GWR-I Cellular Router Series

User Manual

version 1.0

date 10.08.2012.

Content

List of Figures

List of Tables

Description of the GWR-I Cellular Router Series

GWR-I router series represents a group of industrial graded routers specially designed for expansion of existing industrial networks, remote telemetry and data acquisition in harsh environments. Low transmission delay and very high data rates offered by existing cellular networks completely eliminate the need for very complex installation of wired infrastructure in industrial environments. Easy to install, reliable and high performance router models from GWR-I series introduce a completely new dimension into industrial networking area.

Figure 1 – GWR-I Router

The complete series inherited the basic concept of GWR cellular router series – **RELIABILITY COMES FIRST**. Therefore all router models have dual SIM card support. The form factor of the router is adjusted to industrial environments and DIN rail mounting kit is part of standard equipment for GWR-I series.

Many useful features make GWR-I cellular routers a perfect solution for wide variety of industrial applications:

- Dual SIM card support increases the reliability of the router and provides a solution for those applications where failure of one mobile network must not result in system downtime. Automatic failover feature will detect the failure of primary connection and automatically switch to alternative connection. When the connectivity over primary connection is restored GWR router will perform switchover to primary connection.

- The whole set of advanced WAN settings allow a user to specify desired parameters in order to meet the requirements of specific cellular network. GWR-I routers proved themselves to be reliable and high performance devices in so many countries around the world. All advanced parameters included represent the result of detailed analysis of large number of different cellular networks. In few simple steps it is possible to optimize the performance of the router on almost any cellular network.

- VPN (GRE, IPsec and OpenVPN) tunnel support provides powerful options for network expansion and secure data transfer over the cellular network.

- With Serial-to-IP feature it is possible to connect, control and perform data acquisition from almost any device with serial RS232 port. In addition to this feature, GWR-I router series implements ModbusRTU-to-ModbusTCP functionality designed to support expansion of Modbus SCADA networks over the cellular networks.

- Easy to use web interface, extended CLI (Command Line Interface), detailed log, SMS control feature, partial and full configuration Export/Import and remote management and monitoring software provide wide range of management functionalities. All those features and tools empower a user with full control over GWR-I routers.

Typical application

Data collection and system supervision

• Extra-high voltage equipment monitoring
• Running water, gas pipe line supervision
• Centralized heating system supervision
• Environment protection data collection
• Flood control data collection
• Alert system supervision
• Weather station data collection
• Power Grid
• Oilfield
• Light Supervision
• Solar PV Power Solutions

Financial and department store

• Connection of ATM machines to central site
• Vehicle based bank service
• POS
• Vending machine
• Bank office supervision

Security

• Traffic control
• Video Surveillance Solutions

Other

• Remote Office Solution
• Remote Access Solution

There are numerous variations of each and every one of above listed applications. Therefore GENEKO formed highly dedicated, top rated support team that can help you analyze your requirements and existing system, chose the right topology for your new system, perform initial configuration and tests and monitor the complete system after installation. Enhance your system performance and speed up the ROI with high quality cellular routers and all relevant knowledge of GWR support team behind you.

Technical Parameters

Complies with standards	EMC		Directive 2004/108/EC
			EN 301 489-1 V1.6.1(2005-09)
			EN 301 489-7 V1.3.1(2005-11)
	LVD		EN 60950-1:2001(1st Ed.) and/or EN 60950-1:2001
	R&TTE		Directive 1999/05/EC
			ETSI EN 301 511 V9.0.2
			EN 301 908-1 & EN 301 908-2(v2.2.1)
	RoHS		Directive 2002/95/EC
			EU Commission 2005/618/EC, 2005/717/EC, 2005/747/EC, 2006/310/EC, 2006/690/EC, 2006/691/EC and 2006/692/EC
Ethernet interface	Connector RJ-45 Standard: IEEE 802.3 Physical layer: 10/100Base-T Speed: 10/100Mbps Mode: full or half duplex		
Other interfaces	1 x RS-232C / RS485 / RS422 – RJ45 (+/- 15KV ESD protection) 1 x RS-232C / RS485 / RS422 – DB9 (+/- 15KV ESD protection) 1 x digital input (0/48VDC;1.5KV isolation) 1 x digital output (700mA@60VDC; 1.5KV isolation)		
RF characteristics	GWR-I202	GPRS	Tri-band: 900/1800/1900 GPRS multi-slot class 10, mobile station class B GPRS DL: 85.6Kbps, UL: 42.8Kbps
	GWR-I252	GPRS EDGE	Quad band: GSM 850/900/1800/1900MHz GPRS/EDGE multi-slot class 12, mobile station class B EDGE DL: 236.8Kbps, UL: 236.8Kbps GPRS DL: 85.6Kbps, UL: 85.6Kbps
	GWR-I352	GPRS EDGE UMTS HSPA	UMTS/HSDPA/HSUPA: Quad band, 850/900/1900/2100MHz GSM/GPRS/EDGE: Quad band, 850/900/1800/1900MHz GPRS/EDGE multi-slot class 12, mobile station class B HSUPA DL: 7.2Mbps, HSDPA: UL: 5.76Mbps UMTS DL: 384Kbps, UL: 384Kbps EDGE DL: 236.8Kbps, UL: 236.8Kbps GPRS DL: 85.6Kbps, UL: 85.6Kbps
RF Connector	SMA, 50Ω		
Status LED	Ethernet activity/network traffic Power on GSM link activity Signal quality Reset		
Power requirements	12 - 48VDC		
Environmental	Operating temperature: -25° C to 70° C (-13° F to 158° F) Storage temperature: -40° C to +75° C (-40° F to +167° F) Relative humidity: 5% to 95% (non-condensing)		

Dimensions and weight	Width: 50mm Length: 104mm Height: 135mm Weight: 500g
Housing and mounting options	Robust metal housing DIN rail mounting kit

Table 1 - Technical parameters

Protocols and features

Features	*Short description*
Network	
Routing	Static
DHCP Server: • **Static lease reservation** • **Address exclusions**	DHCP Server support
RIP	The Routing Information Protocol is a dynamic routing protocol used in local and wide area networks
Port forwarding	IP, TCP, UDP packets from WAN to LAN
DMZ support	**DMZ**, or **Demilitarized Zone**, is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
SNMPv1,2c	Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention
NTP(RFC1305)	The Network Time Protocol is a protocol for synchronizing the clocks of router
DynDNS	Dynamic DNS (DDNS) is a domain name service allowing to link dynamic IP addresses to static hostname. To start using this feature firstly you should register to DDNS service provider.
Firewall: • **NAT** • **PAT** • **IP filtering**	IP address / Network filtering
Serial-to-IP	Serial to Ethernet converter
Modbus RTU-to-TCP gateway	Modbus to Ethernet converter.
VPN	
GRE	Generic Routing Encapsulation is a tunneling protocol that can encapsulate a wide variety of network layer protocol packet types inside IP tunnels
GRE Keepalive	Keepalive for GRE tunnels
IPSec pass-through	ESP tunnels
IPsec	Internet Protocol Security is a suite of protocols for securing IP communications by authenticating and encrypting each IP packet of a data stream
OpenVPN	OpenVPN site to site graphical user interface (GUI) implementation allows connecting two remote networks via

	point-to-point encrypted tunnel. OpenVPN implementation offers a cost-effective simply configurable alternative to other VPN technologies.
IPSec IKE failover	Feature that allows a user to specify number of unsuccessful retries to establish PPP connection before routers switches to another SIM.
IPSec tunnel failover	Quality control mechanism of IPSec tunnel.
Management	
WEB Application	HTTP based
Command Line Interface	Serial console, telnet and SSH
GWR connection wizard	Initial setup utility.
SMS Control	Control the basic router functionalities by SMS.
Remote management and monitoring software	Additional software for management and control of large number of remote GWR/GWR-I routers.
Detailed system log	Advanced monitoring and diagnostics of the device.
Default reset	Reset the router to a factory default settings.
Firmware upload	Upgrade the firmware version on the router.
Configuration Export/Import	Partial or Full Export/Import of router configuration.

Table 2 – GWR-I Router features

Product Overview

Front panel

On the front panel (*Figure 2*) the following connectors are located:

- one RJ45 connector – Ethernet port for connection into local computer network;
- one RJ45 connector for RS232 serial communication;
- one DB9 connector for RS232/422/485 serial communication;
- reset button;

Ethernet connector LED:

- ACT (yellow) on – Network traffic detected (off when no traffic detected).
- Network Link (green LED) on - Ethernet activity or access point engaged.

LED Indicator Description:

1. Reset (red LED) on – the GWR-I Router reset state.
2. Power status (green LED) on – Power supply. Power status LED will blink when the GWR Router is in initializing state.
3. Link (red LED) will blink when connection is active.

4. Signal strength LED indicator:
    - –107 to –98 dBm = Weak (LED I)
    - –98 to –80 dBm = Moderate (LED II)
    - –80 or better dBm = Excellent (LED III).
    - 0 is not known or not detectable (running LED)

Signal strength LED will blink when GPRS/EDGE/HSPA/HSPA+/LTE connection is not active. When connection is active Signal strength LED is on. Reset condition will be indicated by blinks of the first and last Signal strength LED. When signal quality is not known or not detectable there will be running LED indication.

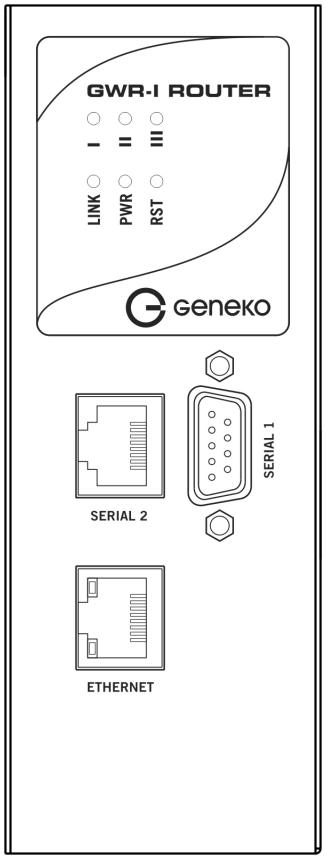


Figure 2 - GWR-I Router front panel

Top Panel

On the top panel following connectors are located:

- SMA connector for connection of the GSM/UMTS antenna
- Grounding connector
- 1 x digital input (0/48VDC;1.5KV isolation)
- 1 x digital output (700mA@60VDC; 1.5KV isolation)
- Detachable screw terminal for 9 - 48VDC power supply
- Reset button

The Reset button can be used for a warm reset or a reset to factory defaults.

Warm reset: If the GWR-I Router is having problem connecting to the Internet, press and hold the reset button for a second using the tip of a pen.

Reset to Factory Defaults: To restore the default settings of the GWR-I Router, hold the RESET button pressed for a few seconds. Restoration of the default configuration will be signaled by blinks of the first and last signal strength LED on the top panel. This will restore the factory defaults and clear all custom settings of the GWR-I Router. You can also reset the GWR-I Router to factory defaults using the Maintenance > Default Settings screen.

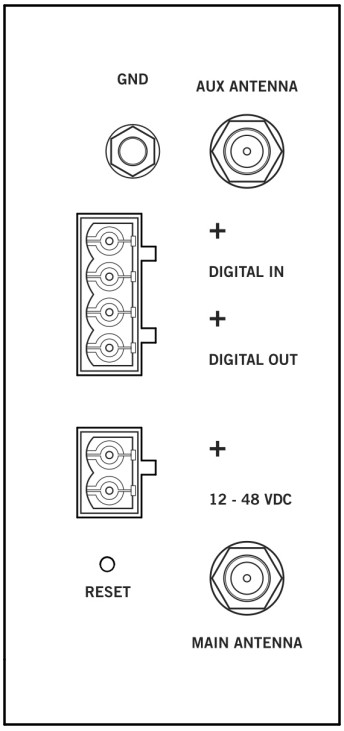


Figure 3 – GWR-I Router top panel side

Putting Into Operation

Before putting the GWR-I Router in operation it is necessary to connect all components needed for the operation:

- GSM antenna;
- Ethernet cable and
- SIM card must be inserted.

And finally, device should have powered up external power supply.

NOTE: Since the router is dedicated for operation in rough environments SIM card slots are located within the router chassis. In order to insert the SIM card please remove the screws pointed on the following image. SIM slots are located directly on the PCB of the router. After the SIM cards are inserted and before the router is put in the operation make sure that router box is properly sealed.

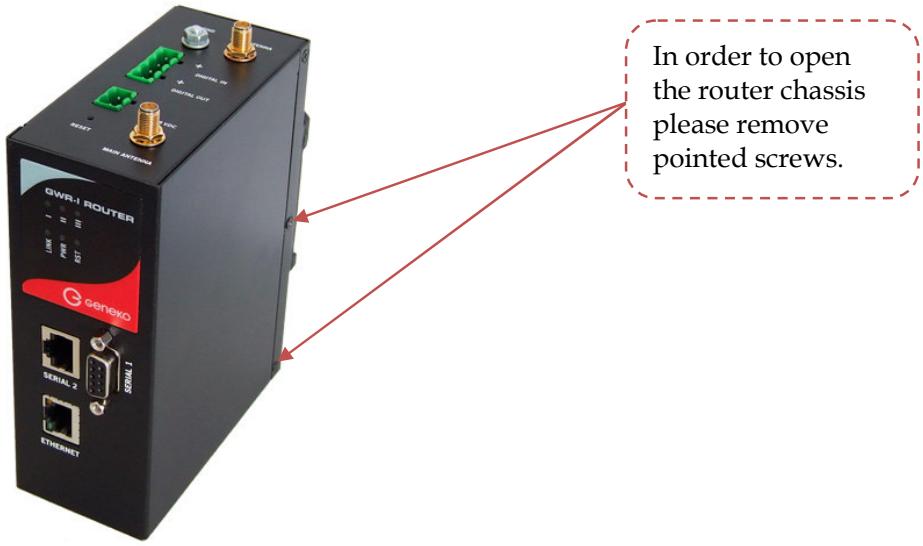


Figure 4 – Inserting the SIM card

SIM card must not be changed, installed or taken out while device operates. This procedure is performed when power supply is not connected.

Declaration of conformity

RB General Ekonomik
HARDWARE·SOFTWARE·ENGINEERING

CE

DECLARATION OF CONFORMITY

We hereby declare, that following product

COMMUNICATION EQUIPMENT WIRELESS ROUTER

Model/Type reference	Trade Mark	Ratings
GWR202-XXXXXX, GWR252-XXXXXX, GWR302-XXXXXX, GWR352-XXXXXX, GWR-I202-XXXXXX, GWR-I252-XXXXXX, GWR-I352-XXXXXX*	**GENEKO GWR ROUTER**	**Input for GWR routers: 9-12 V⎓1A** **Input for GWR-I routers: 12-48 V⎓1A**

* Where x can be any combination of numbers or characters, and represents non-safety relevant information

are in conformity with standards harmonised with directives:

LVD	IEC 60950-1:2005 (Second Edition), Am 1: 2009 Test report No. T223-0258/11
EMC	EN 301 489-1 V1.8.1 (2008-04) EN 301 489-7 V1.3.1 (2005-11) Test report No. T251-0689/11
R&TTE	Article 10 (5) and Annex IV of R&TTE Directive 1999/5/EC EN 60950-1:2006+A11:2009 EN 301 489-1 V1.8.1, EN 301 489-7 V1.3.1 EN 301 511 V9.0.2, EN 301 908-1 V3.2.1, EN 301 908-2 V3.2.1. Statement of Opinion No. 1304-R&TTE-C251-0119/11
RoHS	EU Directive 2002/95/EC EU Commission Decision 2005/618/EC, 2005/717/EC 2005/747/EC, 2006/310/EC, 2006/690/EC 2006/691/EC and 2006/692/EC Test report No. T211-0129/08

CE

Year of affixing of CE mark:

2008

Place and date:

Belgrade, August 08, 2012

Director

Borisav Bojkovic

RB GeneralEkonomik

Bul. Despota Sefana 59a · 11000 Belgrade · Serbia · Phone: +381 11 3340-591, 3340-178 · Fax: +381 11 3224-437 · office@geneko.rs · www.geneko.rs

Device Configuration

There are two methods which can be used to configure the GWR-I Router. Administrator can use following methods to access router:

- Web browser
- Command line interface

Default access method is by web interface. This method provides administrator full set of privileges for configuring and monitoring the router. Configuration, administration and monitoring of the GWR-I Router can be performed through the web interface. The default IP address of the router is 192.168.1.1. Another method is by command line interface. This method has limited options for configuring the GWR-I Router but still represents a very powerful tool when it comes to router setup and monitoring. Another document deals with CLI commands and instructions.

Device configuration using web application

The GWR-I Router's web-based utility allows you to set up the Router and perform advanced configuration and troubleshooting. This chapter will explain all of the functions in this utility.

For local access to the GWR-I Router's web-based utility, launch your web browser, and enter the Router's default IP address, 192.168.1.1, in the address field. A login screen prompts you for your User name and Password. Default administration credentials are admin/admin.

If you want to use web interface for router administration please enter IP address of router into web browser. Please disable *Proxy server* in web browser before proceed.

