NSG–1700

M2M Access Router

User Manual

(NSGate shipment)

Moscow 2019

CONTENTS

NOTE NSG products are permanently developed and enhanced, thus discrepancies between the actual product and the present document may occur, without sacrificing the stated characteristics of the product.

© NSG Ltd. 2017–2019
NSG logo is a registered trademark of NSG Ltd.

1. General product description

1.1. Product destination and composition

NSG–1700 is an M2M access router designed for connecting a variety of terminal equipment, as well as PC, to IP networks over public Ethernet, LTE, and/or Wi-Fi networks. Its applications include, but are not limited to:

— Connection of ATMs, POS terminals, self-service kiosks and other types of banking terminals, with or without built-in TCP/IP stack.
— Internet access and WLAN set-up for small offices.
— Connection of remote offices to corporate VPNs.
— Remote control of telecommunications and other equipment, as well as systems with digital and analog I/O in various industries.

Basic NSG–1700 configuration has two fixed Fast Ethernet ports and one RS–232/console port. Additionally they may be supplemented (on demand, or on the supplier's discretion) with another RS–232, another Ethernet, and 1–Wire ports. On the wireless side, the device may contain up to two LTE and/or Wi-Fi options, with two SIM-card slots available to both or the only LTE option.

The Ethernet and Wi-Fi ports may be utilized for both connecting to the public (WAN) networks and building the LAN of the user side. All the ports are physically independent (i.e. routed), yet may be joined in a software switch (*aka* bridge groups).

The RS–232/console ports may be utilized for both the device management and the user data.

The optional 1–Wire port is destined for connecting external sensors and actuators supported by NSG software.

The device is powered from an external adapter or a DC source.

The product runs NSG Linux software, version 2.1 and higher. Detailed description of software functionality and setup is available in Russian online at the website:

http://www.nsg.ru/help/

1.2. NSGate custom setup and documentation

Due to vast functional abilities and complexity of configuring them, the device is shipped by NSGate with a preset configuration up to a particular networking solution. For the end user's convenience, a custom user account is also set up with access to a limited scope of parameters that may need configuration on-site. The involved parameters are documented below in the current documents.

When needed, access to the full-featured user account is also available. This makes possible deeper re-configuration according to NSGate guidelines and supervision.

1.3. Technical specifications

Hardware specifications

- NXP (ex-Freescale) i.MX6 CPU
- 512 MB RAM
- 128 Flash ROM or SDHC card
- 2 Fast Ethernet 10/100/Base–T ports
- 1 RS–232/console port
- 2 SIM-card slots
- Wired options:
  - 2nd RS–232 (up to 1)
  - 3rd Ethernet port (up to 1, low-speed)
  - 1–Wire port (up to 1)
- Wireless options (up to 2 total):
  - Wi-Fi IEEE 802.11 b/g/n
  - LTE/UMPS/GSM
- 1 programmable LED
- 1 programmable h/w button

Physical specifications

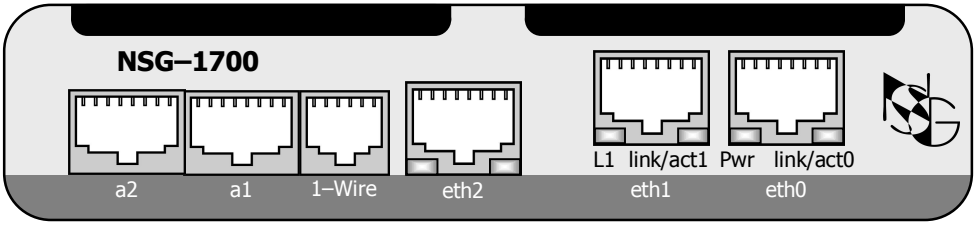
- Dimensions: 140×110×35 mm (without antennas)
- Weight: (w/o power adapter): 0,4 kg
- Power: 9…30V, 2A DC

