Client

This feature may be used to update the real time clock of Arctic using NTP protocol.

NTP server – When set to "Yes", Arctic updates system clock from NTP server.

Query interval – How often NTP query is sent.

Minimum time difference (seconds) – Minimal time difference, when the clock is updated.

Maximum time difference – Maximum time difference between local system time and NTP time, when the clock is updated.

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

Time adjust value (minutes) – value to add or subtract from NTP value.

5.2.14 SMS Config

This feature may be used to monitor the Arctic status and to issue simple commands remotely via SMS messages. For detailed information, refer to "SMS Config Application Note".

Enabled – Selects whether the SMS Config function is enabled or disabled.

Get commands

Access – Are get commands allowed for everybody, only for defined phone or are these disabled.

Allowed phone – Defined phone number for get commands.

Require password – Require system password for get commands.

Set commands

Access – Are set commands allowed for everybody, only for defined phone or are these disabled.

Allowed phone – Defined phone number for set commands.

Require password – Require system password for set commands.

Allow execute commands – Allow execute commands to be run on Arctic.

Other

Reply error to unknown commands – If set to "No", incorrect commands are silently disregarded. If set to "Yes", Arctic will send error SMS.

Reply error to unauthorized commands – If set to "No", unauthorized command are also silently disregarded. If set to "Yes", Arctic will send error SMS.

Factory reset command (8 chars min) – Command to issue device back to factory settings. This does not require system password. After issuing this SMS command, Arctic will have factory settings (eg. password is set back to factory default also).

5.3 Firewall Menu

Through the Firewall menu, you can configure built-in firewall of the Arctic. Firewall can be disabled or enabled and separate rules may be created for GPRS to Arctic, GRPS to LAN and LAN to GPRS.

Figure 24. GPRS to Arctic Firewall Settings

Arctic™ Configurator

System | Network | **Firewall** | Services | Applications | Tools

Enabled
GPRS to Arctic
GPRS to LAN
LAN to GPRS

GPRS to Arctic Firewall settings

Use GPRS to Arctic Firewall: **Yes**

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

Apply **Reset**

Commit **Reboot**

Logout

The firewall rules are processed from top to bottom. If strict rules are wanted, last rule should be DROP.

The parameter “From IP” can be used for limiting access based on IP address. For example “192.168.100.0/24” would limit access only packets coming from 192.168.100.0 network.

Figure 25. GPRS Settings

GPRS to Arctic Firewall settings

Use GPRS to Arctic Firewall: **Yes**

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

Apply **Reset**

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

5.4 Service Menu

5.4.1 WWW

These settings enable or disable the web server functionality.

Figure 26. Service Menu

The screenshot shows the 'Arctic™ Configurator' web interface. The top navigation bar includes 'System', 'Network', 'Firewall', 'Services', 'Applications', and 'Tools'. The 'Services' tab is selected. On the left sidebar, a list of services includes 'WWW Server', 'Telnet Server', 'DHCP Server', 'DNS Proxy', and 'Eserv Buffer'. The main content area is titled 'WWW Server Settings' and contains three configuration items: 'Web Server' with radio buttons for 'Enabled' (selected) and 'Disabled'; 'Web Configuration Access' with radio buttons for 'Enabled' (selected) and 'Disabled'; and 'Server port (standard=80)' with a text input field containing '80'. Below these settings are 'Apply' and 'Reset' buttons. At the bottom left of the interface are 'Commit', 'Reboot', and 'Logout' buttons.

Web Server – Disables or enables the www server.

Web Configuration Access – Disables or enables web configuration access.

Note!

If you disable the web access settings, web configurator stops functioning and you will have to enable it via console if you should need to use it again later.

5.4.2 SSH

SSH server is available in Arctic for secure connections. Configuration file located at **/etc/sshd_config** may be edited manually.

SSH Server – Enables or disables the SSH server.

5.4.3 Telnet

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

Telnet server – Enables or disables the telnet server.

5.4.4 DHCP

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

DHCP Server

Enables or disables the DHCP server.

Figure 27. DHCP Server Settings

DHCP Server Settings	
DHCP Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Mandatory parameters	
Specify Subnet and Netmask of Ethernet interface to listen	
Subnet	<input type="text" value="10.0.0.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Address range to share	
Low	<input type="text" value="10.0.0.10"/>
High	<input type="text" value="10.0.0.20"/>
Optional parameters, leave blank if not used	
If Arctic DNS proxy is enabled type Arctic Ethernet address to DNS server field. If Arctic is the Default GW for LAN hosts type Arctic Ethernet address to Default GW field.	
Subnet mask	<input type="text" value="255.255.255.0"/>
Domain name	<input exampledomain.com\""="" type="text" value="\"/>
DNS servers	<input type="text" value="10.0.0.2,10.0.0.3"/>
Default gateway	<input type="text" value="10.0.0.1"/>
Broadcast address	<input type="text"/>
Default lease time	<input type="text"/>
Max. lease time	<input type="text"/>
NTP server	<input type="text"/>
Lpr server	<input type="text"/>
WINS server	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Delete leases"/> <input type="button" value="Reset"/>	

Note!