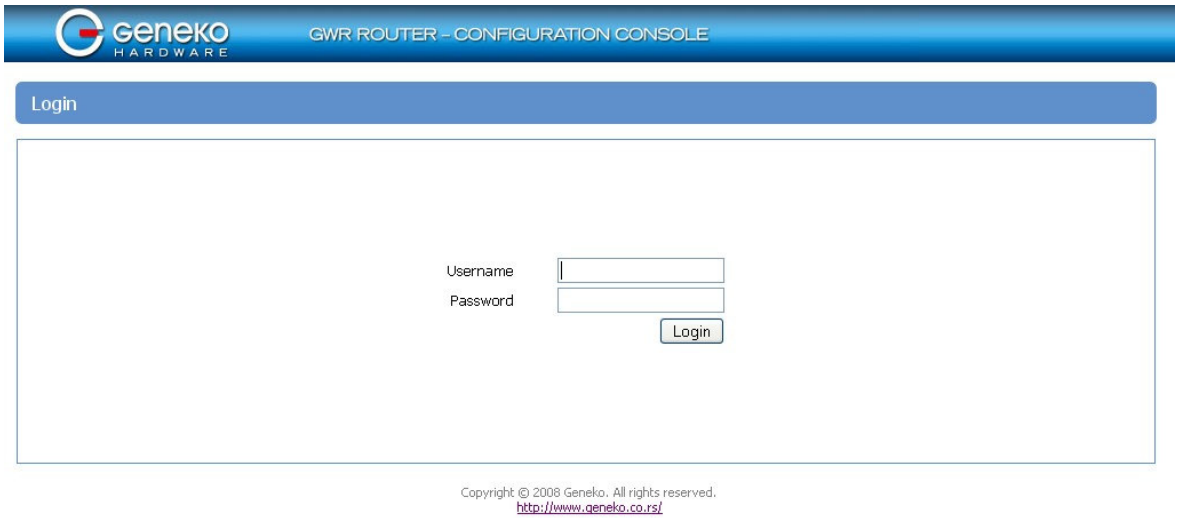


Figure 5 - User authentication

After successfully finished process of authentication of *Username/Password* you can access ***Main Configuration Menu***.

You can set all parameters of the GWR-I Router using web application. All functionalities and parameters are organized within few main tabs (windows).

NOTE

Add/Remove/Update manipulation in tables

*To **Add** a new row (new rule or new parameter) in the table please do following:*

- *Enter data in fields at the bottom row of the table (separated with a line).*
- *After entering data in all fields click **Add** link.*

*To **Update** the row in the table:*

- *Change data directly in fields you want to change*

*To **Remove** the row from the table:*

- *Click **Remove** link to remove selected row from the table.*

Save/Reload changes

*To save all the changes in the form press **Save** button. By clicking **Save** data are checked for validity. If they are not valid, error message will be displayed. To discard changes press the **Reload** button. By clicking **Reload**, previous settings will be loaded in the form.*

Status Information

The GWR-I Router's Status menu provides general information about router as well as real-time network information. Status information is divided into following categories:

- General Information,
- Network Information (LAN),
- WAN Information.

Status - General

General Information Tab provides general information about device type, device firmware version, kernel version, CPU vendor, Up Time since last reboot, hardware resources utilization and MAC address of LAN port. Screenshot of General Router information is shown at *Figure 6*. Data in Status menu are read only and cannot be changed by user. If you want to refresh screen data press ***Refresh*** button.

SIM Card detection is performed only at time booting the system, and you can see the status of SIM slot by checking the Enable SIM Card Detection option.

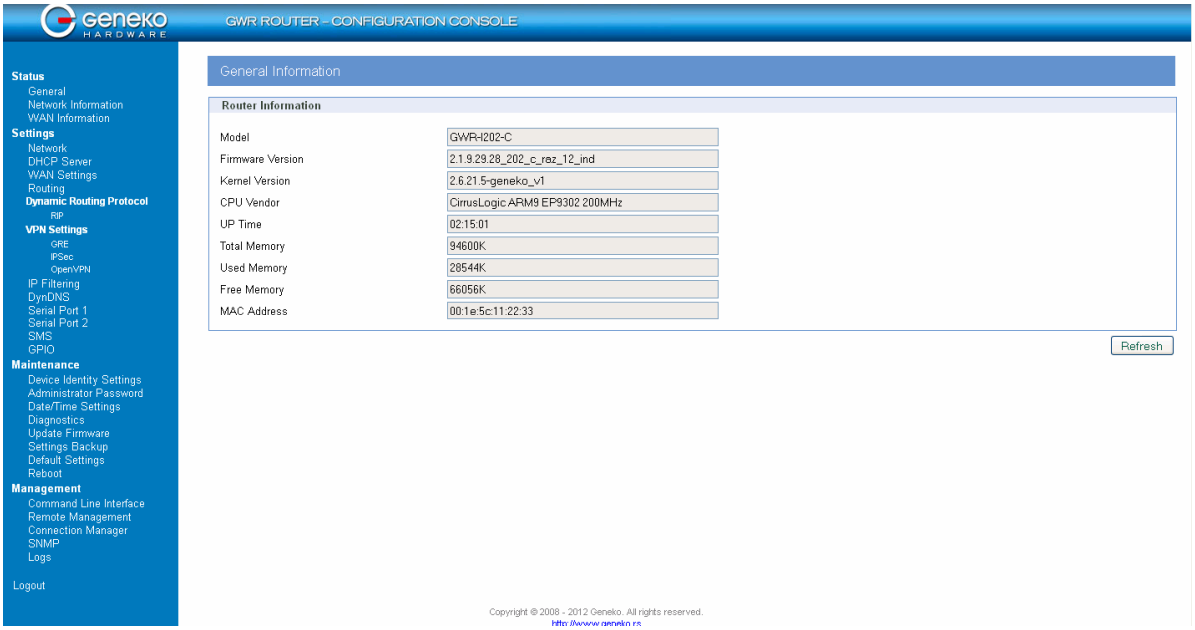


Figure 6 - General router information

Status - Network Information

Network Information Tab provides information about Ethernet port and Ethernet traffic statistics. Screenshot of Network Router information is shown in *Figure 7*.

Status - WAN Information

WAN Information Tab provides information about GPRS/EDGE/HSPA connection and traffic statistics. *WAN information menu* has three submenus which provide information about:

- GPRS/EDGE/HSPA mobile module(manufacturer and model);
- Mobile operator and signal quality;
- Mobile traffic statistics.

Screenshot of WAN information from the router is shown in *Figure 8*.

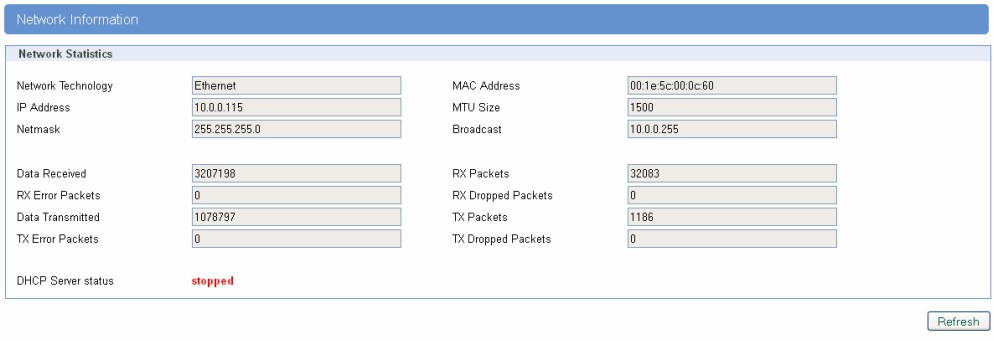


Figure 7 - Network Information

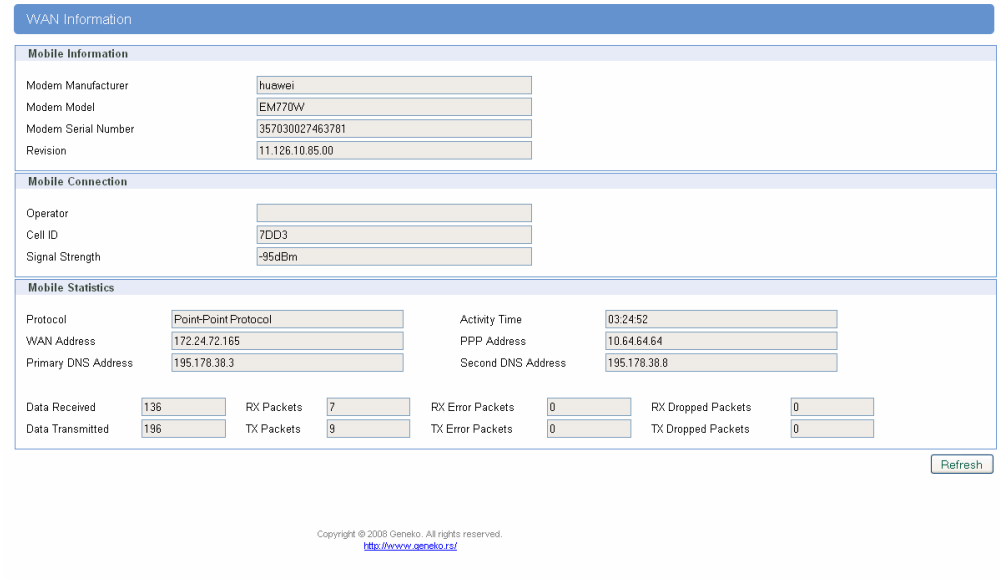


Figure 8 - WAN Information

Settings - Network

Click ***Network*** Tab, to open the LAN network screen. Use this screen to configure LAN TCP/IP settings.

Network Tab Parameters	
Label	**Description**
Use the following IP address	Choose this option if you want to manually configure TCP/IP parameters of Ethernet port.
IP Address	Type the IP address of your GWR-I Router in dotted decimal notation. 192.168.1.1 is the factory default IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. The GWR-I Router support sub-netting. You must specified subnet mask for your LAN TCP/IP settings.
Local DNS	Type the IP address of your local DNS server.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR-I Router. Whether you make changes or not, router will reboot every time you click ***Save***.

Table 3 - Network parameters

In the *Figure 9* you can see screenshot of ***Network*** Tab configuration menu.

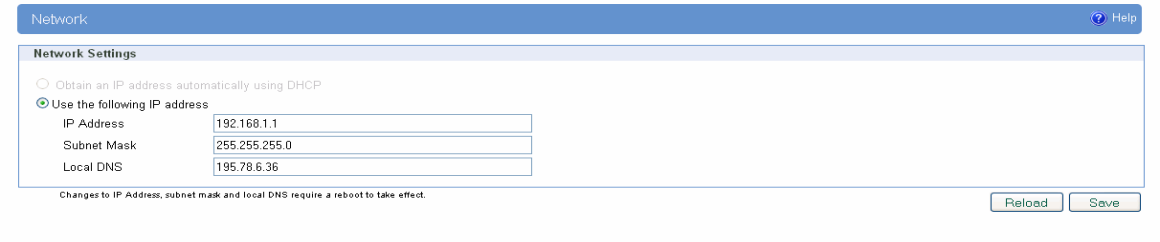


Figure 9 - Network parameters configuration page

Settings - DHCP Server

The GWR-I Router can be used as a DHCP (Dynamic Host Configuration Protocol) server on your network. A DHCP server automatically assigns available IP addresses to computers on your network. If you choose to enable the DHCP server option, all of the computers on your LAN must be set to obtain an IP address automatically from a DHCP server. (By default, Windows computers are set to obtain an IP automatically.)

To use the GWR-I Router as your network's DHCP server, click ***DHCP Server*** Tab for DHCP Server setup. The GWR-I Router has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DHCP Server Parameters	
Label	**Description**
Enable DHCP Server	DHCP (Dynamic Host Configuration Protocol) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. When configured as a server, the GWR-I Router provides TCP/IP configuration for the clients. To activate DHCP server, click check box ***Enable DHCP Server***. To setup DHCP server fill in the IP Starting Address and IP Ending Address fields. Uncheck ***Enable DHCP Server*** check box to stop the GWR-I Router from acting as a DHCP server. When Unchecked, you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Starting Address (From)	This field specifies the first of the contiguous addresses in the IP address pool.
IP Ending Address (To)	This field specifies last of the contiguous addresses in the IP address pool.
Lease Duration	This field specifies DHCP session duration time.
Primary DNS, Secondary DNS	This field specifies IP addresses of DNS server that will be assigned to systems that support DHCP client capability. Select ***None*** to stop the DHCP Server from assigning DNS server IP address. When you select None, computers must be manually configured with proper DNS IP address. Select ***Used by ISP*** to have the GWR-I Router assign DNS IP address to DHCP clients. DNS address is provided by ISP (automatically obtained from WAN side). This option is available only if GSM connection is active. Please establish GSM connection first and then choose this option. Select ***Used Defined*** to have the GWR-I Router assign DNS IP address to DHCP clients. DNS address is manually configured by user.
Static Lease Reservation	This field specifies IP addresses that will be dedicated to specific DHCP Client based on MAC address. DHCP server will always assign same IP address to appropriate client.
Address Exclusions	This field specifies IP addresses that will be excluded from the pool of DHCP IP address. DHCP server will not assign this IP to DHCP clients.
Add	Click ***Add*** to insert (add) new item in table to the GWR-I Router.
Remove	Click ***Remove*** to delete selected item from table.
Save	Click ***Save*** to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 4 - DHCP Server parameters

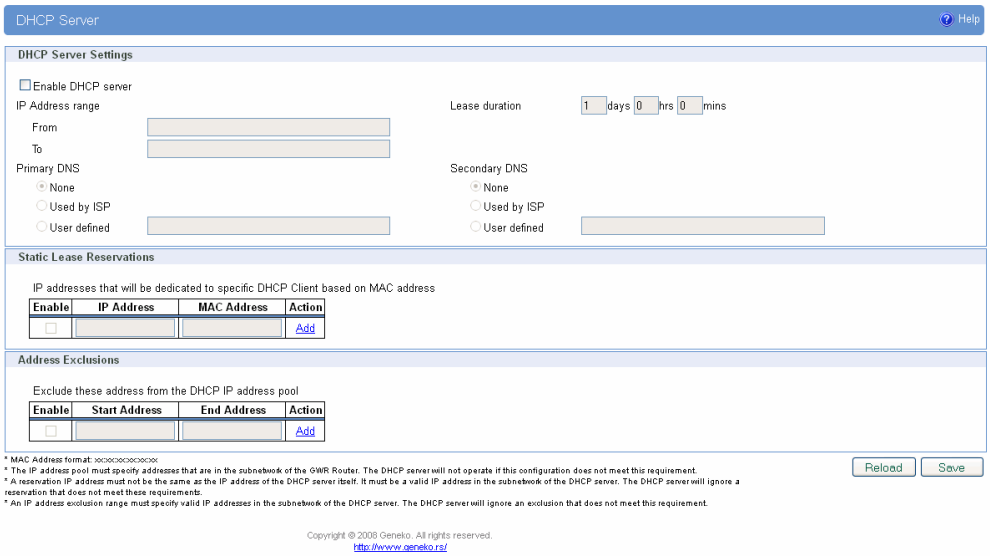


Figure 10 - DHCP Server configuration page

Settings - WAN Setting

Click ***WAN Settings*** Tab, to open the Wireless screen. Use this screen to configure the GWR-I Router GPRS/EDGE/HSPA/HSPA+/LTE parameters (Figure 11).

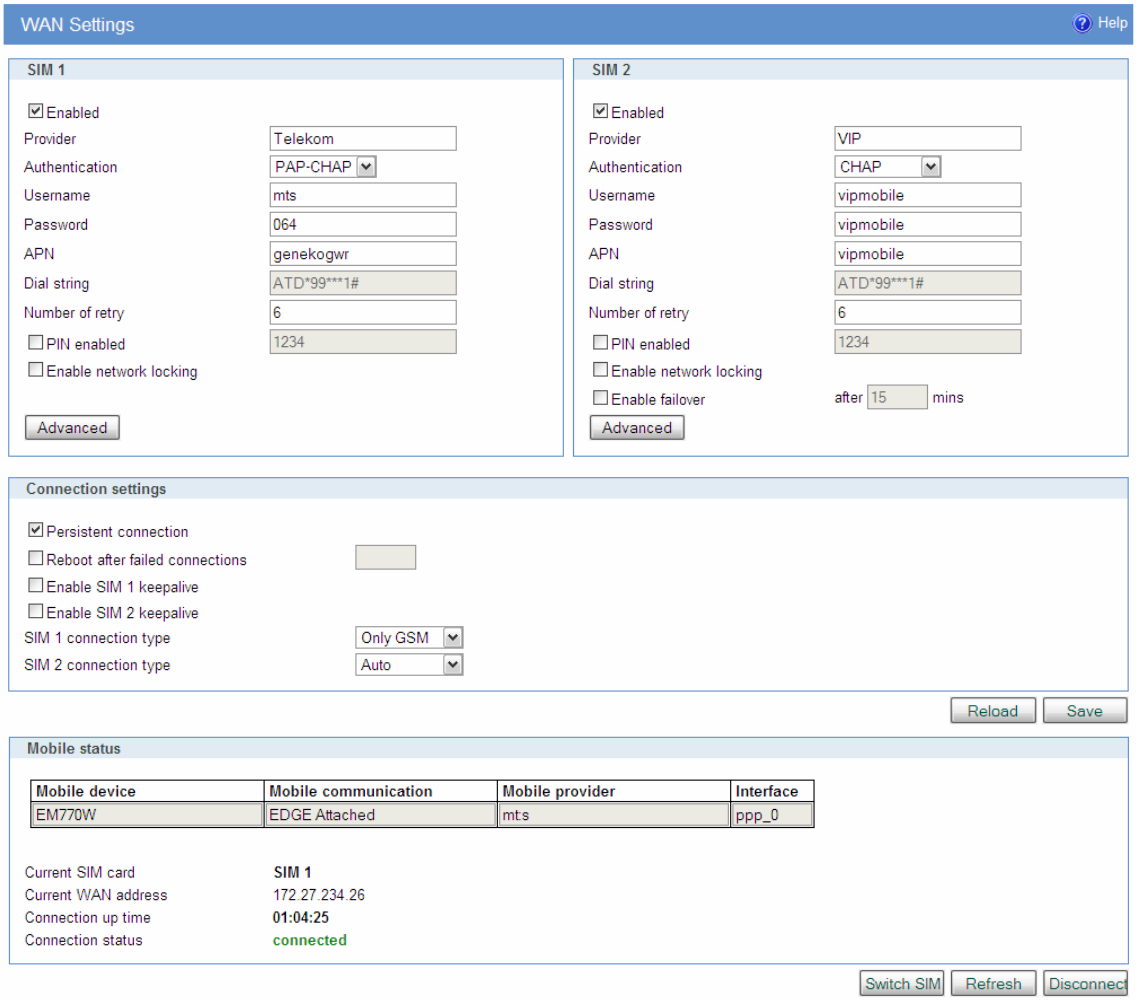


Figure 11 - WAN Settings configuration page

WAN Settings	
Label	**Description**
Provider	This field specifies name of GSM/UMTS ISP. You can setup any name for provider.
Authentication	This field specifies password authentication protocol. Select the appropriate protocol from drop down list. (PAP, CHAP, PAP - CHAP).
Username	This field specifies Username for client authentication at GSM/UMTS network. Mobile provider will assign you specific username for each SIM card.
Password	This field specifies Password for client authentication at GSM/UMTS network. Mobile provider will assign you specific password for each SIM card.
APN	This field specifies APN.