Environmental specifications

- Temperature: 0…+50°C
- Humidity: 10…85%

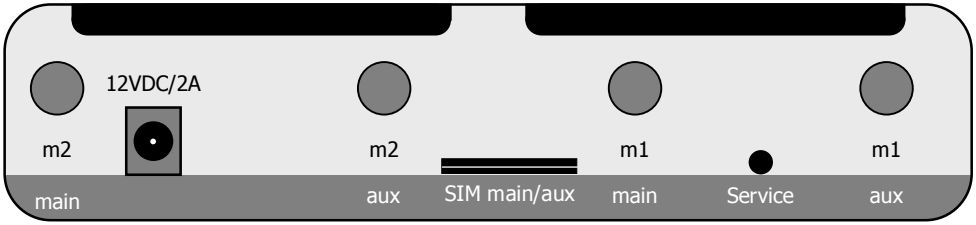
2. Appearance and connectors

2.1. Front panel



a2	2nd RS–232 port (optional). Hardware flow control always on.
a1	RS–232/console port. Hardware flow control always on. **Note:** In NSGate configuration, always used as dedicated system console at 115200 bps, 8n1.
1–Wire	1–Wire port (optional).
eth2	Low-speed Ethernet 10Base–T port (optional). Half-duplex only. No autoMDI/MDI-X selection.
eth1, eth0	Ethernet 10/100Base–T ports. AutoMDI/MDI-X selection supported. **Note:** In NSGate configuration, all Ethernet ports are included into a single bridge group. The device is available over any port at IP address 172.16.0.1.
L1	Programmable LED (green).
link/act	Link (lighted on) and activity (flashing) indicators for Fast Ethernet ports.
Pwr	Power indicator.

2.2. Rear panel



12VDC/2A	DC power input. Voltages 9 thru 30 V are tolerated.
Service	Programmable button. **Note:** not used in NSGate configuration.
m2, m1 main/aux	SMA–F antenna connectors. Each LTE or Wi-Fi option, if installed, utilizes 2 antennas. Otherwise, dummy caps. **Note:** NSGate configuration comes with a single m1 LTE option installed.
SIM main SIM aux	SIM card slots. (Present regardless of LTE options being actually installed.) Both slots can be used by either m1 or m2 LTE option, if present. See "LTE port node" for software SIM cards management.

ATTENTION: SIM cards should be inserted into the slots as depicted at the panel. Pay attention to fit into the correct slot out of the two. Never apply excess force to insert the cards. **Destruction of the slots by brute force is not covered by warranty.** Once inserted completely, the SIM cards protrude from the panel by approx. 3 mm.
Never should be SIM cards put in or out while the device is switched on.

3. Installation and set-up

3.1. Physical installation

To install the device at the site, one should:

1. Unpack the box and check that all relevant accessories are in place. If not, contact your supplier.
2. Connect LTE (long, with cable) and/or Wi-Fi (short, attached directly) antennas to the connectors, in strict accordance with the types of preinstalled options. Each wireless option utilizes two connectors.
3. Insert SIM card(s). **Pay attention to note in Section 2.2.**
4. Connect Ethernet ports to LAN hosts or switch. The two principal Fast Ethernet ports do support auto-negotiation of speed, duplex, and pin layout (MDI/MDI-X), thus both straight and cross-over cables may be used in any case.
   The additional eth2 port, if any, should be used for low-speed M2M applications only. The port supports only 10Base–T half-duplex mode at approx. 1 Mbps. The port does not support MDI/MDI-X autodetection; thus, if neither the other side of the connection supports it, proper selection of Ethernet cable is essential:
   — use cross cable for a switch downlink port;
   — use straight cable for a host (PC, server, Web camera, etc.) or a switch upstream port.
5. Connect the PC COM port or an RS–232 port of another hardware to a1, a2 ports, if supposed for usage. Use NSG CAS–V24/D9/FC/A cable or similar cables with Cisco-like pin layout.
6. Connect the 1–Wire devices to 1–Wire port in daisy-chain, if supposed for usage.
7. Connect the DC power source to the power jack.