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

DNS Proxy

With DNS proxy, computers connected to Arctic Ethernet interface can use Arctic as DNS server. Arctic will forward DNS queries to correct DSN server and local computers DNS setting are not needed to be changed. This can be used with GPRS settings (Network ->GPRS) parameter "DNS servers: From GPRS network".

DNS Proxy/Forwarder –When set to "Enabled" Arctic can be used as DNS server for local computers.

SNMP Agent

Arctic supports MIB-II SNMP Agent.

SNMP agent (SNMP Set/Get) – Set SNMP agent enabled or disabled.

Read only SNMP community – read only community string.

Read and write SNMP community – rw snmp community

Server port (standard=161) – Agent listen port (UDP)

Bind to interface – The interface is used as source address.

5.5 Application Menu

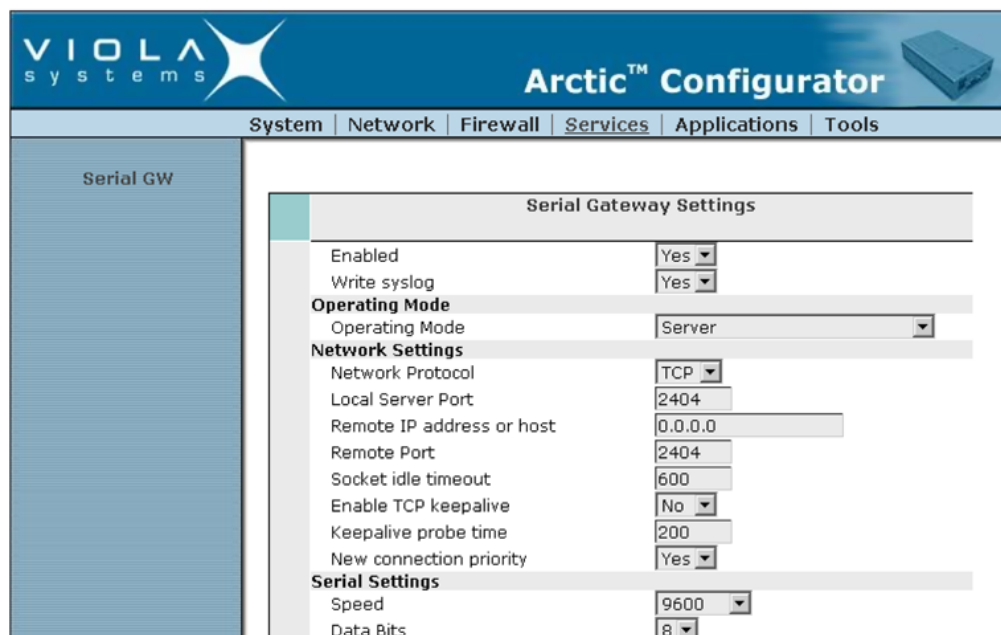
Application menu contains the serial device server application. With this application, serial devices can be connected to the Arctic Gateway and used over the TCP/IP network.

Serial GW

Serial gateway can be enabled from this menu. When enabled in “Server” operation mode, TCP/IP (or UDP) connections can be made to the Arctic (Local Server Port). When Serial GW is in “Client” operation mode, Arctic Gateway sends the received serial data via TCP/IP to host (Remote IP Address or host) to remote host (Remote Port).

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

Figure 28. Serial Gateway Settings



Serial Gateway Settings	
Enabled	Yes
Write syslog	Yes
Operating Mode	
Operating Mode	Server
Network Settings	
Network Protocol	TCP
Local Server Port	2404
Remote IP address or host	0.0.0.0
Remote Port	2404
Socket idle timeout	600
Enable TCP keepalive	No
Keepalive probe time	200
New connection priority	Yes
Serial Settings	
Speed	9600
Data Bits	8

Arctic IEC-104 Gateway specific settings are described in the chapter [IEC-104 application settings](#) on page 46.

For example, a device connected to an Arctic GW application (when in server operation mode) serial port could be accessed with telnet utility as follows:

telnet <Arctic IP Address> 2404

5.6 Tools Menu

The Tools menu provides the access to web based tools used for troubleshooting with the Arctic. It is possible to execute simple shell commands through the Web console. Also GPRS information can be obtained from "Modem Info" menu.

Figure 29. Tools Menu

The screenshot displays the Arctic Configurator web interface. At the top, there is a blue header with the 'VIOLA systems' logo on the left and 'Arctic™ Configurator' on the right, accompanied by a small image of the device. Below the header is a navigation bar with tabs for 'System', 'Network', 'Firewall', 'Services', and 'Tools'. The 'Tools' tab is currently selected. On the left side of the interface, there is a vertical menu with the following options: 'Console', 'System Log', 'Recent events', 'Modem info', 'Send SMS', and 'Default settings'. Below this menu are three buttons: 'Commit', 'Reboot', and 'Logout'. The main content area on the right is titled 'Send SMS message' and contains two input fields: 'Phone number' and 'Message'. A 'Send' button is located at the bottom right of the message input field.