Dial String	This field specifies Dial String for GSM/UMTS modem connection initialization. In most cases you have to change only APN field based on parameters obtained from Mobile Provider. This field cannot be altered.
Enable Failover	Check this field in order to enable failover feature. This feature is used when both SIM are enabled. You specify the amount of time after which Failover feature brings down current WAN connection (SIM2) and brings up previous WAN connection (SIM1).
Enable network locking	Option that allows a user to lock a SIM card for a desired operator by specifying PLMN id of the operator. This option is very useful in border areas since you can avoid roaming expenses.
Persistent connection	Keep connection alive, after Do not exit after a connection is terminated. Instead try to reopen the connection
Reboot after failed connections	Reboot after n consecutive failed connection attempts.
Enable SIM1/SIM2 keepalive	Make some traffic periodically in order to maintain connection active. You can set keepalive interval value in minutes
Ping target	This field specifies the target IP address for periodical traffic generated using ping in order to maintain the connection active.
Ping interval	This field specifies ping interval for keepalive option.
Advanced ping interval	This field specifies the time interval of advanced ping proofing.
Advanced ping wait for a response	This field specifies the timeout for advanced ping proofing.
Maximum number of failed packets	This field specifies maximum number of failed packets in percent before keepalive action is performed.
Keepalive action	This menu provides a choice between two possible keepalive actions in case maximum number of failed packets is exceeded. If Switch SIM option is selected router will try to establish the connection using the other SIM card after the maximum number of failed packets is exceeded. If Current SIM option is selected router will only restart the PPP connection.
Connection type	Specifies the type of connection router will try to establish. There are three available options: only GSM, only UMTS and AUTO. For example, if you select Only GSM option, router will not try to connect to UMTS, instead router will automatically try to connect to GSM. By selecting AUTO option, router will first try to establish UMTS connection and if it fails, router will go for GSM connection.
Mobile status	Displays data related to mobile connection. (current WAN address, uptime, connection status…)
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR-I Router.
Switch SIM	Click Switch SIM try to establish the connection using the other SIM card.
Refresh	Click ***Refresh*** to see updated mobile network status.
Connect/ Disconnect	Click ***Connect/Disconnect*** to connect or disconnect from mobile network.

Table 5 - WAN parameters

Figure 11 shows screenshot of GSM/UMTS tab configuration menu. GSM/UMTS menu is divided into two parts.

- Upper part provides all parameters for configuration GSM/UMTS connection. These parameters can be obtained from Mobile Operator. Please use exact parameters given from Mobile Operator.
- Bottom part is used for monitoring status of GSM/UMTS connection (create/maintain/destroy GSM/UMTS connection). Status line show real-time status: connected/disconnected.

If your SIM Card credit is too low, the GWR-I Router will performed periodically connect/disconnect actions.

WAN Settings(advanced)	
Label	**Description**
Enable	This field specifies if Advanced WAN settings is enabled at the GWR-I Router.
Accept Local IP Address	With this option, pppd will accept the peer's idea of our local IP address, even if the local IP address was specified in an option.
Accept Remote IP Address	With this option, pppd will accept the peer's idea of its (remote) IP address, even if the remote IP address was specified in an option.
Idle time before disconnect (sec)	Specifies that pppd should disconnect if the link is idle for *n* seconds. The link is idle when no data packets are being sent or received.
Refuse PAP	With this option, pppd will not agree to authenticate itself to the peer using PAP.
Require PAP	Require the peer to authenticate using PAP (Password Authentication Protocol) authentication.
Refuse CHAP	With this option, pppd will not agree to authenticate itself to the peer using CHAP.
Require CHAP	Require the peer to authenticate using CHAP (Challenge Handshake Authentication Protocol) authentication.
Max. CHAP challenge transmissions	Set the maximum number of CHAP challenge transmissions to *n* (default 10).
CHAP restart interval sec	Set the CHAP restart interval (retransmission timeout for challenges) to *n* seconds (default 3).
Refuse MS-CHAP	With this option, pppd will not agree to authenticate itself to the peer using MS-CHAP.
Refuse MS-CHAPv2	With this option, pppd will not agree to authenticate itself to the peer using MS-CHAPv2.
Refuse EAP	With this option, pppd will not agree to authenticate itself to the peer using EAP.
Connection debugging	Enables connection debugging facilities. If this option is selected, pppd will log the contents of all control packets sent or received in a readable form.
Maximum Transmit Unit (bytes)	Set the MTU (Maximum Transmit Unit) value to *n*. Unless the peer requests a smaller value via MRU negotiation, pppd will request that the kernel networking code send data packets of no more than *n* bytes through the PPP network interface.
Maximum Receive Unit (bytes)	Set the MRU (Maximum Receive Unit) value to *n*. Pppd will ask the peer to send packets of no more than *n* bytes. The value of *n* must be between 128 and 16384; the default is 1500.

VJ-Compression	Disable Van Jacobson style TCP/IP header compression in both directions.
VJ-Connection-ID Compression	Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression. With this option, pppd will not omit the connection-ID byte from Van Jacobson compressed TCP/IP headers.
Protocol Field Compression	Disable protocol field compression negotiation in both directions.
Address/Control Compression	Disable Address/Control compression in both directions.
Predictor-1 Compression	Disable or enable accept or agree to Predictor-1 compression.
BSD Compression	Disable or enable BSD-Compress compression.
Deflate Compression	Disable or enable Deflate compression.
Compression Control Protocol negotiation	Disable CCP (Compression Control Protocol) negotiation. This option should only be required if the peer is buggy and gets confused by requests from pppd for CCP negotiation.
Magic Number negotiation	Disable magic number negotiation. With this option, pppd cannot detect a looped-back line. This option should only be needed if the peer is buggy.
Passive Mode	Enables the "passive" option in the LCP. With this option, pppd will attempt to initiate a connection; if no reply is received from the peer, pppd will then just wait passively for a valid LCP packet from the peer, instead of exiting, as it would without this option.
Silent Mode	With this option, pppd will not transmit LCP packets to initiate a connection until a valid LCP packet is received from the peer (as for the "passive" option with ancient versions of pppd).
Append domain name	Append the domain name *d* to the local host name for authentication purposes.
Show PAP password in log	When logging the contents of PAP packets, this option causes pppd to show the password string in the log message.
Time to wait before re-initiating the link (sec)	Specifies how many seconds to wait before re-initiating the link after it terminates. The holdoff period is not applied if the link was terminated because it was idle.
LCP-Echo-Failure	If this option is given, pppd will presume the peer to be dead if *n* LCP echo-requests are sent without receiving a valid LCP echo-reply. If this happens, pppd will terminate the connection. This option can be used to enable pppd to terminate after the physical connection has been broken (e.g., the modem has hung up) in situations where no hardware modem control lines are available.
LCP-Echo-Interval	If this option is given, pppd will send an LCP echo-request frame to the peer every *n* seconds. Normally the peer should respond to the echo-request by sending an echo-reply. This option can be used with the *lcp-echo-failure* option to detect that the peer is no longer connected.
Use Peer DNS	With this option enabled, router resolves addresses using ISP's DNS servers.
Modem Initialization String	This field provides an option to directly specify AT commands.
Roaming Mode	By enabling this option router will be able to connect to roaming network.

Table 6 – Advanced WAN Settings

Settings – Routing

The static routing function determines the path that data follows over your network before and after it passes through the GWR-I Router. You can use static routing to allow different IP domain users to access the Internet through the GWR-I Router. Static routing is a powerful feature that should be used by advanced users only. In many cases, it is better to use dynamic routing because it enables the GWR-I Router to automatically adjust to physical changes in the network's layout.

The GWR-I Router is a fully functional router with static routing capability. *Figure 12* shows screenshot of Routing page.

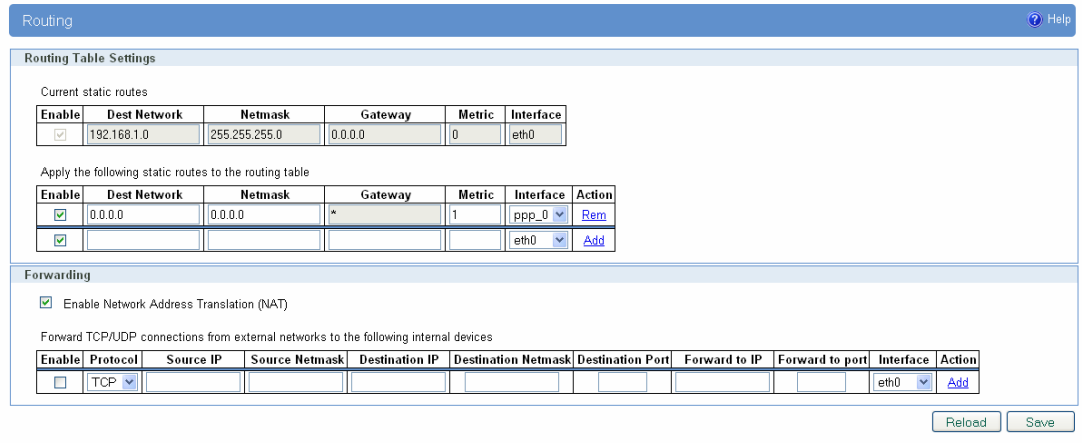


Figure 12 – Routing configuration page

Use this menu to setup all routing parameters. Administrator can perform following operations:

- Create/Edit/Remove routes (including default route),
- Port translation – Reroute TCP and UPD packets to desired destination inside the network.

Routing Settings	
Label	**Description**
Routing Table	
Enable	This check box allows you to activate/deactivate this static route.
Source IP	Source IP address from which portforwarding is allowed, all other traffic is denied
Source Netmask	Subnet mask for allowed IP subnet
Dest Network	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Netmask	This parameter specifies the IP netmask address of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch (next hope) on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their final destinations. For every routing rule enter the IP address of the gateway. Please notice that *ppp0* interface has only one default gateway (provided by Mobile operator) and because of that that there is no option for gateway when you choose *ppp0* interface.

Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Interface	Interface represents the "exit" of transmission for routing purposes. In this case *Eth0* represents LAN interface and *ppp0* represents GSM/UMTS mobile interface of the GWR-I Router.
TCP/UDP Traffic forwarding	
Enable	This check box allows you to activate/deactivate this static port translation.
Protocol	Choose between TCP and UDP protocol.
Destination IP	This field specifies IP address of the incoming traffic.
Destination Netmask	This field specifies netmask for the previous address.
Destination Port	This is the TCP/UDP port of application.
Forward to IP	This filed specifies IP address where packets should be forwarded.
Forward to port	Specify TCP/UDP port on which the traffic is going to be forwarded.
Interface	Select interface where portforwarding is done. Portforwarding from outside (WAN) interface to inside (LAN) interface is done on PPP, and in reverse direction on Ethernet interface
Add	Click ***Add*** to insert (add) new item in table to the GWR-I Router.
Remove	Click Remove to delete selected item from table.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR-I Router. After pressing ***Save*** *button* it make take more than 10 seconds for router to save parameters and become operational again.

Table 7 – Routing parameters

Port translation

For incoming data, the GWR-I Router forwards IP traffic destined for a specific port, port range or GRE/IPsec protocol from the cellular interface to a private IP address on the Ethernet "side" of the GWR-I Router.

Settings – Dynamic Routing Protocol

Dynamic routing performs the same function as static routing except it is more robust. Static routing allows routing tables in specific routers to be set up in a static manner so network routes for packets are set. If a router on the route goes down the destination may become unreachable. Dynamic routing allows routing tables in routers to change as the possible routes change.

Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP) using the distance-vector routing

algorithm. The Routing Information Protocol provides great network stability, guaranteeing that if one network connection goes down the network can quickly adapt to send packets through another connection.

Click ***RIP*** Tab, to open the Routing Information Protocol screen. Use this screen to configure the GWR-I Router RIP parameters (*Figure 13*).

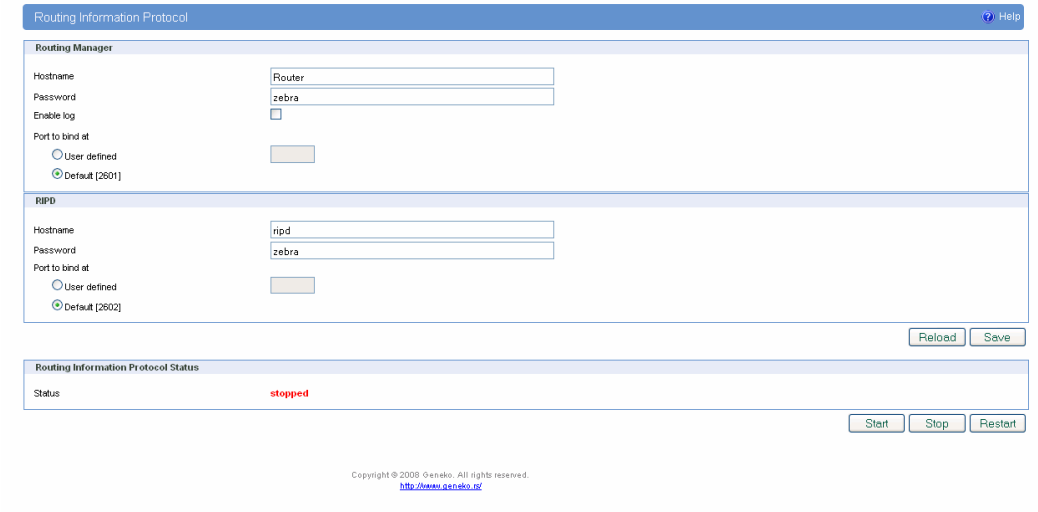


Figure 13 – RIP configuration page

RIP Settings	
Label	**Description**
Routing Manager	
Hostname	Prompt name that will be displayed on telnet console.
Password	Login password.
Enable log	Enable log file.
Port to bind at	Local port the service will listen to.
RIPD	
Hostname	Prompt name that will be displayed on telnet console of the Routing Information Protocol Manager.
Password	Login password.
Port to bind at	Local port the service will listen to.
Routing Information Protocol Status	
Start	Start RIP.
Stop	Stop RIP.
Restart	Restart RIP.
Save	Click ***Save*** to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 8 – RIP parameters

RIP routing engine for the GWR-I Router

Use telnet to enter in global configuration mode.

```
telnet 192.168.1.1 2602     // telnet to eth0 at TCP port 2602///
```

To enable RIP, use the following commands beginning in global configuration mode:

```
router# router rip
```

To associates a network with a RIP routing process, use following commans:

```
router# network [A.B.C.D/Mask]
```

By default, the GWR-I Router receives RIP version 1 and version 2 packets. You can configure the GWR-I Router to receive an send only version 1. Alternatively, tou can configure the GWR-I Router to receive and send only version 2 packets. To configure GWR-I Router to send and receive packets from only one version, use the following command:

```
router# rip version [1|2]       // Same as other router //
```

Disable route redistribution:

```
router# no redistribute kernel
router# no redistribute static
router# no redistribute connected
```

Disable RIP update (optional):

```
router# passive-interface eth0
router# no passive-interface eth0
```

Routing protocols use several timer that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, an other parameters. You can adjust these timer to tune routing protocol performance to better suit your internetwork needs. Use following command to setup RIP timer:

```
router# timers basic [UPDATE-INTERVAL] [INVALID] [TIMEOUT] [GARBAGE-COLLECT]
router# no timers basic
```

Configure interface for RIP protocol

```
router# interface greX
router# ip rip send version [VERSION]
router# ip rip receive version [VERSION]
```

Disable rip authentication at all interface.

```
Router(interface)# no ip rip authentication mode [md5|text]
```

Debug commands:

```
router# debug rip
router# debug rip events
router# debug rip packet
router# terminal monitor
```

Settings – VPN Settings

Virtual private network (VPN) is a communications network tunneled through another network and dedicated to a specific network. One common application of VPN is secure communication through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

A VPN may have best-effort performance, or may have a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point. The distinguishing characteristics of VPNs are not security or performance, but that they overlay other network(s) to provide a certain functionality that is meaningful to a user community.

Generic Routing Encapsulation (GRE)

Originally developed by Cisco, generic routing encapsulation (GRE) is now a standard, defined in RFC 1701, RFC 1702, and RFC 2784. GRE is a tunneling protocol used to transport packets from one network through another network.

If this sounds like a virtual private network (VPN) to you, that's because it theoretically is: Technically, a GRE tunnel is a type of a VPN — but it isn't a secure tunneling method. However, you can encrypt GRE with an encryption protocol such as IPSec to form a secure VPN. In fact, the point-to-point tunneling protocol (PPTP) actually uses GRE to create VPN tunnels. For example, if you configure Microsoft VPN tunnels, by default, you use PPTP, which uses GRE.