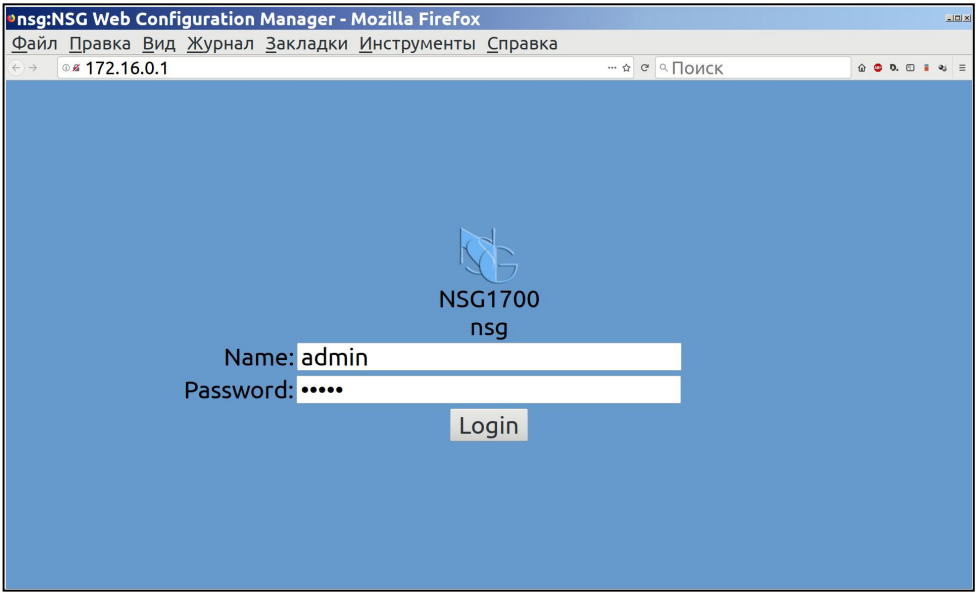
3.2. Software setup

Initial setup is done over the eth0 port using any modern Web browser or a Telnet client. ~~In the factory settings, the port is configured with IP address 192.168.1.1/24. Thus, to access it, set your PC network adapter to any address like 192.168.1.*x* (where *x* = 2 … 254) and netmask 255.255.255.0.~~

NOTE In NSGate configuration, all the Ethernet ports are configured as members of a single bridge group. Thus the device may be accessed over any port. The configured address is 172.16.0.1/16. Thus, the PC should be configured to any address between 172.16.0.2 and 172.16.255.254, with netmask 255.255.0.0.

~~To enter the device, log in as nsg with an empty password.~~

NOTE In NSGate configuration, user nsg is locked. Log in as admin, password admin, to get access to the shortened set of parameters.



Once configured, the device may be managed remotely over the IP network.

NOTE With LTE options installed and SIM cards put in, the device connects to the mobile network immediately. In most modern network, the connection is done without additional setup, thus the device becomes available for remote management over the mobile network, too.

Within the Web interface, all configuration parameters and single-time commands are arranged as a tree. To expand any branch of it, double-click it or click the [+] button left of it. To edit a parameter, double-click into its input field, or click the right of it

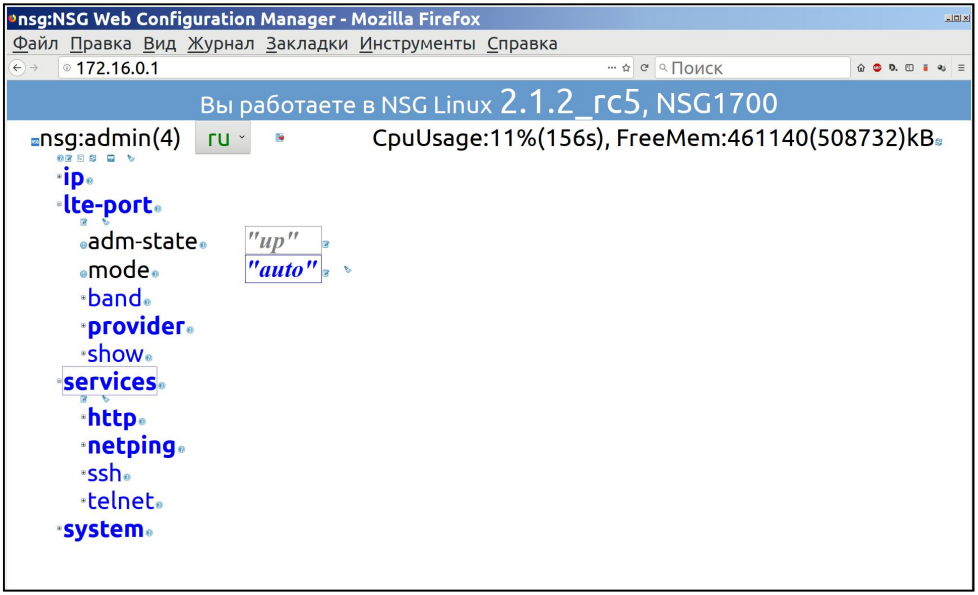
To apply the changes, that is, to put them into effect, click right of the changed parameter or in any node located closer to the root of the tree. To save the configuration, click at the root of the tree.