Console

Console can be used for running command over the web interface. Example commands:

```
ping -c 10 172.30.30.1  
firmware
```

System Log and Recent events

Arctic system log can be seen on system log and recent event. When support for device is need, full copy&paste from system log is needed.

Modem info

Arctic modem info show information about GPRS and GSM status. Also the signal strength is shown here. This can be used for GPRS connection problems on site.

Send SMS

Arctic may be used for sending test SMS. This can be used for example checking the phone number of current SIM-card.

Default Settings

Arctic may be set to factory default settings from the Tools menu. This restores factory settings excluding network settings.

6 GPRS

The Arctic with GPRS includes a FME connector (male type) for an external antenna. It is possible to use any kind of external 50Ω dual-band antenna intended for GSM frequency bands (quad-band).

In this Chapter, the specialities related to GPRS operation are described.

6.1 Placing Arctic

When choosing the installation site of Arctic models with the GPRS option, please remember that it uses radio waves for data transmission. The surrounding environment affects the behavior of the radio signals. Therefore, if you are using an Arctic with the antenna mounted directly to the antenna connector (without an extension cable), try to avoid placing the unit in a location where the radio signal might be shadowed by nearby obstacles. Note also that large metallic surfaces (racks) or walls with metallic structures (cabling, concrete iron) may highly degrade the antenna performance. In case of metal racks or surfaces, it is recommended to use an external antenna with an appropriate cable. This allows placing of the Arctic more freely.

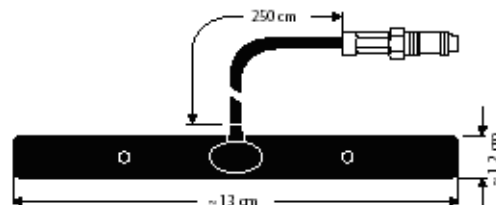
6.2 GPRS Antenna

The Arctic with GPRS includes a FME connector (male type) for an external antenna. It is possible to use any kind of external 50Ω dual-band antenna intended for GSM900 (880–960 MHz) and GSM1800 (also known PCN) (1710–1880 MHz) frequency bands. Connect the antenna directly to the connector provided for the antenna on the back panel of the Arctic unit.

Typically, commercially available antennas are provided with a flexible 50Ω cable having a length of 2–3 meters and having a female type FME-connector.

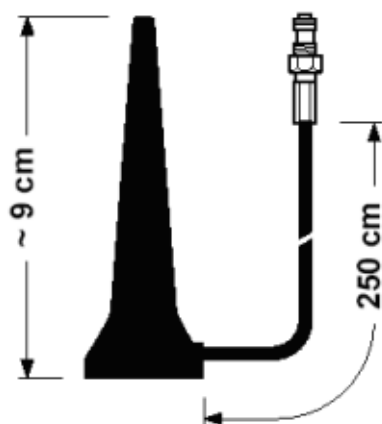
The Arctic IEC-104 Gateway is tested with antennas from Hirschmann Rheinmetall Elektronik GmbH. Examples of tested external antennas include the sticker-type and magnetic mount antennas shown in Figure 30 and 31 respectively:

Figure 30. External Antennas



MCA 18 90 STRIPE, sticker type patch antenna (above), and MCA 18 90 MH , magnetic mount antenna (right). Both antennas have a FME (female) connector and L=250 cm RG174 cable.

Figure 31. *Magnetic Mount Antenna*



6.3 SIM Card and Card Holder

Standard 3 V SIM cards may be used with the Arctic IEC-104 Gateway. A SIM card holder is located on the back panel near the GPRS antenna connector. If you have the PIN code query enabled, check that the Arctic Configurator has a correct PIN code entered in the GPRS submenu. To operate with SIM card follow the procedure below:

1. Power off the Arctic.
2. The SIM card holder contains a tray with a yellow eject button. Push this button in order to eject the tray from the holder.
3. Put the SIM card onto the tray.
4. Insert the tray carefully back to the holder and press the tray until it is locked.

Note!

The card should only be inserted or removed while the GSM module has been placed in shutdown mode. The SIM card holder has a card detection circuit that will in theory allow hot insertion and removal of the card. However, hot insertion and removal are not recommended, since the SIM card content may be corrupted if the card is removed while the GSM module is writing data to it.

6.4 Configuring Arctic's GPRS Settings

1. If your SIM card has the PIN code querying set, make sure you configure the PIN code before inserting the card in the card holder. If PIN querying is not set, you may proceed with the card installation procedure.
2. Connect to the Arctic and log in to Configurator.
3. Navigate to Network page from main navigation bar and select the GPRS sub page.
4. Set the access point name appropriately (usually "INTERNET") .
5. Set the GPRS network username and password appropriately if your GPRS service requires authentication.
6. Set default route to *enabled*.