Solution where you can use GRE protocol:

- You need to encrypt multicast traffic. GRE tunnels can carry multicast packets — just like real network interfaces — as opposed to using IPSec by itself, which can't encrypt multicast traffic. Some examples of multicast traffic are OSPF, EIGRP. Also, a number of video, VoIP, and streaming music applications use multicast.
- You have a protocol that isn't routable, such as NetBIOS or non-IP traffic over an IP network. You could use GRE to tunnel IPX/AppleTalk through an IP network.
- You need to connect two similar networks connected by a different network with different IP addressing.

Click ***VPN Settings*** Tab, to open the VPN configuration screen. In the *Figure 14* you can see screenshot of ***GRE*** Tab configuration menu.

VPN Settings / GRE Tunneling Parameters	
Label	**Description**
Enable	This check box allows you to activate/deactivate VPN/GRE traffic.
Local Tunnel Address	This field specifies IP address of virtual tunnel interface.
Local Tunnel Netmask	This field specifies the IP netmask address of virtual tunnel. This field is unchangeable, always 255.255.255.252
Tunnel Source	This field specifies IP address or hostname of tunnel source.
Tunnel Destination	This field specifies IP address or hostname of tunnel destination.
Interface	This field specifies GRE interface. This field gets from the GWR-I Router.
KeepAlive Enable	Check for keepalive enable.
Period	Defines the time interval (in seconds) between transmitted keepalive packets. Enter a number from 3 to 60 seconds.
Retries	Defines the number of times retry after failed keepalives before determining that

	the tunnel endpoint is down. Enter a number from 1 to 10 times.
Add	Click ***Add*** to insert (add) new item in table to the GWR-I Router.
Remove	Click ***Remove*** to delete selected item from table.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR-I Router.

Table 9 – GRE parameters

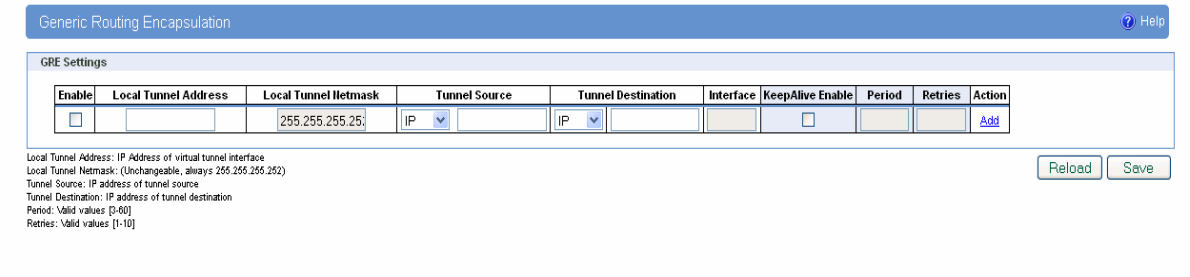


Figure 14 – GRE tunnel parameters configuration page

GRE Keepalive

GRE tunnels can use periodic status messages, known as keepalives, to verify the integrity of the tunnel from end to end. By default, GRE tunnel keepalives are disabled. Use the keepalive check box to enable this feature. Keepalives do not have to be configured on both ends of the tunnel in order to work; a tunnel is not aware of incoming keepalive packets. You should define the time interval (in seconds) between transmitted keepalive packets. Enter a number from 1 to 60 seconds, and the number of times to retry after failed keepalives before determining that the tunnel endpoint is down. Enter a number from 1 to 10 times.

Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol communication by authenticating and encrypting each IP packet of a data stream.
Click ***VPN Settings*** Tab, to open the VPN configuration screen. At the *Figure 17* you can see IPSec Summary screen. This screen gathers information about settings of all defined IPSec tunnels. You can define up to 5 Device-to-Device tunnels. Two different firmware versions of GWR-I have slightly different IPSec Advanced options.
First firmware version provides single Negotiation mode:

- Main

Second version has IPSec Negotiation mode options:

- Aggressive
- Main
- Base

Router is delivered with first firmware version as more reliable and secure solution. Only with this version you have option to define IKE retry failover mechanism and log level of IPSec system messages.
If you cannot use IP address as a peer identifier at one side of the tunnel (private IP subnet) aggressive mode has to be utilized (second version)

Default firmware version (without Aggressive Mode)

IPSec Summary and IPSec Settings related with second firmware version are briefly displayed in following figures and tables

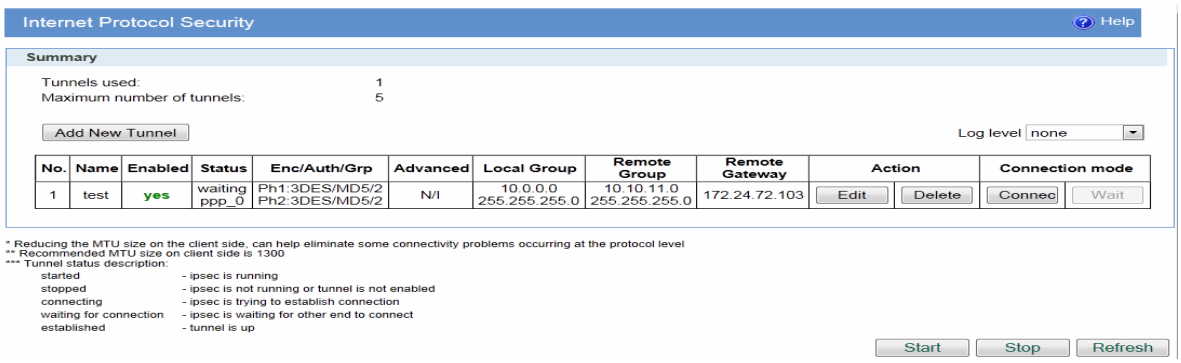


Figure 15 - IPSec Summary screen for second firmware version

VPN Settings / IPSec Summary	
Label	**Description**
Tunnels Used	This is the number of IPSec tunnels being defined.
Maximum number of tunnels	This is the maximum number of tunnels which can be defined.
No	This filed indicates the number of the IPSec tunnel.
Name	Field shows the Tunnel Name that you gave to the IPSec tunnel.
Enabled	This field shows if tunnel is enabled or disabled. After clicking on ***Start*** button,

	only enabled tunnels will be started.
Status	Field indicates status of the IPSec tunnel. Click on ***Refresh*** button to see current status of defined IPSec tunnels.
Enc/Auth/Grp	This field shows both Phase 1 and Phase 2 details, Encryption method (DES/3DES/AES), Authentication method (MD5/SHA1), and DH Group number (1/2/5) that you have defined in the IPSec Setup section.
Advanced	Field shows the chosen options from IPSec Advanced section by displaying the first letters of enabled options.
Local Group	Field shows the IP address and subnet mask of the Local Group.
Remote Group	Field displays the IP address and subnet mask of the Remote Group.
Remote Gateway	Field shows the IP address of the Remote Device.
Connection mode	Field displays connection mode of the current tunnel ***Connect -*** IPSec tunnel initiating side in negotiation process ***Wait -*** IPSec tunnel responding side in negotiation process
Log level	Set IPSec log level
Delete	Click on this link to delete the tunnel and all settings for that particular tunnel.
Edit	This link opens screen where you can change the tunnel's settings.
Add New Tunnel	Click on this button to add a new Device-to-Device IPSec tunnel. After you have added the tunnel, you will see it listed in the Summary table.
Start	This button starts the IPSec negotiations between all defined and enabled tunnels. If the IPSec is already started, Start button is replaced with Restart button.
Stop	This button will stop all IPSec started negotiations.
Refresh	Click on this button to refresh the Status field in the Summary table.

Table 10 - IPSec Summary for second firmware version

To create a tunnel click Add New Tunnel button. Depending on your selection, the Local Group Setup and Remote Group Setup settings will differ. Proceed to the appropriate instructions for your selection.

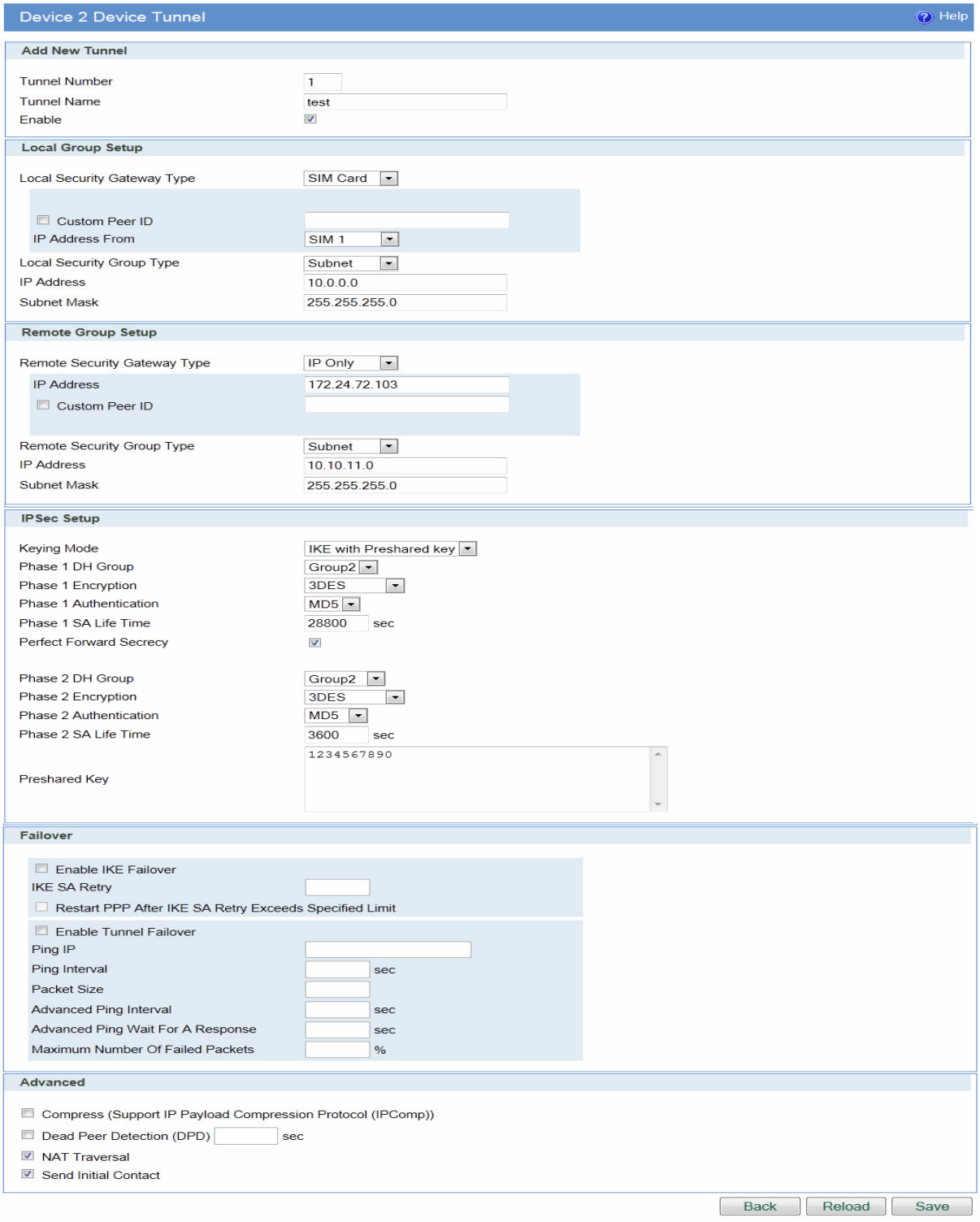


Figure 16 - IPSec Settings for second firmware version

VPN Settings / IPSec Settings	
Label	**Description**
Tunnel Number	This number will be generated automatically and it represents the tunnel number.
Tunnel Name	Enter a name for the IPSec tunnel. This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
Enable	Check this box to enable the IPSec tunnel.
IPSec Setup	In order to establish an encrypted tunnel, the two ends of an IPSec tunnel must agree on the methods of encryption, decryption and authentication. This is done by sharing a key to the encryption code. For key management, the Router uses only IKE with Preshared Key mode.
Keying Mode	**IKE with Preshared Key** IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Preshared Key to authenticate the remote IKE peer. Both ends of IPSec tunnel must use the same mode of key management. **Certificates** This option will be available in future release
Phase 1 DH Group	Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol used during Phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits and Group 5 is 1536 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.
Phase 1 Encryption	Select a method of encryption: DES (56-bit), 3DES (168-bit) or AES-128 (128-bit). The method determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Make sure both ends of the IPSec tunnel use the same encryption method.
Phase 1 Authentication	Select a method of authentication: MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the IPSec tunnel use the same authentication method.
Phase 1 SA Life Time	Configure the length of time IPSec tunnel is active in Phase 1. The default value is 28800 seconds. Both ends of the IPSec tunnel must use the same Phase 1 SA Life Time setting.
Perfect Forward Secrecy	If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys. Both ends of the IPSec tunnel must enable this option in order to use the function.
Phase 2 DH Group	If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits, and Group 5 is 1536 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You do not have to use the same DH Group that you used for Phase 1, but both ends of the IPSec tunnel must use the same Phase 2 DH Group.
Phase 2 Encryption	Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. Select a method of encryption: NULL, DES (56-bit), 3DES (168-bit) or AES-128 (128-bit). It determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Both ends of the IPSec tunnel must use the same Phase 2 Encryption setting.

	NOTE: If you select a NULL method of encryption, the next Phase 2 Authentication method cannot be NULL and vice versa.
Phase 2 Authentication	Select a method of authentication: NULL, MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Both ends of the IPSec tunnel must use the same Phase 2 Authentication setting. *NOTE: If you select a NULL method of authentication, the previous Phase 2 Encryption method cannot be NULL.*
Phase 2 SA Life Time	Configure the length of time an IPSec tunnel is active in Phase 2. The default is 3600 seconds. Both ends of the IPSec tunnel must use the same Phase 2 SA Life Time setting.
Preshared Key	This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., Ay_%4222 or 345fa929b8c3e. This field allows a maximum of 1023 characters and/or hexadecimal values. Both ends of the IPSec tunnel must use the same Preshared Key. *NOTE: It is strongly recommended that you periodically change the Preshared Key to maximize security of the IPSec tunnels.*
Local Security gateway type	When **SIM Card** is selected the WAN (or Internet) IP address of the Router automatically appears. If the Router is not yet connected to the GSM/UMTS network this field is without IP address.
Custom Peer ID	Authentication identity for one of the participant. Can be an IP address or fully-qualified domain name preceded by @
IP Address From	Select SIM card over which the tunnel is established
Local Security Group Type	Select the local LAN user(s) behind the Router that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. *NOTE: The Local Security Group Type you select should match the Remote Security Group Type selected on the IPSec device at the other end of the tunnel.*
IP Address	Only the computer with a specific IP address will be able to access the tunnel.
Subnet Mask	Enter the subnet mask.
Remote Security Gateway Type	Select the remote LAN user(s) behind the Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. *NOTE: The Remote Security Group Type you select should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.*
IP Address	Only the computer with a specific IP address will be able to access the tunnel.
Custom Peer ID	Authentication identity for one of the participant. Can be an IP address or fully-qualified domain name preceded by @
Remote Security Group Type	Select the remote LAN user(s) behind the Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. *NOTE: The Remote Security Group Type you select should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.*
IP Address	Only the computer with a specific IP address will be able to access the tunnel.
Subnet Mask	Enter the subnet mask.
Enable IKE failover	Enable IKE failover option which try periodically to reastablish security association.

IKE SA retry	Number of IKE retries, before failover.
Enable tunnel failover	Enable tunnel failover. If there is more than one tunnel defined, this option will failover to other tunnel in case that selected one fails to established connection.
Ping IP	IP address on other side of tunnel which will be pinged in order to determine current state.
Ping interval	Specify time period in seconds between two ping
Packet size	Specify packet size for ping message
Advanced Ping Interval	Time interval between advanced ping packets.
Advanced Ping Wait For A Response	Advanced ping proofing timeout.
Maximum numbers of failed packets	Set percentage of failed packets until failover action is performed.
Compress (IP Payload Compression Protocol (IP Comp))	IP Payload Compression is a protocol that reduces the size of IP datagram. Select this option if you want the Router to propose compression when it initiates a connection.
Dead Peer Detection (DPD)	When DPD is enabled, the Router will send periodic HELLO/ACK messages to check the status of the IPSec tunnel (this feature can be used only when both peers or IPSec devices of the IPSec tunnel use the DPD mechanism). Once a dead peer has been detected, the Router will disconnect the tunnel so the connection can be re-established. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent). The default interval is 20 seconds.
NAT Traversal	Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947. *NOTE: If you select this mode the Aggressive mode will be automatically selected because it is obligatory option for NAT-T to work properly.* *NOTE: Keep-alive for NAT-T function is enabled by default and cannot be disabled. The default interval for keep-alive packets is 20 seconds.*
Send initial contact	The initial-contact status message may be used when one side wishes to inform the other that this is the first SA being established with the remote system. The receiver of this Notification Message might then elect to delete any existing SA's it has for the sending system under the assumption that the sending system has rebooted and no longer has access to the original SA's and their associated keying material.
Back	Click ***Back*** to return on IPSec Summary screen.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR-I Router. After that router automatically goes back and begin negotiations of the tunnels by clicking on the Start button.