NOTE Multiple users may access the device simultaneously over Web interface and Telnet/SSH. In this case, only one of them is granted full rights to manage the device; the others work in read-only mode.

ATTENTION To close a user session correctly, click .

To view and edit the configuration in text mode, click button at the root of the tree or at a particular branch. While editing the configuration manually, retain the structure of ": " (colon, space) offsets, otherwise the structure of the tree will be lost and your changes will be rejected. To return to the tree view, click at the same position. To revert your changes, click . To check your changes before reconstructing the tree, click .

Some branches include user-configurable lists of similar objects, e.g. filters or NAT rules. To add an item to a list, click in the parent node. To delete an item, click right of it.



Lists may be either named or numbered. In numbered lists, items are always renumbered sequentially, and their order may by important (e.g. filter rules are applied strictly in the that order). If a rule is deleted from the middle of the list, the numbers of the subsequent ones are decreased by 1 so that all the rules would be numbered in sequence again. If a rule is inserted to the middle of the list (once prompted, enter the number of the desired position), the subsequent ones are shifted downwards.

The button purges all the user's changes in the given parameter or node. When applied to a single parameter, it sets it to the default value. When applied to a list, it deletes all elements of a list. When applied to a node, it sets all the parameters within the node to their defaults and deletes all the list within it.

Nodes and parameters with user-configured values within them are shown in bold. Single-time commands (that is, not stored in the ROM, like reboot) are shown in green and executed by clicking the .

3.3. Device security

To prevent unauthorized access to the device, password protection is essential. **A unique password for admin must be set before connecting the device to any public network.**

It is highly recommended to block access to the device from the public network side whenever possible. If remote management is essential if your network solution, only the secure protocols must be used: HTTPS (and not HTTP) and/or SSH (and not Telnet).

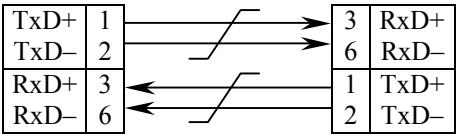
4. Cables and pin layouts

Fast Ethernet ports (eth0, eth1)	
№	**Signal**
1	TxD+ / RxD+
2	TxD– / RxD–
3	RxD+ / TxD+
4	Not connected
5	Not connected
6	RxD– / TxD–
7	Not connected
8	Not connected

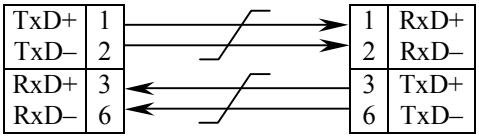
optional Ethernet port (eth2)	
№	**Signal**
1	RxD+
2	RxD–
3	TxD+
4	Not connected
5	Not connected
6	TxD–
7	Not connected
8	Not connected

RS–232 ports (a1, a2)	
№	**Signal**
1	Flow Control Out
2	Ready Out
3	Data Out
4	GND
5	GND
6	Data In
7	Ready In
8	Flow Control In