7. Optionally, set the PIN code and PPP idle timeout.
 - If your SIM card has the PIN code set, type the code into the PIN code field.
 - PPP idle timeout defines the time in seconds how often the Arctic resets the GPRS connection if the connection is idle.
 - ICMP Echo is used to monitor GPRS connection between Arctic and a remote host. If the designated host cannot be reached the GPRS connection is reset. This feature should be always enabled from Network -> Monitor menu.
8. Finally click on **Apply**, wait for the confirmation and then click on **commit** to store the settings. Again, wait for **commit** confirmation.

Figure 32. GPRS Settings

The screenshot shows the 'Arctic Configurator' web interface. The top navigation bar includes 'System', 'Network', 'Firewall', 'Services', and 'Tools'. The left sidebar lists various configuration categories, with 'GPRS' selected. The main content area is titled 'GPRS Settings' and contains the following fields and options:

- GPRS enabled: No (dropdown)
- Access Point Name (GPRS): INTERNET (text field)
- PIN code: NoPin (text field)
- DNS servers: User defined (dropdown)
- LED indication: Data only (dropdown)
- GPRS username: username (text field)
- GPRS password: passwd (text field)
- PPP idle timeout (sec): 1800 (text field)
- Maximum MTU value: 1500 (text field)
- Use GPRS as default route: ☒ Enabled, ☐ Disabled

At the bottom of the settings area, there is a note: 'IMPORTANT: Define also Network->Monitor to detect connection failures'. Below this note are 'Apply' and 'Reset' buttons. At the bottom of the sidebar, there are 'Commit', 'Reboot', and 'Logout' buttons.

Reboot the Arctic for the settings to take effect. Check GPRS status from Network/Summary Menu.

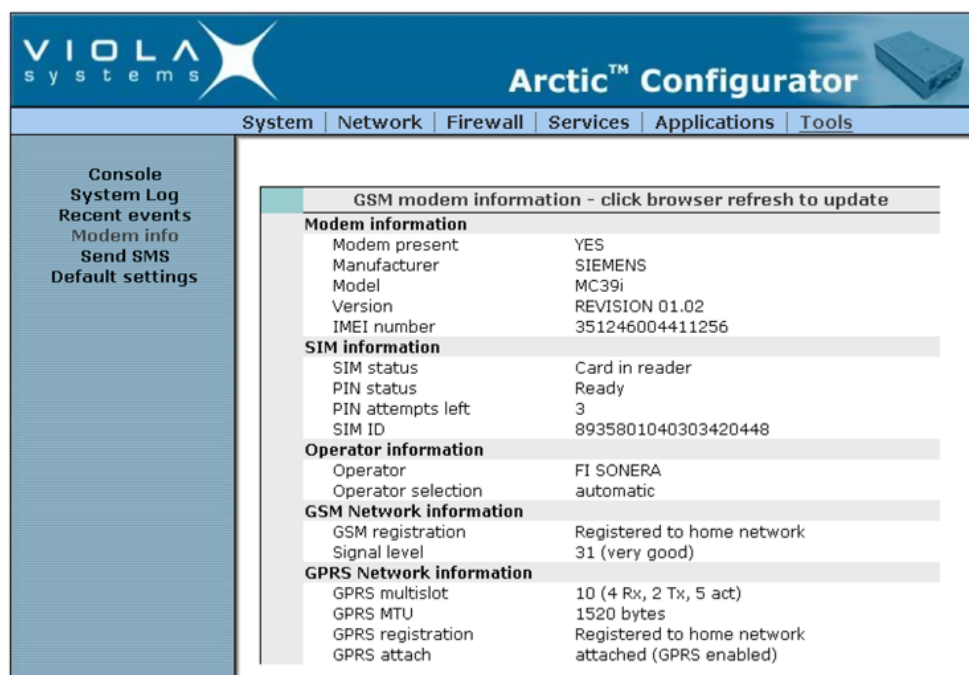
Note!

It is important to set the correct PIN code with the Arctic Configurator before plugging the SIM card in. If an incorrect PIN is set and the PIN is required by the SIM card, the Arctic will not retry with the wrong PIN, thus avoiding the SIM card lock-up. In such a case, you will need to insert the SIM card to a mobile phone and enter the correct PIN before continuing.

6.5 Useful GSM/GPRS Information

Useful GSM/GPRS information can be obtained from Tool -> Modem Info Menu.

Figure 33. Useful GSM/GPRS Information



The screenshot displays the Arctic Configurator web interface. The top navigation bar includes links for System, Network, Firewall, Services, Applications, and Tools. A left sidebar contains links for Console, System Log, Recent events, Modem info, Send SMS, and Default settings. The main content area is titled 'GSM modem information - click browser refresh to update' and contains several sections of status information:

GSM modem information - click browser refresh to update	
Modem information	
Modem present	YES
Manufacturer	SIEMENS
Model	MC39i
Version	REVISION 01.02
IMEI number	351246004411256
SIM information	
SIM status	Card in reader
PIN status	Ready
PIN attempts left	3
SIM ID	8935801040303420448
Operator information	
Operator	FI SONERA
Operator selection	automatic
GSM Network information	
GSM registration	Registered to home network
Signal level	31 (very good)
GPRS Network information	
GPRS multislots	10 (4 Rx, 2 Tx, 5 act)
GPRS MTU	1520 bytes
GPRS registration	Registered to home network
GPRS attach	attached (GPRS enabled)