Table 11 - IPSec Parameters for second firmware version

Alternative firmware version (Aggressive Mode supported)

IPSec Summary and IPSec Settings related with first firmware version are briefly displayed in following figures and tables below

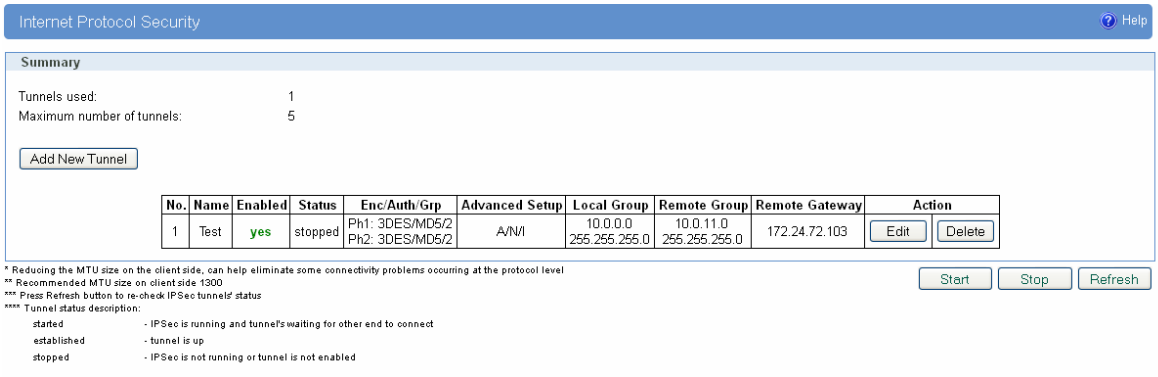


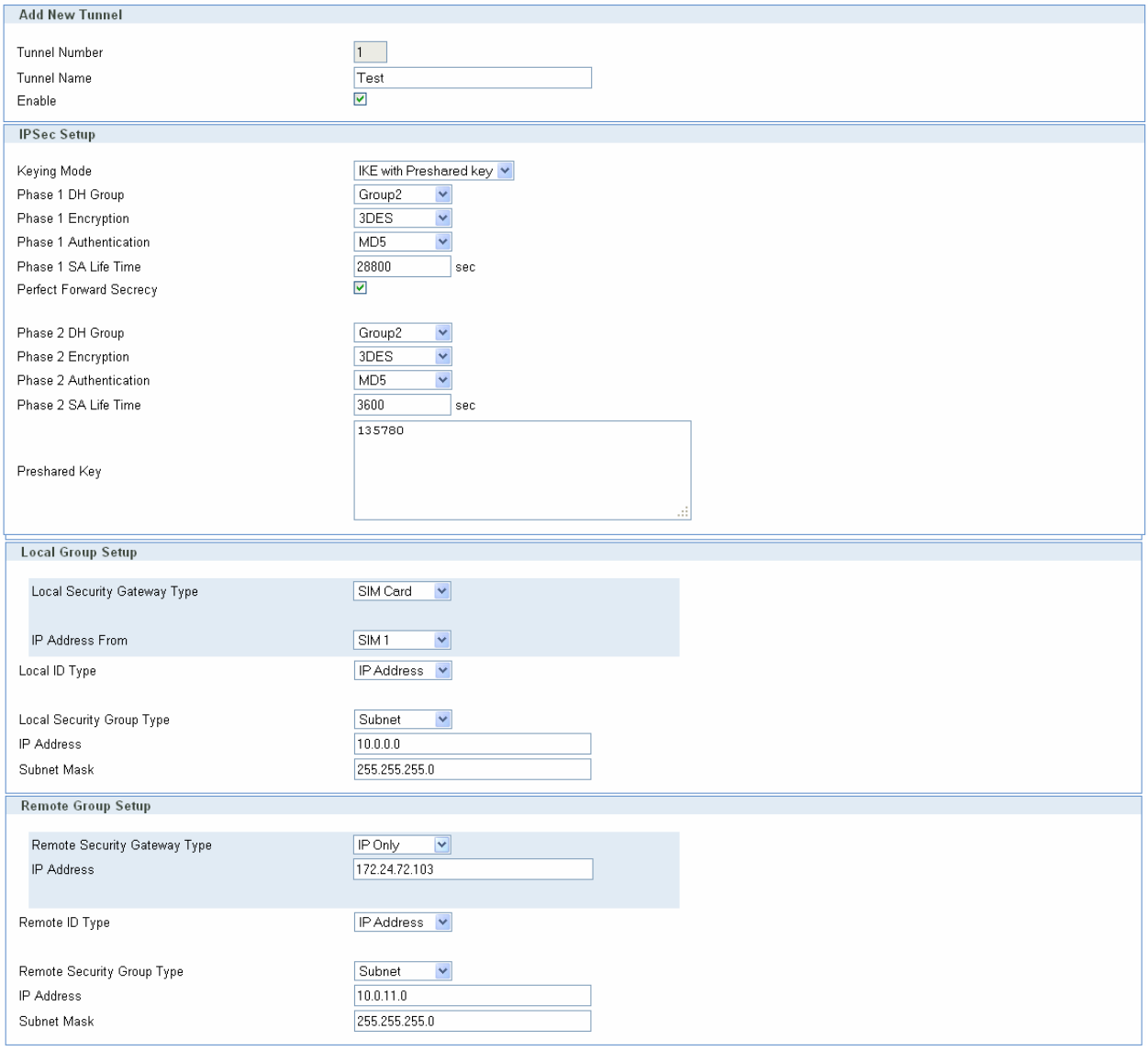
Figure 17 - IPSec Summary screen for first firmware version

VPN Settings / IPSec Summary	
Label	**Description**
Tunnels Used	This is the number of IPSec tunnels being defined.
Maximum number of tunnels	This is the maximum number of tunnels which can be defined.
No	This filed indicates the number of the IPSec tunnel.
Name	Field shows the Tunnel Name that you gave to the IPSec tunnel.
Enabled	This field shows if tunnel is enabled or disabled. After clicking on ***Start*** button, only enabled tunnels will be started.
Status	Field indicates status of the IPSec tunnel. Click on ***Refresh*** button to see current status of defined IPSec tunnels.
Enc/Auth/Grp	This field shows both Phase 1 and Phase 2 details, Encryption method (DES/3DES/AES), Authentication method (MD5/SHA1), and DH Group number (1/2/5) that you have defined in the IPSec Setup section.
Advanced	Field shows the chosen options from IPSec Advanced section by displaying the first letters of enabled options.
Local Group	Field shows the IP address and subnet mask of the Local Group.
Remote Group	Field displays the IP address and subnet mask of the Remote Group.
Remote Gateway	Field shows the IP address of the Remote Device.
Delete	Click on this link to delete the tunnel and all settings for that particular tunnel.
Edit	This link opens screen where you can change the tunnel's settings.
Add New Tunnel	Click on this button to add a new Device-to-Device IPSec tunnel. After you have added the tunnel, you will see it listed in the Summary table.
Start	This button starts the IPSec negotiations between all defined and enabled tunnels. If the IPSec is already started, Start button is replaced with Restart button.

Stop	This button will stop all IPSec started negotiations.
Refresh	Click on this button to refresh the Status field in the Summary table.

Table 12 - IPSec Summary for first firmware version

To create a tunnel click Add New Tunnel button. Depending on your selection, the Local Group Setup and Remote Group Setup settings will differ. Proceed to the appropriate instructions for your selection.



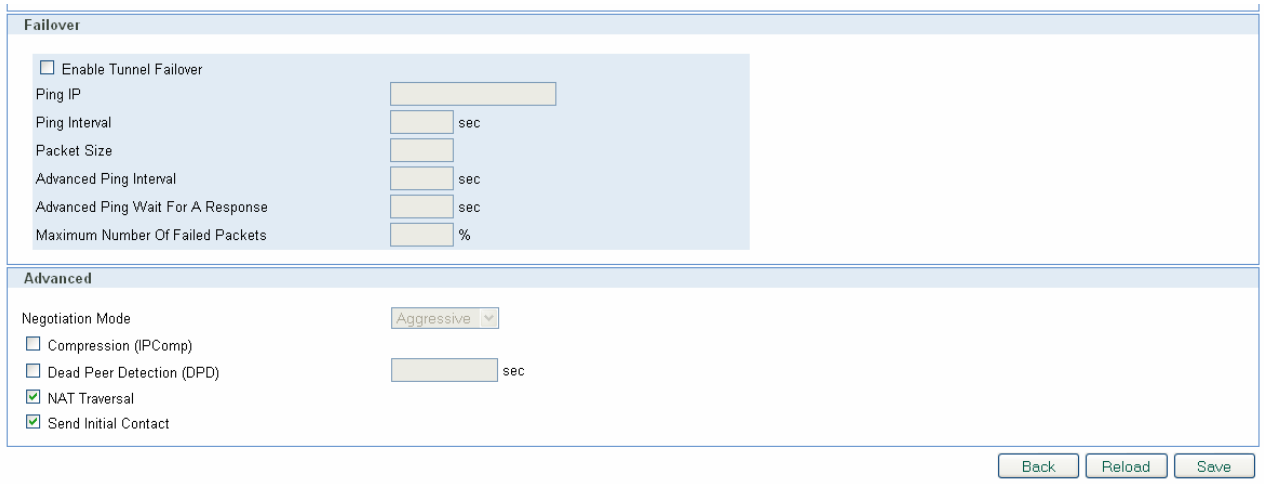


Figure 18 - IPSec Settings for first firmware version

VPN Settings / IPSec Settings	
Label	**Description**
Tunnel Number	This number will be generated automatically and it represents the tunnel number.
Tunnel Name	Enter a name for the IPSec tunnel. This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
Enable	Check this box to enable the IPSec tunnel.
IPSec Setup	In order to establish an encrypted tunnel, the two ends of an IPSec tunnel must agree on the methods of encryption, decryption and authentication. This is done by sharing a key to the encryption code. For key management, the Router uses only IKE with Preshared Key mode.
Keying Mode	**IKE with Preshared Key** IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Preshared Key to authenticate the remote IKE peer. Both ends of IPSec tunnel must use the same mode of key management. **Certificates** This option will be available in future release
Phase 1 DH Group	Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol used during Phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits and Group 5 is 1536 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.
Phase 1 Encryption	Select a method of encryption: DES (56-bit), 3DES (168-bit) or AES-128 (128-bit). The method determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Make sure both ends of the IPSec tunnel use the same encryption method.
Phase 1 Authentication	Select a method of authentication: MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the IPSec tunnel use the same authentication method.
Phase 1 SA Life Time	Configure the length of time IPSec tunnel is active in Phase 1. The default value is 28800 seconds. Both ends of the IPSec tunnel must use the same Phase 1 SA Life

	Time setting.
Perfect Forward Secrecy	If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys. Both ends of the IPSec tunnel must enable this option in order to use the function.
Phase 2 DH Group	If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits, and Group 5 is 1536 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You do not have to use the same DH Group that you used for Phase 1, but both ends of the IPSec tunnel must use the same Phase 2 DH Group.
Phase 2 Encryption	Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. Select a method of encryption: NULL, DES (56-bit), 3DES (168-bit) or AES-128 (128-bit). It determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Both ends of the IPSec tunnel must use the same Phase 2 Encryption setting. *NOTE: If you select a NULL method of encryption, the next Phase 2 Authentication method cannot be NULL and vice versa.*
Phase 2 Authentication	Select a method of authentication: NULL, MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Both ends of the IPSec tunnel must use the same Phase 2 Authentication setting. *NOTE: If you select a NULL method of authentication, the previous Phase 2 Encryption method cannot be NULL.*
Phase 2 SA Life Time	Configure the length of time an IPSec tunnel is active in Phase 2. The default is 3600 seconds. Both ends of the IPSec tunnel must use the same Phase 2 SA Life Time setting.
Preshared Key	This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., Ay_%4222 or 345fa929b8c3e. This field allows a maximum of 1023 characters and/or hexadecimal values. Both ends of the IPSec tunnel must use the same Preshared Key. *NOTE: It is strongly recommended that you periodically change the Preshared Key to maximize security of the IPSec tunnels.*
Local Security gateway type	When **SIM Card** is selected the WAN (or Internet) IP address of the Router automatically appears. If the Router is not yet connected to the GSM/UMTS network this field is without IP address.
IP Address From	Select SIM card over which the tunnel is established
Local ID Type	How the of the participant should be identified for authentication; Can be an IP address, fully-qualified domain name (FQDN) or User FQDN name preceded by @ .
Local Security Group Type	Select the local LAN user(s) behind the Router that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. *NOTE: The Local Security Group Type you select should match the Remote Security Group Type selected on the IPSec device at the other end of the tunnel.*
IP Address	Only the computer with a specific IP address will be able to access the tunnel.
Subnet Mask	Enter the subnet mask.

Remote Security Gateway Type	Select the remote LAN user(s) behind the Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. *NOTE: The Remote Security Group Type you select should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.*
IP Address	Only the computer with a specific IP address will be able to access the tunnel.
Remote ID type	How the of the participant should be identified for authentication; Can be an IP address, fully-qualified domain name (FQDN) or User FQDN name preceded by @
Remote Security Group Type	Select the remote LAN user(s) behind the Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. *NOTE: The Remote Security Group Type you select should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.*
IP Address	Only the computer with a specific IP address will be able to access the tunnel.
Subnet Mask	Enter the subnet mask.
Enable tunnel failover	Enable tunnel failover. If there is more than one tunnel defined, this option will failover to other tunnel in case that selected one fails to established connection.
Ping IP	IP address on other side of tunnel which will be pinged in order to determine current state.
Ping interval	Specify time period in seconds between two ping
Packet size	Specify packet size for ping message
Advanced Ping Interval	Time interval between advanced ping packets.
Advanced Ping Wait For A Response	Advanced ping proofing timeout.
Maximum numbers of failed packets	Set percentage of failed packets until failover action is performed.
Negotiation Mode	This option enables selection from three IPSec modes: **Main, Aggressive** and **Base**. If option NAT Traversal is selected Aggressive mode is predefined.
Compress (IP Payload Compression Protocol (IP Comp))	IP Payload Compression is a protocol that reduces the size of IP datagram. Select this option if you want the Router to propose compression when it initiates a connection.
Dead Peer Detection (DPD)	When DPD is enabled, the Router will send periodic HELLO/ACK messages to check the status of the IPSec tunnel (this feature can be used only when both peers or IPSec devices of the IPSec tunnel use the DPD mechanism). Once a dead peer has been detected, the Router will disconnect the tunnel so the connection can be re-established. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent). The default interval is 20 seconds.
NAT Traversal	Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947. *NOTE: If you select this mode the Aggressive mode will be automatically selected because it is obligatory option for NAT-T to work properly.* *NOTE: Keep-alive for NAT-T function is enabled by default and cannot be disabled. The default interval for keep-alive packets is 20 seconds.*
Send initial contact	The initial-contact status message may be used when one side wishes to inform the other that this is the first SA being established with the remote system. The

	receiver of this Notification Message might then elect to delete any existing SA's it has for the sending system under the assumption that the sending system has rebooted and no longer has access to the original SA's and their associated keying material.
Back	Click ***Back*** to return on IPSec Summary screen.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR-I Router. After that router automatically goes back and begin negotiations of the tunnels by clicking on the Start button.

Table 13 - IPSec Parameters for first firmware version

OpenVPN

OpenVPN site to site allows connecting two remote networks via point-to-point encrypted tunnel. OpenVPN implementation offers a cost-effective simply configurable alternative to other VPN technologies. OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features. The server and client have almost the same configuration. The difference in the client configuration is the remote endpoint IP or hostname field. Also the client can set up the keepalive settings. For successful tunnel creation a static key must be generated on one side and the same key must be uploaded on the opposite side.