Ethernet RJ–45 crossover cable



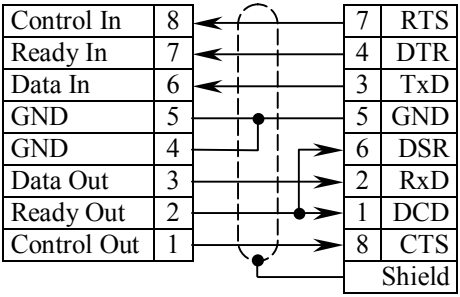
Ethernet RJ–45 straight cable



DCE cable
for RS–232 async ports
CAS–V24/D9/FC/A

To NSG–1700
RJ–45

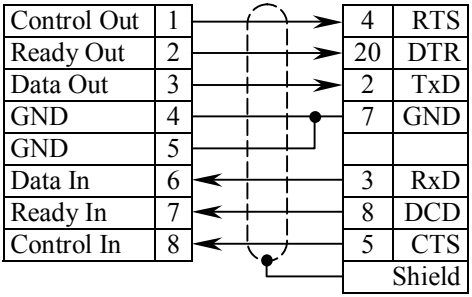
To PC
DB–9f



DTE cable
for RS–232 async ports
CAS–V24/D25/MT/A

To NSG–1700
RJ–45

To dialup modem
DB–25m



5. NSGate custom configuration

5.1.Why and what it is

NSG–1700 is a powerful and cumbersome telecommunication device with about 2000 configuration parameters. To fully utilize it, one should be an expert in networking technologies, and the complete user manual should become available in the proper language.

The device is shipped by NSGate for a relatively simple application and intended for usage by technicians with only a basic training in networking. Thus a custom configuration is done in advance. As a part of this configuration, a simplified user account is set up and a custom configuration tree is built specifically for this application.

5.2. General overview

The provided configuration includes the following elements available for the admin user:

— Configuration of the LTE port.
— Destination NAT (*aka* port forwarding) rules for sessions coming from the public LTE network into the LAN.
— Filtering rules for incoming LTE traffic.
— netping service to monitor the LTE connection by pinging a given host in regular intervals. Once the ping is steadily lost, it restarts the LTE port (but not the entire device.)
— Management services (HTTP/HTTPS, Telnet, SSH).
— System hostname and time settings.
— Password setup for admin and for the advanced nsg user.

Some elements of the custom configuration tree are left there temporarily and should not be used by admin.

In addition, the following configuration elements are done in advance and located beyond the reach of the admin user:

— A bridge group between all the Ethernet ports is configured, with IP address 172.16.0.1/16.
— A NAT masquerading rule for sessions (if any) initiated by LAN hosts towards the public network.
— The admin user itself.

NOTE After switching the device on or reconnecting Ethernet cables, the bridge group takes about 1 minute to reconfigure. As the device is designed for continuous operation during an undefinitely long time, this one-time delay is tolerable.

5.3. IP filters and NAT nodes

ip

IP packets processing setup.

ip.filter-INPUT

Set up filtering rules against undesirable incoming traffic. The node contains a numbered list of rules. Rules are processed in the order of their numbers.

Follow the given examples to configure your own rules. In the given NSGate configuration, two rules are defined to block insecure HTTP and Telnet traffic.

Note: Rule 0 should never by deleted or altered.

ip.filter-INPUT.N

A particular filtering rule setup.

ip.filter-INPUT.N.protocol
ip.filter-INPUT.N.protocol-num

Filtering criterion: the Layer 4 protocol in the incoming packet, either by name (e.g. TCP) or by IANA number. Only one of the settings must be done.

ip.filter-INPUT.N.in-interface

Filtering criterion: interface through which a packet comes in. For the given configuration, m1 is the name of the LTE interface.

ip.filter-INPUT.N.source
ip.filter-INPUT.N.destination

Filtering criteria: IP source and destination addresses of a packet.

ip.filter-INPUT.N.source-port
ip.filter-INPUT.N.destination-port

Filtering criteria: IP source and destination port numbers. To make these criteria available, protocol = "tcp" or "udp" must be set first.

ip.filter-INPUT.N.tcp-flags

Filtering criterion: TCP flags that should be checked and those that should be present in the packet. Available for TCP only. E.g. the following setting

```
tcp-flags = "SYN,RST,ACK,FIN SYN"
```

selects all the packets that initiate TCP connections.

ip.filter-INPUT.N.explicit-matches
ip.filter-INPUT.N.extra-options

Advanced criteria for selection of packets. For experienced Linux users only.