7 IEC-104 application settings

The IEC-104 and IEC-101 protocols share the same ASDU level messaging but differ on the link level. The IEC-104 is intended for packet-switched TCP/IP communication whereas the IEC-101 is intended for serial communication. By using the Arctic IEC-104 gateway, the IEC-101 slaves (e.g. RTUs) can be connected to a IEC-104 master (e.g. SCADA). The Arctic requests 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 GPRS network. This approach also eliminates the IEC-101 parameter adjutancy problems caused by variable round-trip delays on GPRS networks and makes the information exchange faster and more reliable.

Figure 34. IEC-104 Application Settings

The screenshot shows the 'Arctic Configurator' software interface. The top navigation bar includes 'System', 'Network', 'Firewall', 'Services', 'Applications', and 'Tools'. The 'Applications' tab is selected. On the left, a sidebar lists configuration options: 'IEC-104 (RS2)', 'IEC-104 (RS1)', 'Serial GW (RS1)', 'Serial GW (RS2)', and 'IEC-104 IO'. The main panel is titled 'IEC-104 Gateway (RS1 - shared with console) Settings'. It contains several sections of settings:

- RS1 status:** console - application can't currently use RS1
- IEC-104 gateway enabled:** No (dropdown menu)
- Serial settings:**
 - Speed (bps): 9600 (dropdown menu)
 - Data bits: 8 (dropdown menu)
 - Parity: Even (dropdown menu)
 - Stop bits: 1 (dropdown menu)
 - Use HW flow control: No (dropdown menu)
- Network settings:**
 - Network protocol: TCP (dropdown menu)
 - Network port to listen: 2402 (text input)
 - Network idle timeout: 1800 (text input)
 - New connection priority: Yes (dropdown menu)
- IEC-104 settings:**
 - TX window size (k): 12 (text input)
 - RX window size (w): 8 (text input)
 - I frames TX timeout (t1): 60 (text input)
 - I frames RX timeout (t2): 20 (text input)
 - Link test interval (t3): 20 (text input)
 - Test link on suspended state: No (dropdown menu)
 - Suspended timeout: 300 (text input)

7.1 General settings

IEC-104 gateway enabled

Enables or disables IEC-104 to IEC-101 gateway functionality.

Table 6: IEC-104 gateway enabled

IEC-104 gateway enabled	
Type	Boolean
Units	N/A
Value range	No, Yes

IEC-104 gateway enabled

Note

7.2 Serial settings

The serial settings define the properties of physical serial communication between the Arctic and an IEC-101 slave. The selection between RS-232/422/485 is done with physical DIP switches located below the RS2 serial port.

Figure 35. Serial Settings

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

Speed (bps)

Table 7: IEC-101 serial communication speed (bps)

IEC-101 serial communication speed (bps)	
Type	Serial speed
Units	Bits per second
Value range	1200, 2400, 4800, 9600, 19200, 38400, 57600
Note	

Data bits

Table 8: Number of data bits used on IEC-101 serial communication

Number of data bits used on IEC-101 serial communication	
Type	Serial data bits
Units	Bits
Value range	5, 6, 7, 8
Note	

Parity

Table 9: Parity method used on IEC-101 serial communication

Parity method used on IEC-101 serial communication	
Type	Serial data parity

Parity method used on IEC-101 serial communication	
Units	Bits
Value range	None, Even, Odd
Note	

Stop bits

Table 10: Number of stop bits used on IEC-101 serial communication

Parity method used on IEC-101 serial communication	
Type	Serial data stop bits
Units	Bits
Value range	1, 2
Note	

Use HW flow control

Table 11: Number of stop bits used on IEC-101 serial communication

HW flow control mechanism (RTS/CTS) on IEC-101 serial communication	
Type	Boolean
Units	N/A
Value range	Yes, No
Note	The HW handshaking is available only on RS-232 mode.

7.3 Network settings

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

Figure 36. Network Settings

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

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 (e.g. Mobitex), the UDP protocol can be used to minimize the packets transmitted over network.

Table 12: Network protocol on IEC-104 communication

Network protocol on IEC-104 communication	
Type	Network transmission layer protocol
Units	N/A
Value range	UDP, TCP
Note	The IEC-104 standard specifies only TCP protocol.

Network port to listen

Table 13: TCP or UDP port to listen for incoming IEC-104 connections

TCP or UDP port to listen for incoming IEC-104 connections	
Type	Network port
Units	Port number
Value range	0 - 65000
Note	The IEC-104 standard specifies TCP port 2404.

Network idle timeout

It 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 Arctic. 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.

Table 14: Network idle timeout for IEC-104 connections

Network idle timeout for IEC-104 connections	
Type	Timeout
Units	Seconds
Value range	0 – 65000
Note	The network idle timeout must be longer than IEC-104 link test interval (t3).