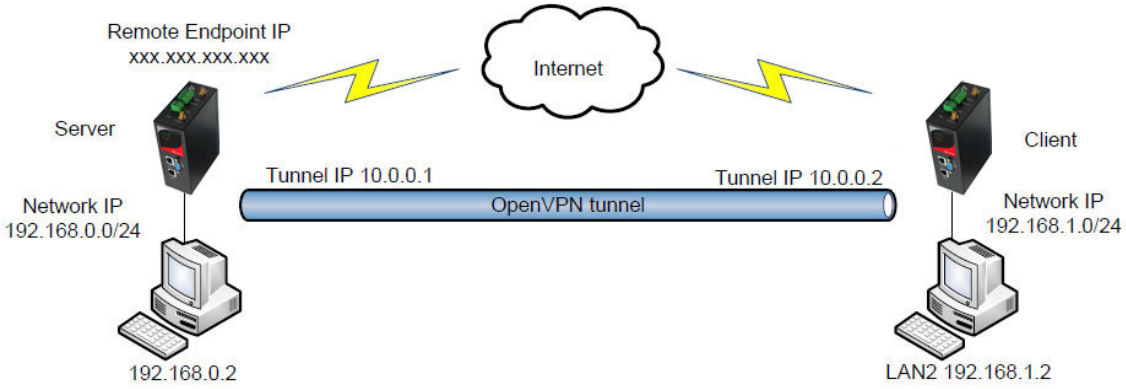


Figure 19 – OpenVPN example

OpenVPN	
Label	**Description**
IP Filtering	
Tunnel Number	Automatically assigned number of the tunnel.
Tunnel Name	This field specifies tunnel name.
Enable	Check this setting in order to enable OpenVPN tunnel.
Allow access from the following devices	
Interface Type	There are two modes of OpenVPN tunnel, routed and bridged mode. For routed mode select option TUN, and for bridged TAP
Authenticate Mode	Choose one of the following options: - none (Select this option if you do not want to use any kind of authentication) - pre-shared secret (Select this option if you want to use PSK as a authentication method) - username/password (Select this option if you want to use username/password along with CA Certificate as a authentication method) - X.509 cert. (client) (Select this option if you want to use X.509 certificates as a authentication method in client mode) - X.509 cert. (server) (Select this option if you want to use X.509 certificates as a authentication method in server mode)

NOTE: Depending on the options selected in the previous steps, some of the following options will be available for configuration.	
Protocol	Selection between TCP in server or client mode and UDP protocol in connect or wait mode.
TCP/UDP port	Depending on the selected protocol, port number should be specified.
LZO Compression	Check the box to enable fast adaptive LZO compression.
NAT Rules	Enables NAT through the tunnel.
Keep Alive	Check the box if you want to use keepalive.
Ping Interval	This field specifies the target IP address for periodical traffic generated using ping in order to maintain the connection active.
Ping Timeout	This field specifies ping interval for keepalive option.
Pre-shared Secret	Generate or Paste the Pre-shared Secret. You have an additional option to Export the PSK.
Max Fragment Size	If you select UDP protocol whether in connect or wait mode you must specify Max Fragment Size (default is 1300 bytes).
Renegotiate interval	Specify renegotiate interval if username/password is selected as authentication method.
CA Certificate	Specify the CA Certificate.
Username	Specify the username.
Password	Specify the password.
Local Certificate	Specify the local certificate.
Local Private Key	Specify the local private key.
DH Group	Choose the DH Group from the following: 786 bits, 1024 bits, 1536 bits, 2048 bits.
Remote Host or IP Address	Specify server IP address or hostname.
Redirect Gateway	This option allows usage of OpenVPN tunnel as a default route.
Tunnel Interface Configuration	Pull tunnel interface configuration from server side.
Manual configuration	
Local Interface IP Address	Specify the IP address of the local VPN tunnel endpoint.
Remote Interface IP Address	Specify the IP address of the remote VPN tunnel endpoint.
Pull from server	
Network Topology	Specify topology of OpenVPN interfaces – NET30, P2P or SUBNET

Table 14 – OpenVPN parameters

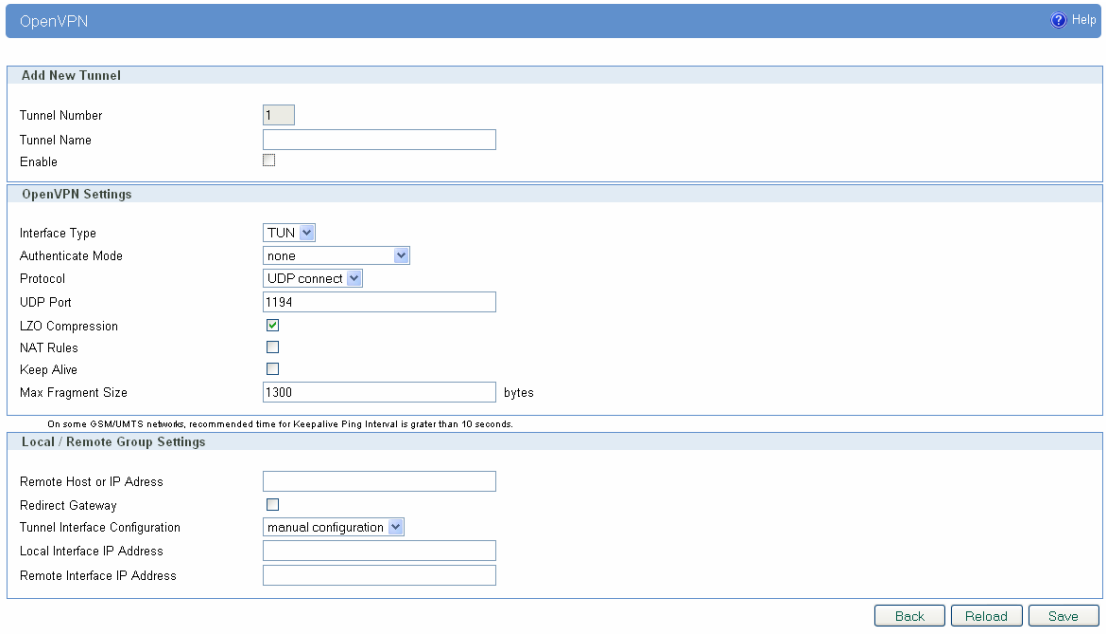


Figure 20 – OpenVPN configuration page

Figure 21 – OpenVPN network topology

Settings - IP Filtering

IP filtering is simply a mechanism that decides which types of IP datagram's will be processed normally and which will be discarded. By discarded we mean that the datagram is deleted and completely ignored, as if it had never been received. You can apply many different sorts of criteria to determine which datagram's you wish to filter; some examples of these are:

- Protocol type: TCP, UDP, ICMP, etc.
- Socket number (for TCP/UPD)
- Datagram type: SYN/ACK, data, ICMP Echo Request, etc.
- Datagram source address: where it came from
- Datagram destination address: where it is going to.

It is important to understand at this point that IP filtering is a network layer facility. This means it doesn't understand anything about the application using the network connections, only about the connections themselves. The IP filtering rule set is made up of many combinations of the criteria listed previously.

Use firewall option to set IP addresses from which is possible remote access on the GWR-I Router. Demilitarized Zone (DMZ) allows one IP Address to be exposed to the Internet. Because some applications require multiple TCP/IP ports to be open, DMZ provides this function by forwarding all the ports to one computer at the same time. In the other words, this setting allows one local user to be exposed to the Internet to use a special-purpose services such as Internet gaming, Video-conferencing and etc. It is recommended that you set your computer with a static IP if you want to use this function.

IP Filtering	
Label	**Description**
IP Filtering	
Disable all	This field specifies if Firewall and DMZ settings are disabled at the GWR-I Router.
Enable Firewall	This field specifies if Firewall is enabled at the GWR-I Router.
Enable DMZ	This field specifies if DMZ settings is enabled at the GWR-I Router.
Allow access from the following devices	
Enable	This check box allows/forbidden host to access to the GWR-I Router.
IP address	This field specifies IP address of the host allow access to the GWR-I Router.
Service	This field specifies service of the host allow access to the GWR-I Router.
Protocol	This field specifies protocol of the host allow access to the GWR-I Router.
Port	This field specifies port of the host allow access to the GWR-I Router.
Add	Click ***Add*** to insert (add) new item in table to the GWR-I Router.
Remove	Click ***Remove*** to delete selected item from table.
Allow access from the following networks	
Enable	This check box allows/forbidden host to access to the GWR-I Router.
IP address	This field specifies IP address of the host allow access to the GWR-I Router.
Subnet mask	This field specifies network mask of the network to allow access to the GWR-I Router.

Service	This field specifies service of the host allow access to the GWR-I Router.
Protocol	This field specifies protocol of the host allow access to the GWR-I Router.
Port	This field specifies port of the host allow access to the GWR-I Router.
Add	Click ***Add*** to insert (add) new item in table to the GWR-I Router.
Remove	Click ***Remove*** to delete selected item from table.
Demilitarized Zone Host Settings	
DMZ Private IP Address	This check box allows/forbidden host to access to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR-I Router.

Table 15 - IP filtering parameters

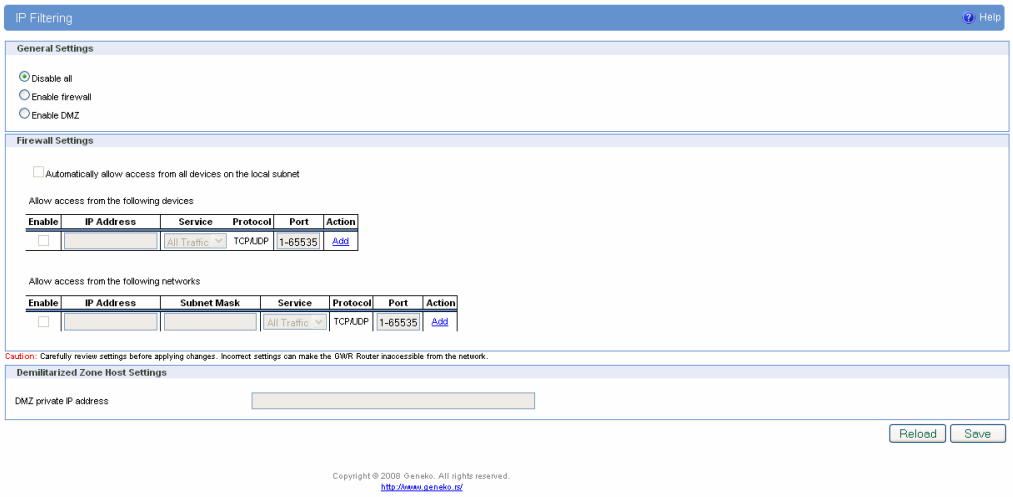


Figure 22 - IP Filtering configuration page

IP Filtering configuration example

This example configuration demonstrates how to secure a network with a combination of routers and a GWR-I Router.

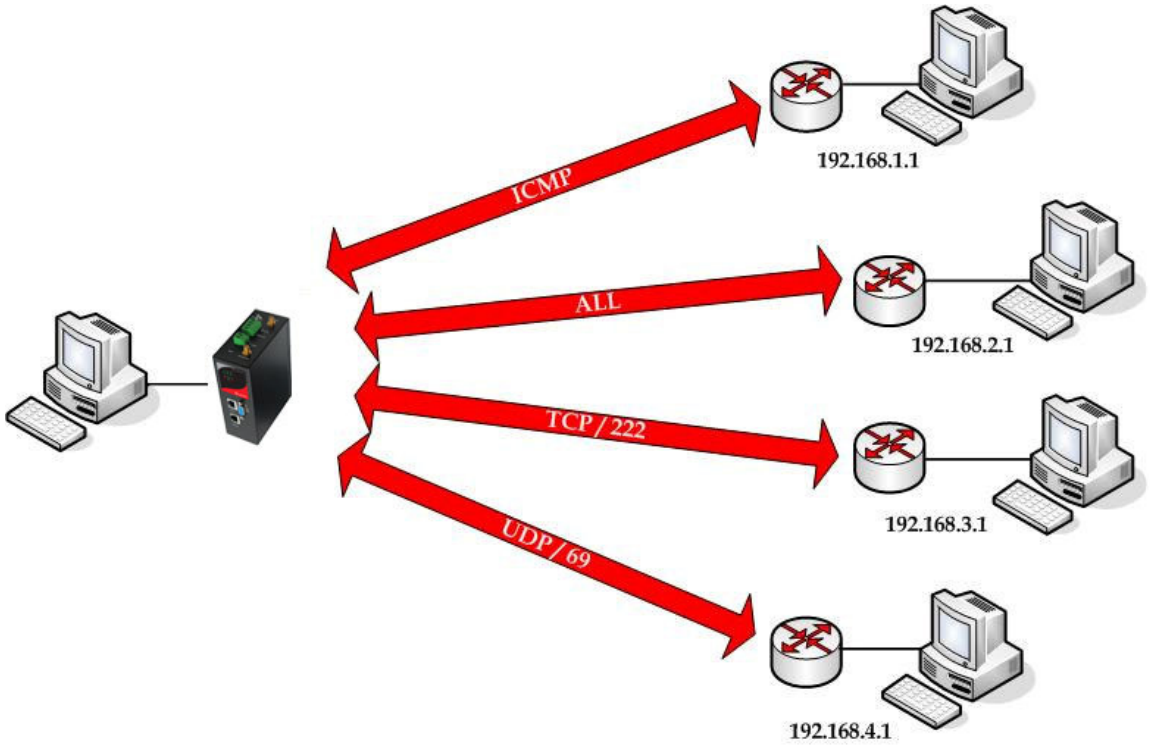


Figure 23 - IP Filtering configuration example

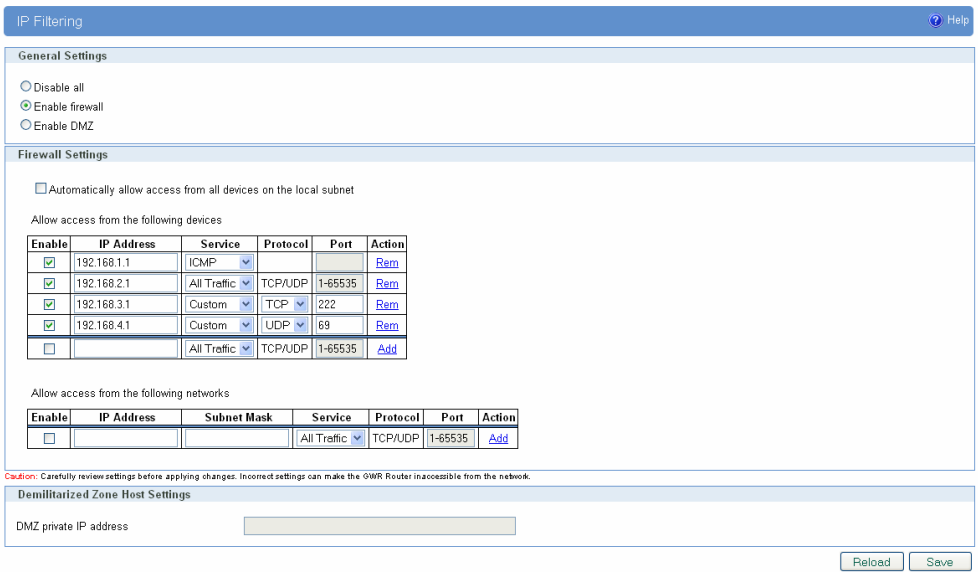


Figure 24 - IP Filtering settings

Settings – DynDNS

Dynamic DNS is a domain name service allowing to link dynamic IP addresses to static hostname. To start using this feature firstly you should register to DDNS service provider. Section of the web interface where you can setup DynDNS parameters is shown in Figure 25.

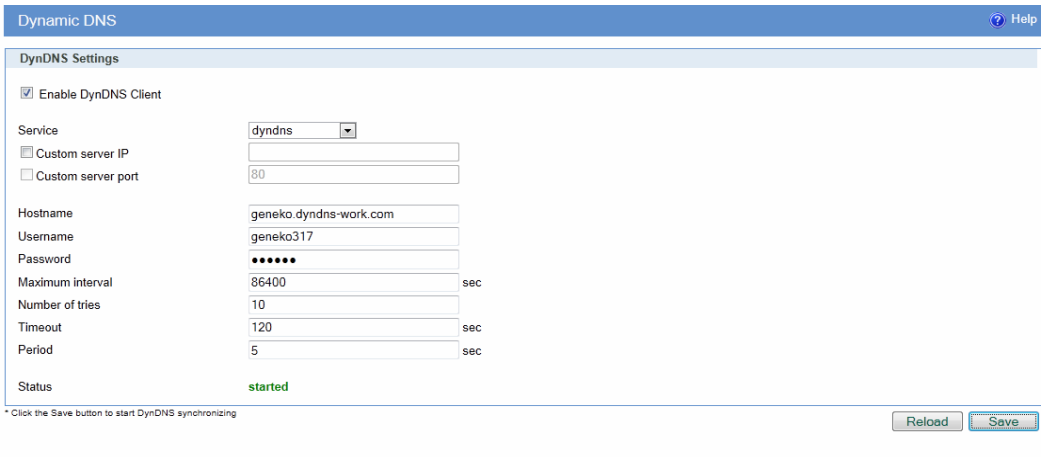


Figure 25 - DynDNS settings

DynDNS	
Label	**Description**
Enable DynDNS Cilent	Enable DynDNS Client.
Service	The type of service that you are using, try one of: dhs, pgpow, dyndns, dyndns-static, dyndns-custom, ods, easydns, dyns, justlinux and zoneedit.
Custom Server IP	The server IP to connect to.
Custom Server port	The server port to connect to.
Hostname	String to send as host parameter.
Username	User ID.
Password	User password.
Maximum interval	Max interval in seconds between updates, default and minimum is 86400.
Number of tries	Number of tries (default: 1) if network problem.
Timeout	The amount of time to wait on I/O (network problem).
Period	Time between update retry attempts, default value is 1800.

Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR-I Router.

Table 16 – DynDNS parameters

Settings - Serial Port 1

Using the router's serial port it is possible to perform serial-to-ethernet conversion (Serial port over TCP/UDP) and ModbusRTU-to-TCP conversion (Modbus gateway). Initial Serial Port Settings page is shown in figure bellow. By default above described features are disabled. Selecting one of two possible applications of Serial port opens up additional options available for configuration.

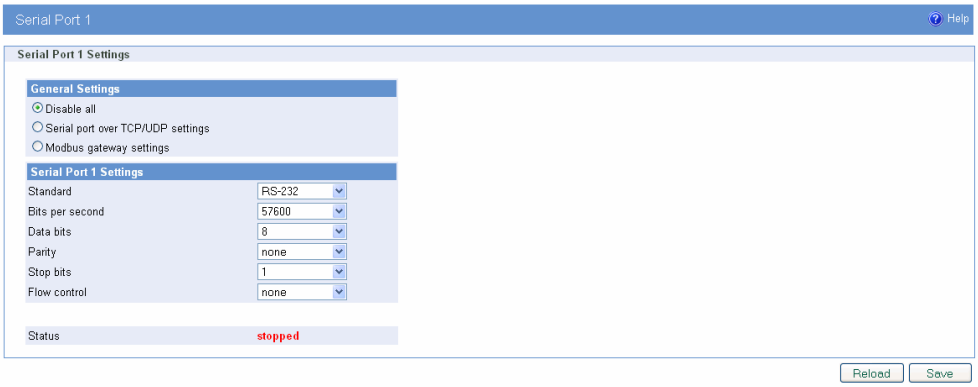


Figure 26 - Serial Port Settings initial menu

Following image shows PINOUT of the Serial Port 1.