ip.filter-INPUT.N.target

Operation to be done with a packet selected by the combination of the above criteria. For filtering, choose only ACCEPT or DROP options.

ip.filter-INPUT.N.extra-target

Advanced target parameters. For experienced Linux users only.

ip.filter-INPUT.default-target

Operation to be done with a packet that does not match any of the explicitly

defined rules. Typically set to ACCEPT for normal use (any packets are allowed, except the explicitly forbidden ones).

ip.nat-PREROUTING
: Set up Destination NAT rules to forward particular sessions from the public LTE network to specified LAN hosts and ports on them.
As an example, 4 rules are set up to forward 2 TCP connections to each of 2 different hosts.

ip.nat-PREROUTING.N
: A particular NAT rule.

ip.nat-PREROUTING.N.*criteria*
: Various criteria for packet selection, same as in the filters (see above).

ip.nat-PREROUTING.N.target
: Operation to be done with a selected packet. For port forwarding, select DNAT and set the destination host and port in the following parameter.

ip.nat-PREROUTING.N.to-destination
: LAN host and its port to which the packet should be forwarded. For TCP and UDP sessions, the syntax is ip.ad.dr.ess:port .

NOTE For NAT and filtering parameters and values not described above, see *man iptables*, *man iptables-extensions* on any Linux PC or online.

5.4. LTE port node

lte-port
: LTE port setup.

lte-port.adm-state
: Set to up to enable the port, down to disable it.

lte-port.mode
: Mode of operation, or Radio Access Technology (RAT) for the mobile interface. Depending on the cellular coverage at a particular site, one may wish to set the made manually (LTE, UMTS, or GSM), or limit the available choices for auto-selection.

lte-port.band
: Frequency bands to be tried and scanned for available networks. You may enable or disable each of them individually according to what is actually used by local operators at a particular site.

NOTE Disabling the RATs and bands that are *a priori* known to be not available at the site may drastically shorten the time of re-connection. Consult your LTE operator about bands used by it.

lte-port.provider
: SIM card and provider-specific settings.

lte-port.provider.main
: Settings for the main (upper) SIM-card.

lte-port.provider.aux
: Settings for the auxiliary (lower) SIM-card.

lte-port.provider...APN
lte-port.provider...username
lte-port.provider...password
: Provider-specific connection and authentication settings. Not needed for public service in most modern mobile networks. May be specified by provider in some cases, e.g. when using a mobile VPN service.

lte-port.provider...attemps
: Specific parameter for dual-SIM usage. The module does main.attempts to connect with the main SIM card, then aux.attempts to connect with the auxiliary SIM card, then starts the loop again.
In particular, the 0 value prohibits usage of that SIM card. The practical configurations are:

A single LTE option using only the main SIM-card (default):

```
provider
: main
: : attempts = 1
: aux
: : attempts = 0
```

A single option may use both slots, provided that both SIM cards are installed. The following configuration makes the LTE module to switch to the other card after each disconnection:

```
provider
: main
: : attempts = 1
: aux
: : attempts = 1
```

In case of the two LTE options installed, one of them should be granted access to one of the SIM cards and denied access to the other, and vice versa:

```
port
: m1
: : provider
: : : main
: : : : attempts = 1      } by default
: : : aux
: : : : attempts = 0      }
: m2
: : provider
: : : main
: : : : attempts = 0
: : : aux
: : : : attempts = 1
```

lte-port.provider...connect-waiting-time
: Maximum time to wait for the connection, in seconds. May be useful in some networks, where the connection procedure sometimes stales or loops. If the LTE port does not come into operation state for the specified time, the port is forced to restart and begin the procedure again. Recommended value for this case is 120 sec. The 0 value sets the port to wait for the connection indefinitely long.

lte-port.show
: A set of diagnostic tools to monitor the wireless operation.

lte-port.show.csq-check
: Output the signal level value. 31 is the best possible value; at values below 10, reception problems are likely. 99 indicates absence of cellular network.

lte-port.show.radio-info
: Output the detailed data on radio operation: signal level, operator name, selected RAT mode, etc.

lte-port.show.module-info
: Output the detailed data about the LTE module and the SIM card: model, firmware version, IMEI, IMSI, etc.