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.

Table 15: New connection priority for IEC-104 connections

New connection priority for IEC-104 connections	
Type	Boolean
Units	N/A

New connection priority for IEC-104 connections	
Value range	No, Yes
Note	It is recommendable to set this value to "Yes" in normal configurations having only one IEC-104 master.

7.4 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 Arctic and the IEC-104 master over the TCP/IP network.

Figure 37. IEC-104 Settings

IEC-104 settings	
TX window size (k)	12
RX window size (w)	8
I frames TX timeout (t1)	60
I frames RX timeout (t2)	20
Link test interval (t3)	200
Test link on suspended state	No <input type="button" value="v"/>
Suspended timeout	300
Max sequence number (0=def)	0
Flush buffered events on connection	No <input type="button" value="v"/>
Cause of transmission length	2 <input type="button" value="v"/>
Common address length	2 <input type="button" value="v"/>
Info object address length	3 <input type="button" value="v"/>

TX window size (k)

TX window size defines the maximum number of I format APDUs the Arctic may send before requiring the IEC-104 master to acknowledge them. If there are k unacknowledged frames sent the Arctic will stop polling IEC-101 slave for events until acknowledgement is received.

Table 16: IEC-104 TX windows size (k)

IEC-104 TX windows size (k)	
Type	Window size
Units	Packets
Value range	1-20
Note	The <i>k</i> must be always less than the maximum sequence number defined below. The IEC-104 standard suggests <i>k</i> to be 12.

RX window size (w)

It defines the maximum number of I format APDUs the Arctic may receive before sending acknowledgement to the IEC-104 master.

Table 17: IEC-104 RX windows size (w)

IEC-104 RX windows size (w)	
Type	Window size
Units	Packets
Value range	1-20
Note	The w should not exceed two-thirds of TX window size k . The IEC-104 standard suggests w to be 8.

I frames TX timeout (t1)

It defines the timeout in seconds the Arctic 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 Arctic will close the network connection and the IEC-101 link.

Table 18: IEC-104 I frames TX timeout (t1)

IEC-104 I frames TX timeout (t1)	
Type	Timeout
Units	Seconds
Value range	1-255
Note	The $t1$ must be longer than the network round-trip-time. The IEC-104 standard suggests 15 seconds.

I frames RX timeout (t2)

This defines the timeout in seconds from the last received I format APDU before sending acknowledgement.

Table 19: IEC-104 I frames RX timeout (t2)

IEC-104 I frames RX timeout (t2)	
Type	Timeout
Units	Seconds
Value range	1-255
Note	The $t2$ must be smaller than $t1$. The IEC-104 standard suggests 10 seconds.

Link test interval (t3)

This defines the interval in seconds how often the IEC-104 link is tested if there is no other activity.

Table 20: IEC-104 link test interval (t3)

IEC-104 link test interval (t3)	
Type	Timeout

IEC-104 link test interval (t3)	
Units	Seconds
Value range	1-65000
Note	Adjust this parameter according to 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.

Suspended timeout

This defines the time in seconds how long a connected IEC-104 link can be in suspended state (STOPD) before the Arctic closes the connection.

Table 21: IEC-104 suspended timeout

IEC-104 suspended timeout	
Type	Timeout
Units	Seconds
Value range	1-65000
Note	Using this parameter increases the probability of detecting partially closed network connections especially in UDP mode.

Max sequence number

These are the maximum sequence number used in IEC-104 communication. The value zero selects the standard value 32767.

Table 22: IEC-104 suspended timeout

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

Cause of transmission length (IEC-104)

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

Table 23: IEC-104 ASDU cause of transmission length

IEC-104 ASDU cause of transmission length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-104 standard defines value 2.

Common address length (IEC-104)

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

Table 24: IEC-104 ASDU common address length

IEC-104 ASDU common address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-104 standard defines value 2.

Info object address length (IEC-104)

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






Table 25: IEC-104 ASDU information object address length

IEC-104 ASDU information object address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-104 standard defines value 3.

7.5 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 Arctic and a IEC-101 slave.

Figure 38. IEC-101 Settings

IEC-101 settings	
Slave link address	10
Link address field length	2 
Event poll interval (x0.1 s)	1
Link test interval (x0.1 s)	200
Keep link open	Yes 
Reply header timeout (msecs)	1000
Reply end timeout (secs)	2
Retry limit	3
Cause of transmission length	1 
Common address length	2 
Info object address length	2 

Slave link address (IEC-101)

Table 26: IEC-101 slave link address

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

Link address field length

Defines the length of the IEC-101 link-level address field in bytes.

Table 27: IEC-101 slave link address field length

IEC-101 slave link address field length	
Type	Field length
Units	Bytes
Value range	1, 2
Note	The link-level address of IEC-101 slave.

Event poll interval

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

Table 28: IEC-101 event poll interval

IEC-101 event poll interval	
Type	Interval
Units	0.1 seconds
Value range	1-65000
Note	The events are polled only when the IEC-104 connection is active.