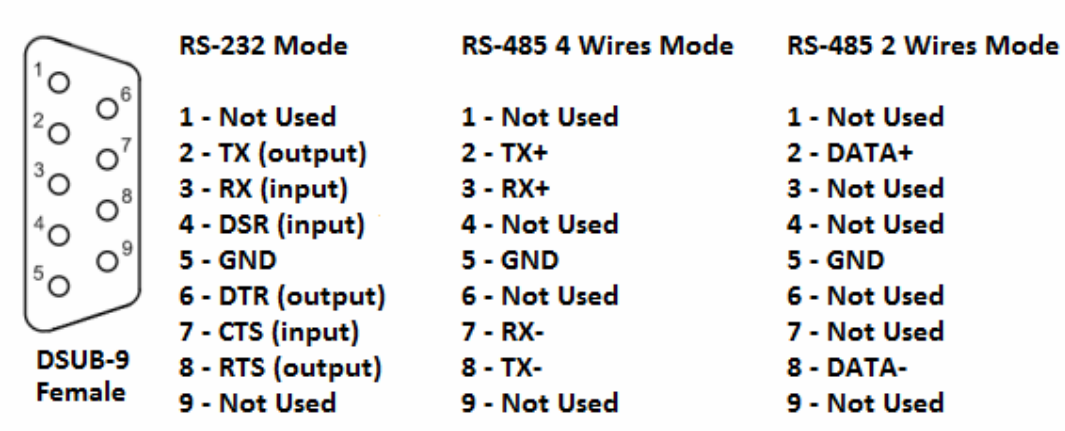


Figure 27 - Serial Port Settings 1 PINOUT

Serial port over TCP/UDP settings

The GWR-I Router provides a way for a user to connect from a network connection to a serial port. It provides all the serial port setup, a configuration file to configure the ports, a control login for modifying port parameters, monitoring ports, and controlling ports. The GWR-I Router supports RFC 2217 (remote control of serial port parameters).

Serial Port over TCP/UDP Settings	
Label	**Description**
Standard	Indicates the standard for serial connection (RS232, RS485 2W, RS485 4W).
Bits per second	The unit and attached serial device, such as a modem, must agree on a speed or baud rate to use for the serial connection. Valid baud rates are 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
Data bits	Indicates the number of bits in a transmitted data package.
Parity	Checks for the parity bit. None is the default.
Stop bits	The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission. The default is 1.
Flow control	Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data. None is the default.
Protocol	Choose which protocol to use [TCP/UDP].
Mode	Select server mode in order to listen for incoming connection, or client mode to establish one.
Bind to TCP/UDP port	Number of the TCP/UDP port to accept connections for this device. (Only on server side)
Server IP address	Specify server IP address. (Only on client side)
Connect to TCP/UDP port	Number of the TCP/UDP port to accept connections from this device. (Only on client side)
Type of socket	Either *raw or telnet*. Raw enables the port and transfers all data like between the port and the log. Telnet enables the port and runs the telnet protocol on the port to set up telnet parameters.
Enable local echo	Enable the local echo feature.
Check TCP connection	Enable connection checking.
Kepalive idle time	Set keepalive idle time in seconds.
Kepalive interval	Set time period between checking.
Log level	Set importance level of log messages.

Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR-I Router and activate/deactivate serial to Ethernet converter.

Table 17 – Ser2IP parameters

Click *Serial Port* Tab to open the Serial Port Configuration screen. Use this screen to configure the GWR-I Router serial port parameters (*Figure 28*).

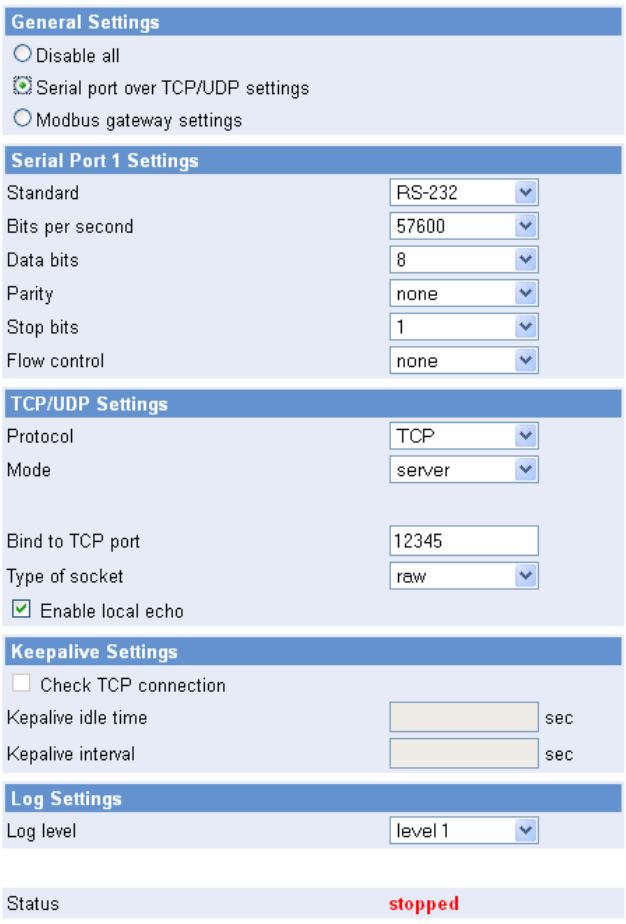


Figure 28 - Serial Port configuration page

Serial Port Settings	
Label	**Description**
Enable configuration console	Enable router configuration console. Default serial port parameters are: Serial port parameters: baud rate - 57600, data bits - 8, parity - none, stop bits - 1, flow control - none.
Enable serial-Ethernet converter	Enable serial to Ethernet converter. This provides a way for a user to connect from a network connection to a serial port.
Standard	Indicates the standard for serial connection (RS232, RS485 2W, RS485 4W).
Bits per second	The unit and attached serial device, such as a modem, must agree on a speed or baud rate to use for the serial connection. Valid baud rates are 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
Data bits	Indicates the number of bits in a transmitted data package.
Parity	Checks for the parity bit. None is the default.
Stop bits	The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission. The default is 1.
Flow control	Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data. None is the default.
Bind to port	Number of the TCP/IP port to accept connections from for this device.
Type of socket	Either *raw, brawl* or *telnet. raw* enables the port and transfers all data as-is between the port and the long. *rawlp* enables the port and transfers all input data to device, device is open without any termios setting. It allows using printers connected to them. *telnet* enables the port and runs the telnet protocol on the port to set up telnet parameters. This is most useful for using telnet.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR-I Router and activate/deactivate serial to Ethernet converter.

Table 18 - Serial port parameters

Modbus Gateway settings

The serial server will perform conversion from Modbus/TCP to Modbus/RTU, allowing polling by a Modbus/TCP master. The Modbus IPSerial Gateway carries out translation between Modbus/TCP and Modbus/RTU. This means that Modbus serial slaves can be directly attached to the unit's serial ports without any external protocol converters.
Click Serial Port Tab to open the Modbus Gateway configuration screen. Choose Modbus Gateway options to configure Modbus. At the Figure 28 you can see screenshot of Modbus Gateway configuration menu.

Modbus Gateway Parameters	
Label	**Description**
Standard	Indicates the standard for serial connection (RS232, RS485 2W, RS485 4W).
Bits per second	The unit and attached serial device, such as a modem, must agree on a speed or baud rate to use for the serial connection. Valid baud rates are 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
Data bits	Indicates the number of bits in a transmitted data package. Valid data bits are: 8 and 7.
Parity	Checks for the parity bit. Valid parity are: none, even and odd. None is the default.
Stop bits	The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission. Valid stop bits are: 1 and 2. The default is 1.
Flow control	Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data. None is the default.
TCP accept port	This field determines the TCP port number that the serial server will listen for connections on. The value entered should be a valid TCP port number. The default Modbus/TCP port number is 502.
Connection timeout	When this field is set to a value greater than 0, the serial server will close connections that have had no network receive activity for longer than the specified period.
Transmission mode	Select RTU, based on the Modbus slave equipment attached to the port.
Response timeout	This is the timeout (in milliseconds) to wait for a response from a serial slave device before retrying the request or returning an error to the Modbus master.
Maximum number of retries	Should no valid response be received from a Modbus slave, the value in this field determines the number of times the serial server will retransmit request before giving up.
Log level	Set importance level of log messages.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR-I Router and activate/deactivate serial to Ethernet converter.

Table 19 – Modbus gateway parameters

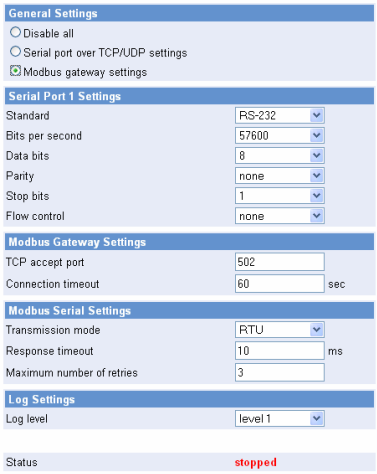


Figure 29 – Modbus gateway configuration page

Settings - Serial Port 2

Most of the settings related to Serial Port 2 are equivalent to the Serial Port 1 settings. The only difference is in type of connector and serial port standard. Namely, serial port 2 supports RS232 and RS485 4W standards.

Please find the PINOUT of the Serial Port 2 presented on the following image.

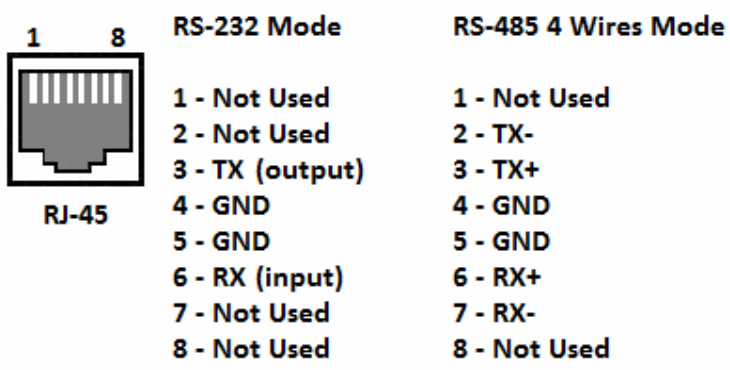


Figure 30 - Serial Port Settings 1 PINOUT

Settings - SMS

SMS remote control feature allows users to execute a short list of predefined commands by sending SMS messages to the router. GWR-I router series implement following predefined commands:

1. In order to establish PPP connection, user should send SMS containing following string
   :PPP-CONNECT
   After the command is executed, router sends a confirmation SMS with "OK" if the command is executed without errors or "ERROR" if something went wrong during the execution of the command.

2. In order to disconnect the router from PPP, user should send SMS containing following string
   :PPP-DISCONNECT
   After the command is executed, router sends a confirmation SMS with "OK" if the command is executed without errors or "ERROR" if something went wrong during the execution of the command.

3. In order to reestablish (reconnect the router) the PPP connection, user should send SMS containing following string
   :PPP-RECONNECT
   After the command is executed, router sends a confirmation SMS with "OK" if the command is executed without errors or "ERROR" if something went wrong during the execution of the command.

4. In order to obtain the current router status, user should send SMS containing following string
   :PPP-STATUS
   After the command is executed, router sends one of the following status reports to the user:
   - CONNECTING
   - CONNECTED, WAN_IP: {WAN IP address or the router**}**
   - DISCONNECTING
   - DISCONNECTED

Remote control configuration page is presented on the following figure. In order to use this feature, user must enable the SMS remote control and specify the list of SIM card numbers that will be used for SMS remote control. The SIM card number should be entered in the following format: {Country Code}{Mobile Operator Prefix}{Phone Number} (for example **+38164111222**).

As presented on the Figure 31. configuration should be performed for separately for both SIM cards. After the configuration is entered, user must click on SAVE button in order to save the configuration.

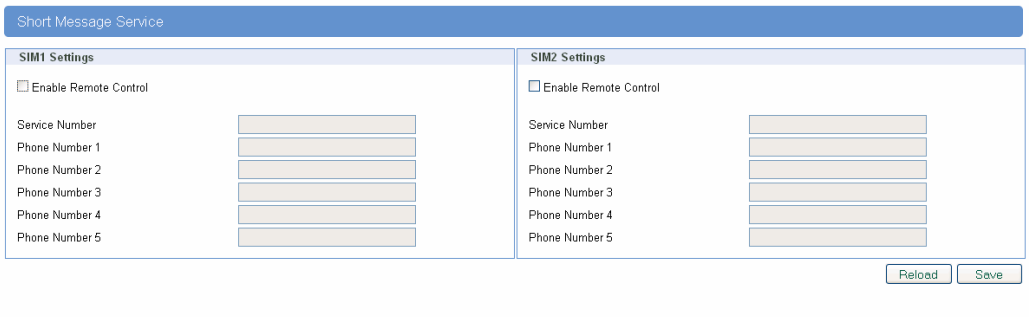


Figure 31– SMS remote control configuration

Settings - GPIO

GWR-I router series implements one digital input and one digital output. Numerous telemetry and data acquisition applications imply using digital input and output for providing simple control over certain system functionalities. GPIO (General Purpose Input Output) settings page is displayed on the image bellow:

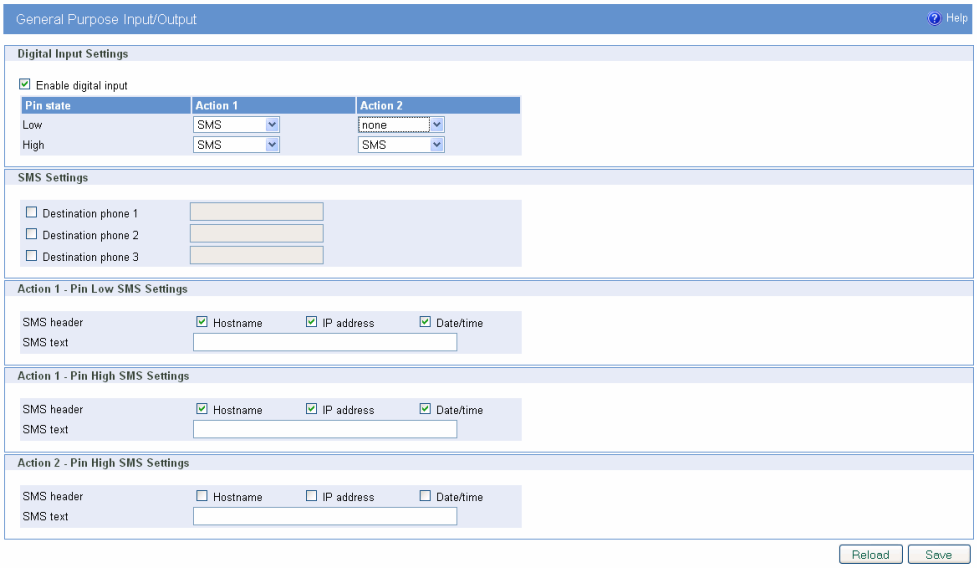


Figure 32– GPIO settings page

GPIO settings	
Label	**Description**
Enable digital input	Enable or disable digital input on the GWR-I
Low (Action1/Action2)	Setup required action when router detects low level on digital input. It is possible to define two separate actions for this event. User can choose between sending an SMS alert on input change to LOW or setting up the digital output HIGH or LOW.
High (Action1/Action2)	Setup required action when router detects high level on digital input. It is possible to define two separate actions for this event. User can choose between sending an SMS alert on input change to HIGH or setting up the digital output HIGH or LOW.
Destination phone 1-3	Specify up to three mobile phone numbers that will receive SMS alert.
SMS header	Define the content of SMS header. Following three options are available: Host name (name of the router defined in Device Identity Settings), IP address (router IP address) of the router and Date/Time.
SMS text	Custom text of SMS message.
Save	Click ***Save*** button to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 20 – GPIO parameters

Maintenance

The GWR-I Router provides administration utilities via web interface. Administrator can setup basic router's parameters, perform network diagnostic, update software or restore factory default settings.

Maintenance - Device Identity Settings

Within ***Device Identity Settings Tab*** there is an option to define name, location of device and description of device function. These data are kept in device permanent memory. ***Device Identity Settings*** window is shown on *Figure 33*.

Device Identity Settings	
Label	**Description**
Name	This field specifies name of the GWR-I Router.
Description	This field specifies description of the GWR-I Router. Only for information purpose.
Location	This field specifies location of the GWR-I Router. Only for information purpose.
Save	Click ***Save*** button to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 21 - Device Identity parameters

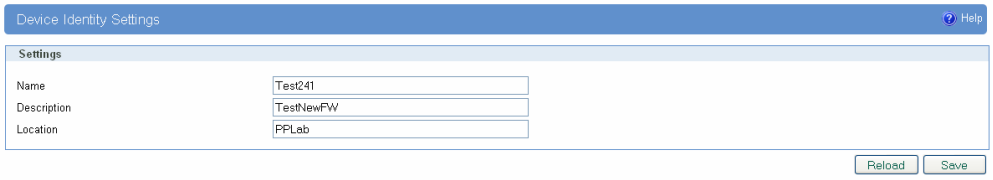


Figure 33 - Device Identity Settings configuration page

Maintenance - Administrator Password

By ***Administrator Password*** Tab it is possible to activate and deactivates device access system through ***Username*** and ***Password*** mechanism. Within this menu change of authorization data Username/Password is also done. ***Administer Password*** Tab window is shown on *Figure 34*.

NOTE: The password cannot be recovered if it is lost or forgotten. If the password is lost or forgotten, you have to reset the Router to its factory default settings; this will remove all of your configuration changes.

Figure 34 - Administrator Password configuration page

Administrator Password	
Label	**Description**
Enable Password Authentication	By this check box you can activate or deactivate function for authentication when you access to web/console application.
Username	This field specifies Username for user (administrator) login purpose.
Old Password	Enter the old password. The default is ***admin*** when you first power up the GWR-I Router.
New Password	Enter a new password for GWR-I Router. Your password must have 20 or fewer characters and cannot contain any space.
Confirm Password	Re-enter the new password to confirm it.
Save	Click ***Save*** button to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 22 - Administrator password

Maintenance - Date/Time Settings

To set the local time, select ***Date/Time Settings*** using the Network Time Protocol (NTP) automatically or Set the local time manually. Date and time setting on the GWR-I Router are done through window Date/Time Settings.