NOTE The above 3 commands make sense only during stable operation of the LTE port. Once the port is not connected, it regularly restarts, boots its firmware, searches for the mobile networks, etc. The responses of the commands during this process may be arbitrary, depending on which phase of it takes place at the moment.

lte-port.show.log
: Output the log of the LTE daemon. Nothing specific.

lte-port.show.progress
: Output the log of the current LTE session: SIM check, RAT negotiation, etc. In case of successful connection, the last line must read RUNNING... If this state is not reached within reasonable time, and no obvious errors are reported above (e.g. SIM missing), try limiting the timeout with the lte-port.provider...connect-waiting-time .

lte-port.show.down-count
: Output the number of reconnections. By dividing the total operation time of the device by this value, one may roughly estimate the average duration of an LTE session. A result of a few hours may typically be considered as acceptable. The perfect case is that reconnection occurs only by the provider's initiative (typically every 24 or 8 hours). If the counter increases by tens per day, and the average session lasts for less than one hour, the connection is bad and it worths changing something (e.g. selecting specific RAT modes or frequency bands manually).

lte-port.show.interface
: Show status and statistics of the IP interface attached to LTE port. E.g. one may see the IP address assigned by the provider. (Or none, if the port is not in operational status.)
In addition to standard Linux output, the active SIM card (main or aux) and the number of remaining attempts with this card are displayed.

lte-port.restart
: A one-time command for manual restart of the port. Optionally, main or aux may be typed in the input field to restart with a specified SIM card. (E.g. to test the connection with a particular operator.) If the card is not specified, the port follows its regular main.attempts/aux.attempts routine.

5.5. Services node

services
: Configuration of various application-level services.

services.http
: HTTP/HTTPS management setup.

services.http.enable
: Enable HTTP/HTTPS management.
Note: Setting this parameter to false disables both HTTP and HTTPS management. If only HTTPS should be allowed but not HTTP, the incoming HTTP traffic (over the specified TCP port) must be blocked by filters.

services.http.port
: TCP port to be used for HTTP access.

services.http.https
: Enable HTTPS **in addition** to HTTP. The TCP port for HTTPS is always 443 and is not configurable by admin.
Note: keys and certificates for HTTPS connections are generated automatically when needed. The certificate is self-signed. Follow instructions of your Web browser to set up an exclusion to accept it.

services.https.renew-cert
: One-time command to regenerate the certificates manually.

services.http.log
: View the log of the HTTP server.

services.ssh
: SSH management setup.

services.ssh.enable
: Enable SSH management.

services.ssh.port
: TCP port to be used for SSH access.

services.ssh.keygen
: One-time command to regenerate the SSH keys of this host (as SSH server) manually. Type yes in the input field to confirm the operation.
In normal operation, the keys are generated automatically when SSH is enabled for the first time.

services.ssh.log
: View log of the SSH server.

services.ssh.debug-level
: Set detalization level (0 thru 3) for SSH log messages.

services.ssh.options
: Extra options for SSH server. Not to be used in the given application.

services.telnet
: Telnet management setup.
Note: For security reasons, it is highly recommended to disable Telnet before putting the device into operation in real world, and use SSH instead.

services.telnet.enable
: Enable Telnet management.

services.telnet.port
: TCP port to be used for Telnet access.

netping
: Daemons to ping some test hosts in the network and to run specified scripts when the ping steadily fails or resumes.

netping.check-m1
: The preconfigured daemon to monitor connection over the LTE port. Monitoring is essential for LTE modules as they do not involve built-in monitoring capabilities (like LCP Echo for 2G/3G modules in PPP mode). In most cases, cellular modems detect the disconnection correctly and reconnect themselves; however, it is still possible — and unlikely to be completely avoided in any foreseeable future — that the module remains formally connected, yet with zero throughput. These are the situations when the external monitoring comes into the scene.

netping.check-m1.adm-state
: Administrative status of the daemon.

netping.check-m1.description
: Textual description of the daemon. Has no effect on actual operation.