Link test interval

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

Table 29: IEC-101 link test interval

IEC-101 link test interval	
Type	Interval
Units	0.1 seconds
Value range	1-65000
Note	The link test is performed if there is no other activity during defined interval.

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 Arctic 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.

Table 30: IEC-101 keep link open

IEC-101 keep link open	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	Some IEC-101 slaves require the link to be continuously open in order to operate.

Reply header timeout

Defines the timeout Arctic waits the reply to start from IEC-101 slave after command or request.

Table 31: IEC-101 reply start timeout

IEC-101 reply start timeout	
Type	Timeout
Units	Milliseconds
Value range	1-65000
Note	

Reply end timeout

Defines the maximum duration of IEC-101 slave response.

Table 32: IEC-101 reply end timeout

IEC-101 reply end timeout	
Type	Timeout
Units	Seconds
Value range	1-65000
Note	

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 Arctic closes the IEC-101 and IEC-104 connections.

Table 33: IEC-101 retry limit

IEC-101 retry limit	
Type	Retry limit

IEC-101 retry limit	
Units	Retries
Value range	0-65000
Note	

Cause of transmission length (IEC-101)

Defines the length of IEC-101 Cause of transmission ASDU header field in bytes.

Table 34: IEC-101 ASDU cause of transmission length

IEC-101 ASDU cause of transmission length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-101 standard defines value 1.

Common address length (IEC-101)

Defines the length of the IEC-101 Common address ASDU header field in bytes.

Table 35: IEC-101 ASDU common address length

IEC-101 ASDU common address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-101 standard defines value 2.

Info object address length (IEC-101)

Defines the length of IEC-101 Information object address ASDU header field in bytes.

Table 36: IEC-101 ASDU information object address length

IEC-101 ASDU information object address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-101 standard defines value 2.

7.6 ASDU Converter

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

Figure 39. ASDU Converter

ASDU Converter	
Use ASDU converter	Yes <input type="button" value="v"/>
Use ASDU type replacer	Yes <input type="button" value="v"/>
IEC-101 ASDU type	128
IEC-104 ASDU type	30
Convert short IEC-101 time stamps	No <input type="button" value="v"/>

Use ASDU converter

This defines if the ASDU header level IEC-101 <-> IEC-104 conversion 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.

Table 37: Use ASDU converter

Use ASDU converter	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	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.

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.

Table 38: Use ASDU type replacer

Use ASDU type replacer	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	

Original type

The original ASDU type searched by ASDU type replacer.

Applied type

The new ASDU type is replaced by the original type.

7.7 Packet collector

The packet collector can be used to collect many IEC-101 messages/events to a single network packet instead of sending every message separately.

This function is useful for slow packet switched communication network (e.g. Mobitex) for speeding up especially the general interrogation response.

Figure 40. Packet Collector

Packet collector	
Use packet collector	No 
Max bytes	500
Max time (x0.1 s)	20
Max packets	5

Use packet collector

Table 39: Use packet collector

Use packet collector	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	

Max bytes

Max bytes is defined as 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.

Table 40: Maximum collected bytes

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

Max time

Max time is defined as the maximum collect time trigger for packet collector in 0.1 secs increments for packet collector. If there has been data on packet collector over MAX TIME the data is sent to network.

Table 41: Maximum collected time

Maximum collected time	
Type	Timeout
Units	0.1 seconds

Maximum collected time	
Value range	1-255
Note	The value must be smaller than t1.

Max packets

Max packets are defined as the maximum amount of IEC-101 packets stored into the packet collector before sending the data to the network.

Table 42: Maximum collected packets

Maximum collected packets	
Type	Packet count
Units	Packets
Value range	1-255
Note	

7.8 IO extension

Note!

Arctic IEC-104 Gateway (product code 2205) does not have an IO extension board.

7.9 Other settings

Write syslog

It defines whether the error messages are stored to system log file or not.

Table 43: Write system log

Write system log	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	The system log is available by using WEB UI.

8 IEC-104 IO Application Settings

Figure 41. IEC-104 IO application settings

The screenshot shows the Arctic Configurator web interface. The top navigation bar includes tabs for System, Network, Firewall, Services, Applications, and Tools. The left sidebar lists configuration options: IEC-104 (RS2), IEC-104 (RS1), Serial GW (RS1), Serial GW (RS2), and IEC-104 IO. The main content area is titled "IEC-104 Direct control IO (requires IO extension board)". It contains several sections of settings:

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

Note!

Arctic IEC-104 Gateway (product code 2205) does not have an IO extension board.

9 Troubleshooting

This Chapter provides a list of the common problems encountered while installing, configuring or administering the Arctic. If you are unable to resolve your problem, refer to the Warranty and Technical Support Sections at the end of this User's Guide for information about contacting Viola Systems Technical Support representatives.

Q: When setting up routing mode "tunnel the following network", routing to M2M Gateway eth1 does not work?

A: Check that IP forwarding has been enabled and internal firewall does not block packets.

Q: From Arctic Ethernet connection to M2M Gateway Ethernet is not working?