netping.check-m1.mode
: Not to be altered in the given application.

netping.check-m1.log
: View the log of the netping daemon.

netping.check-m1.destination
: IP address or domain name of the test host. In the given example, the well-known Google DNS is used. Another reliable host may be chosen to user's discretion.

netping.check-m1.source
: Source IP address for outgoing *ping* packets. Optional. Not needed in the given application.

netping.check-m1.failure-script
netping.check-m1.restore-script
: Scripts to be run if the ping fails for the specified number of attempts in a row, and if the ping resumes, respectively. In the given application, the failure-script restarts the LTE port. Both not to be altered by user.

netping.check-m1.interval
netping.check-m1.packets
netping.check-m1.retry
netping.check-m1.timeout
Timeout parameters to detect the failure. The ping requests are sent in series, packets requests in one attempt, each waiting for the response for timeout seconds. If at least one response in received, the attempt is considered as successful. The next series starts in interval seconds after the previous one is completed. Once there are retry unsuccessful attempts in a row, a failure status is set and the failure-script is executed.
These parameters may be altered up to user's discretion.

netping.check-m1.start-delay
Initial delay before starting the daemon, to give the LTE port extra time to start and connect.

netping.check-m1.test-script
netping.check-m1.event-generator
Not to be used in the given application.

5.6. System node

system
General system configuration.

system.hostname
Set hostname of the given device, to distinguish it from the other ones.

system.clock-set
Set the system time manually, in the following format:
[YYYY-MM-DD] hh:mm[:ss]
This is a rather rough setting. NTP synchronization is preferable. See also timezone.

system.ntp
NTP client setup. Use to synchronize the system clock precisely over the network.

system.ntp.enable
Enable the NTP client.

system.ntp.host
The NTP server to synchronize with. It is highly recommended to synchronize all the devices in your network solution from a single source.

system.ntp.period
Interval between re-synchronizations. May be set in seconds (30...604800) or to hour, day, week.

system.ntp.log
View log of the NTP client.

system.timezone
Set local timezone.

system.timezone.location
: Select the geographic location from a list. Since there are only Russian locations in the list in the present software version, other is selected to set the time offset manually.

system.timezone.TZ
: TZ variable in Linux format. By default, set to Central European Time with Central European Summer Time.

system.factory-conf
: Set the configuration to the factory default and reboot. For this customized solution, the default NSGate configuration is restored.
To execute the command, type yes in the input field and click ▶.

system.reboot
: Reboot the device. To execute the command, type yes in the input field and click ▶.

system.software.full-update
: Update the software.

system.software.full-update.url
: Load the file with the new software from a third resource. The following URL syntax is accepted:
proto://[username[:password]@]host[:port]/[path]/file
where proto may be http, ftp, tftp, or file.

system.software.full-update.load-from-browser
: Load the file onto the device directly from your Web browser. To execute the command, select the file on your local PC and click ▶. Once the file is loaded, it is substituted automatically into the url field as a resource of the file:// type.

system.software.full-update.launch
: Launch the update, whichever of the above methods is used to transfer the file to the device. To execute the command, type yes in the input field and click ▶.
Note: The current configuration of the device is preserved during the update.

system.software.full-update.rm-loaded-file
: In case of loading file directly from the browser, you may decide to refuse from updating and remove the file already loaded to the device.

system.software.user-password-admin
: One-time command to set password for the admin user interactively.

system.software.user-password-nsg
: One-time command to set password for the nsg user interactively. nsg is an advanced user with full access to all the device features and is disabled in the NSGate factory configuration. To enable it, you should set the new password for it. Then exit the admin session and log in as nsg with its newly set password.
Once the desired operations for nsg are done, it is recommended to disable it again, to prevent damage from incautious use. For this purpose, set (in nsg session):
system.users.nsg.hash = "*"
save and apply the change. Then exit and re-login as admin.

Network Systems Group Ltd.
Volnaya 35
Moscow 105187 Russia
Phone/fax: (+7–495) 727–19–59

http://www.nsg.ru/
mailto:info@nsg.net.ru
mailto:sales@nsg.net.ru
mailto:support@nsg.net.ru