A: Check that IP forwarding has been enabled on Arctic.

Q: If only one public IP is available, can the M2M Gateway be used?

A: Yes, if firewall connected to public IP can forward incoming SSH connections to the M2M Gateway.

9.1 Common Problems

Problem #1

Q: Console does not receive characters.

A: Disable HW and SW handshaking from your terminal software (e.g. Hyperterm or Minicom).

Problem #2

Q: GPRS interface is up but no traffic flows through it.

A: Default gateway in Ethernet settings submenu has to be set as "0" and also default gateway has to be enabled from Network/GPRS menu when using GPRS interface as the default gateway.

Problem #3

Q: GPRS connection is not established.

A: Check that the SIM card has the correct PIN number settings and that it has not been locked after a wrong number was entered three times successively. PIN status can be checked from Tools/Modem Info menu.

Problem #4

Q: GPRS connection is ended after approximately two minutes.

A: You have enabled connection checking from Network/Monitor menu but not set the correct IP to GPRS "ICMP Echo settings".

Specifications

Technical Specifications	
Processor	32-bit 48 MHz RISC Processor
Memory	<ul style="list-style-type: none"> 32 MB RAM 8 MB Flash ROM
Network Interface	<ul style="list-style-type: none"> 10/100 Base-T. Shielded RJ45 Ethernet (IEEE 802.3) 1.5 kV isolation transformer
Serial Device Interface	<ul style="list-style-type: none"> 2 x Male DB9 connector DTE 15kV ESD and short circuit protection Full serial and modem signals Speed: 300–460800 bit/s Data bits: 7 or 8; Stop bits: 1 or 2 Parity: None, Even, Odd Flow control: None, RTS/CTS Console port / application port 1: Console: RS-232, 19200 bit/s, 8 data bit, 1 stop bit, no parity Application port 2: Serial port selectable: RS-232 or RS-422/485
Power Requirements	<ul style="list-style-type: none"> Resettable fuse and ESD protected input External 110–230 VAC adapter (optional)
Temperature Range	<ul style="list-style-type: none"> Operating: –20 to 55° C Storage: –30 to 85 °C
Relative Humidity	Operating: 5 to 85 % RH non-condensing
Operating System	µCLinux embedded multitasking operating system
Network Protocols Supported	PPP, IP, ICMP, UDP, TCP, ARP, DNS, DHCP,FTP, TFTP, HTTP
Tunneling (VPN)	<ul style="list-style-type: none"> SSH-VPN client (requires Viola M2M Gateway) L2TP-VPN client (requires Viola M2M Gateway) SSH client
Management	WWW, SSH, Telnet and console FTP, TFTP and HTTP software update
Routing and Firewall	Static routing, proxy ARP, port forwarding, IP masquerading/NAT, firewall
Serial Device Connectivity	<ul style="list-style-type: none"> Device server application (IEC-104 GW) Simultaneous GPRS, CSD and SMS SMS configuration and status reporting

Technical Specifications	
Dimensions and Weight	<ul style="list-style-type: none">Models in aluminum frame:Size: 180 mm x 110 mm x 45 mm (WxLxH)Weight: 0.7 kgAttachment rail for optional and custom mounting

Limited Warranty

Coverage

Viola Systems warrants this hardware product to be free from defects in materials and workmanship for the warranty period. This non-transferable, limited warranty is only to you, the first end-user purchaser. The warranty begins on the date of purchase and lasts for the period specified below:

Arctic : one (1) year

Excluded Products and Problems

This warranty does not apply to: (a) Viola Systems software products; (b) expendable components such as cables and connectors; or (c) third party products, hardware or software, supplied with the warranted product. Viola Systems makes no warranty of any kind on such products which, if included, are provided "AS IS." Excluded is damage caused by accident, misuse, abuse, unusually heavy use, or external environmental causes.

Remedies

Your sole and exclusive remedy for a covered defect is repair or replacement of the defective product, at Viola Systems' sole option and expense, and Viola Systems may use new or refurbished parts or products to do so. If Viola Systems is unable to repair or replace a defective product, your alternate exclusive remedy shall be a refund of the original purchase price.

The above is Viola Systems' entire obligation to you under this warranty. IN NO EVENT SHALL VIOLA SYSTEMS BE LIABLE FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, USE, OR PROFITS EVEN IF VIOLA SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Viola Systems' liability exceed the original purchase price of the device server. Some states or countries do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

You must notify Viola Systems within the warranty period to receive warranty service. During the warranty period, Viola Systems will repair or replace, at its option, any defective products or parts at no additional charge, provided that the product is returned, shipping prepaid, to Viola Systems. All replaced parts and products become the property of Viola Systems. Before returning any product for repair, customers are required to contact the Viola Systems.

Technical Support

Contacting Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: <http://www.violasystems.com>

Recording Arctic Information

Before contacting our Technical Support staff, please record (if possible) the following information about your Arctic product:

Product name:

Serial no:

Note the status of your Arctic in the space below before contacting technical support. Include information about error messages, diagnostic test results, and problems with specific applications.