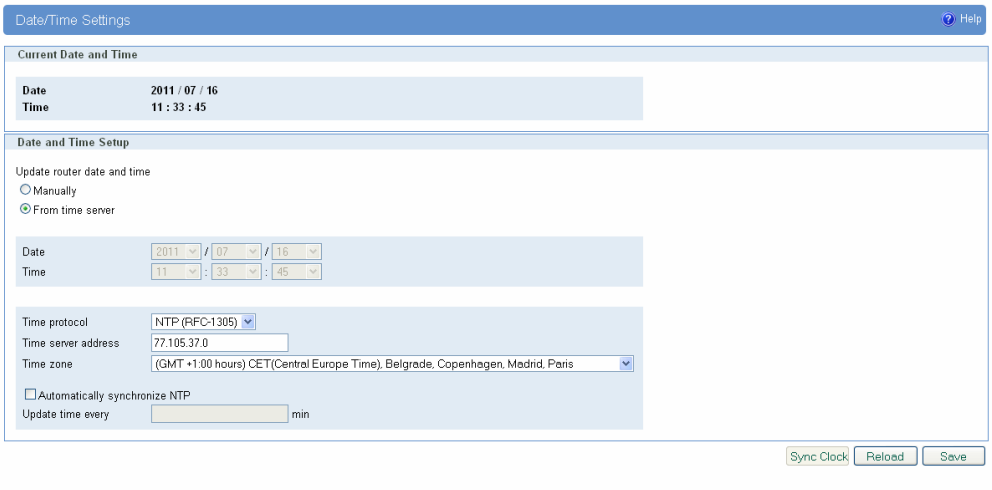


Figure 35 - Date/Time Settings configuration page

Date/Time Settings	
Label	**Description**
Manually	Sets date and time manually as you specify it.
From time server	Sets the local time using the Network Time Protocol (NTP) automatically.
Time/Date	This field species Date and Time information. You can change date and time by changing parameters.
Sync Clock With Client	Date and time setting on the basis of PC calendar.
Time Protocol	Choose the time protocol.
Time Server Address	Time server IP address.
Time Zone	Select your time zone.
Automatically synchronize NTP	Setup automatic synchronization with time server.
Update time every	Time interval for automatic synchronization.
Save	Click ***Save*** button to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 23 - Date/time parameters

Maintenance - Diagnostics

The GWR-I Router provide built-it tool, which is used for troubleshooting network problems. The ping test bounces a packet of machine on the Internet back to the sender. This test shows if the GWR-I Router is able to connect the remote host. If users on the LAN are having problems accessing service on the Internet, try to ping the DNS server or other machine on network.

Click ***Diagnostic*** tab to provide basic diagnostic tool for testing network connectivity. Insert valid IP address in ***Hostname*** box and click ***Ping***. Every time you click ***Ping*** router sends four ICMP packets to destination address.

Before using this tool make sure you know the device or host's IP address.

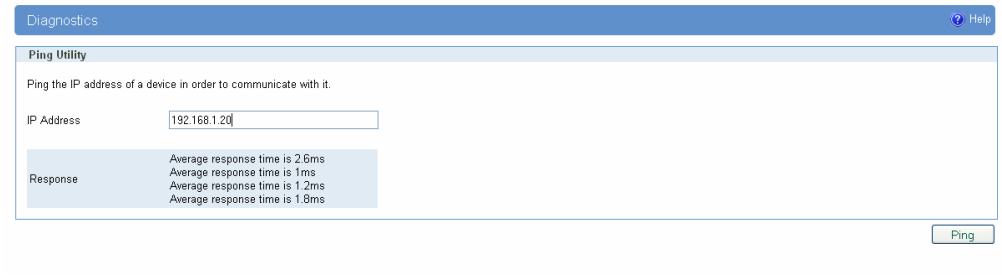


Figure 36 - Diagnostic page

Maintenance - Update Firmware

You can use this feature to upgrade the GWR-I Router firmware to the latest version. If you need to download the latest version of the GWR-I Router firmware, please visit Geneko support site. Follow the on-screen instructions to access the download page for the GWR-I Router.

If you have already downloaded the firmware onto your computer, click ***Browse*** button, on ***Update firmware*** Tab, to look for the firmware file. After selection of new firmware version through ***Browse*** button, mechanism the process of data transfer from firmware to device itself should be started. This is done by ***Upload*** button. The process of firmware transfer to the GWR-I device takes a few minutes and when it is finished the user is informed about transfer process success.

NOTE: The Router will take a few minutes to upgrade its firmware. During this process, do not power off the Router or press the Reset button.

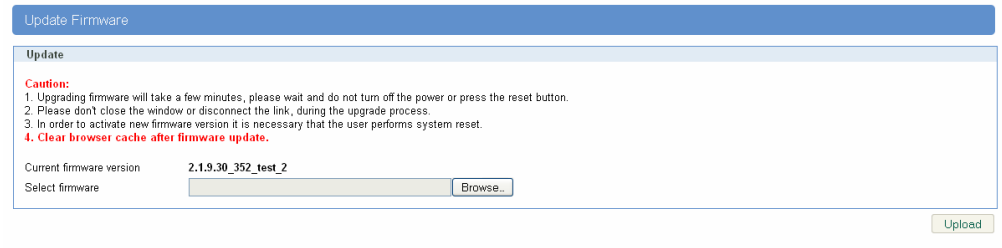


Figure 37 - Update Firmware page

In order to activate new firmware version it is necessary that the user performs system reset. In the process of firmware version change all configuration parameters are lost and after that the system continues to operate with default values.

Maintenance - Settings Backup

This feature allows you to make a backup file of complete configuration or some part of the configuration on the GWR-I Router. In order to backup the configuration, you should select the part of configuration you would like to backup. The list of available options is presented on the image 35. To use the backup file, you need to import the configuration file that you previously exported.

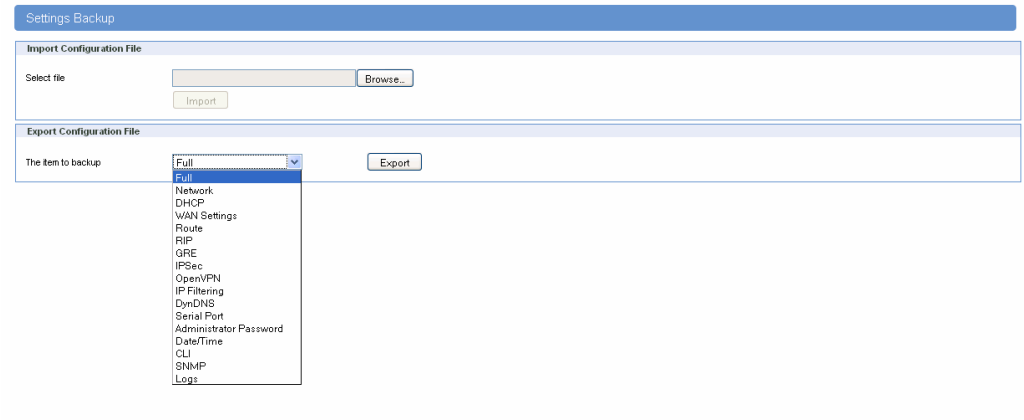


Figure 38 – Export/Import the configuration on the router

Import Configuration File

To import a configuration file, first specify where your backup configuration file is located. Click **Browse**, and then select the appropriate configuration file.

After you select the file, click Import. This process may take up to a minute. Restart the Router in order to changes will take effect.

Export Configuration File

To export the Router's current configuration file select the part of the configuration you would like to backup and click ***Export***.

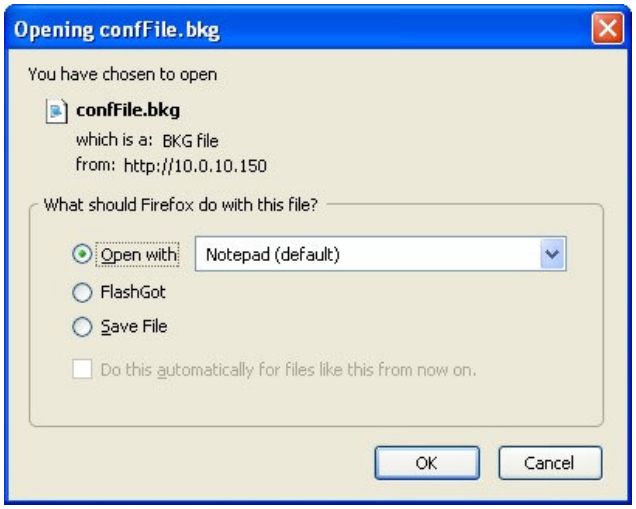


Figure 39 - File download

Select the location where you want to store your backup configuration file. By default, this file will be called confFile.bkg, but you may rename it if you wish. This process may take up to a minute.

Maintenance - Default Settings

Use this feature to clear all of your configuration information and restore the GWR-I Router to its factory default settings. Only use this feature if you wish to discard all the settings and preferences that you have configured.

Click ***Default Setting*** to have the GWR-I Router with default parameters. ***Keep network settings*** check-box allows user to keep all network settings after factory default reset. System will be reset after pressing ***Restore*** button.

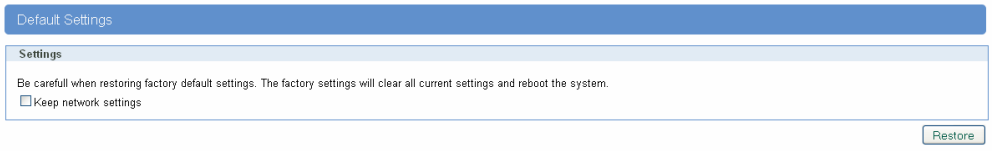


Figure 40 - Default Settings page

Maintenance - System Reboot

If you need to restart the Router, Geneko recommends that you use the Reboot tool on this screen. Click ***Reboot*** to have the GWR-I Router reboot. This does not affect the router's configuration.

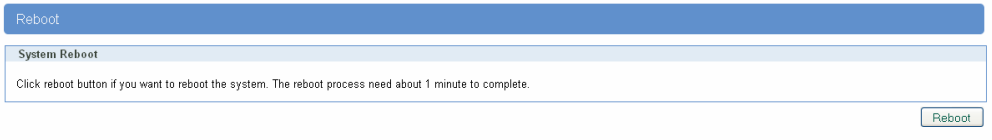


Figure 41 - System Reboot page

Management – Command Line Interface

CLI (command line interface) is a user text-only interface to a computer's operating system or an application in which the user responds to a visual prompt by typing in a command on a specified line and then receives a response back from the system.
In other words, it is a method of instructing a computer to perform a given task by "entering" a command. The system waits for the user to conclude the submitting of the text command by pressing the "Enter" or "Return" key. A command-line interpreter then receives, parses, and executes the requested user command.

On router's Web interface, in Management menu, click on Command Line Interface tab to open the Command Line Interface settings screen. Use this screen to configure CLI parameters (Figure 42).

Command Line Interface	
Label	**Description**
CLI Settings	
Enable	Enable or disable CLI
CLI on	Telnet, SSH, Serial
View Mode Username	Login name for View mode
View Mode Password	Password for View mode
Confirm Password	Confirm password for View mode
View Mode Timeout	Inactivity timeout for View mode in seconds. After timeout, user will be put in Main mode.
Edit Mode Timeout	Inactivity timeout for Edit mode in seconds. Note that Username and Password for Edit mode are the same as Web interface login parameters. After timeout, user will be put in Main mode.
Console Type	Windows, other.
Save	Click ***Save*** to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 24 – Command Line Interface parameters

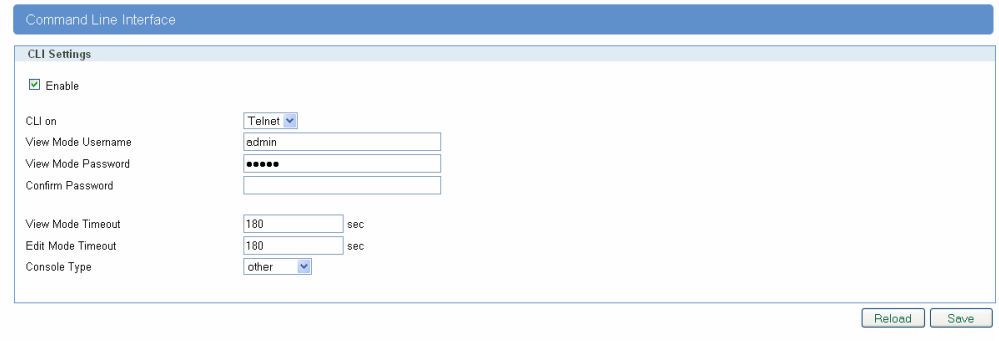


Figure 42 – Command Line Interface

Detailed instructions related to CLI are located in other document (Command_Line_Interface.pdf file on CD that goes with the router). You will find detailed specifications of all commands you can use to configure the router and monitor routers performance.

Management – Remote Management

Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of GWR-I routers. More information about this utility can be found in other document (Remote_Management.pdf). In order to use this utility user has to enable Remote Management on the router (Figure 43).

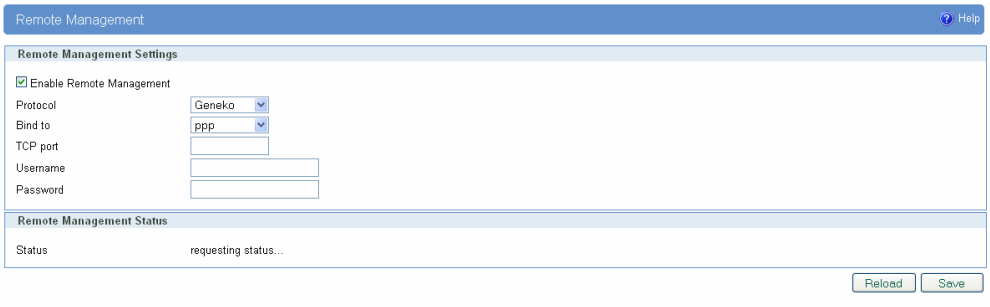


Figure 43 – Remote Management

Command Line Interface	
Label	**Description**
Enable Remote Management	Enable or disable Remote Management.
Protocol	Choose between Geneko and Sarian protocol.
Bind to	Specify the interface.
TCP port	Specify the TCP port.
Username	Specify the username.
Password	Specify the password.
Save	Click ***Save*** to save your changes back to the GWR-I Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 25 – Remote Management parameters

Management – Connection Manager

Enabling Connection Manager will allow Connection Wizard (located on setup CD that goes with the router) to guide you step-by-step through the process of device detection on the network and setup of the PC-to-device communication. Thanks to this utility user can simply connect the router to the local network without previous setup of the router. Connection Wizard will detect the device and allow you to configure some basic functions of the router. Connection Manager is enabled by default on the router and if you do not want to use it you can simply disable it (Figure 44).

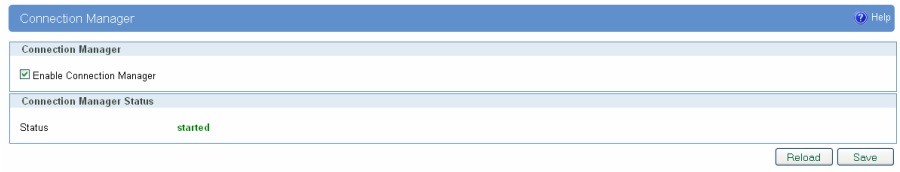


Figure 44 – Connection Manager

Getting started with the Connection Wizard:

Connection Wizard is installed through few very simple steps and it is available immediately upon the installation. After starting the wizard you can choose between two available options for configuration:

- **GWR-I Router's Ethernet port** - With this option you can define LAN interface IP address and subnet mask.
- **GWR-I router's Ethernet port and GPRS/EDGE/HSPA network connection** - Selecting this option you can configure parameters for LAN and WAN interface

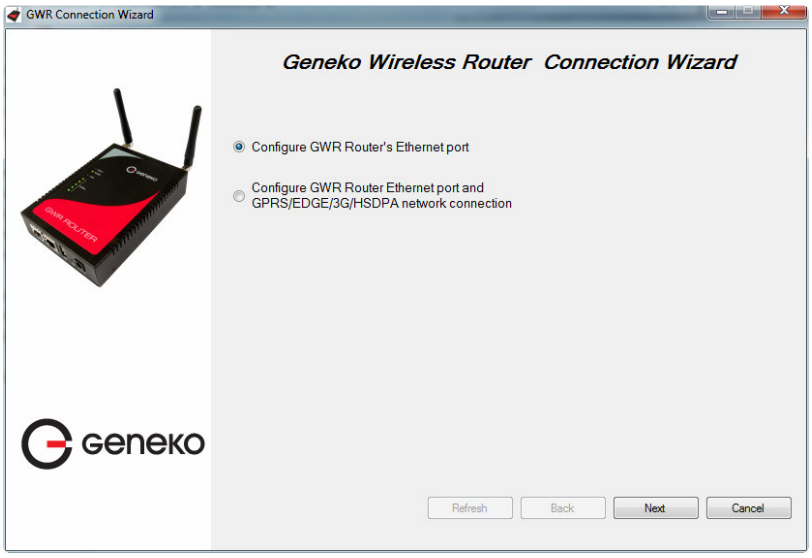


Figure 45 – Connection Wizard – Initial Step

Select one of the options and click *Next*. On the next screen after Connection Wizard inspects the network (whole broadcast domain) you'll see a list of routers present in the network, with following information:

- Serial number
- Model
- Ethernet IP
- Firmware version
- Pingable (if Ethernet IP address of the router is in the same IP subnet as PC interface then this field will be marked, i.e. you can access router over web interface)

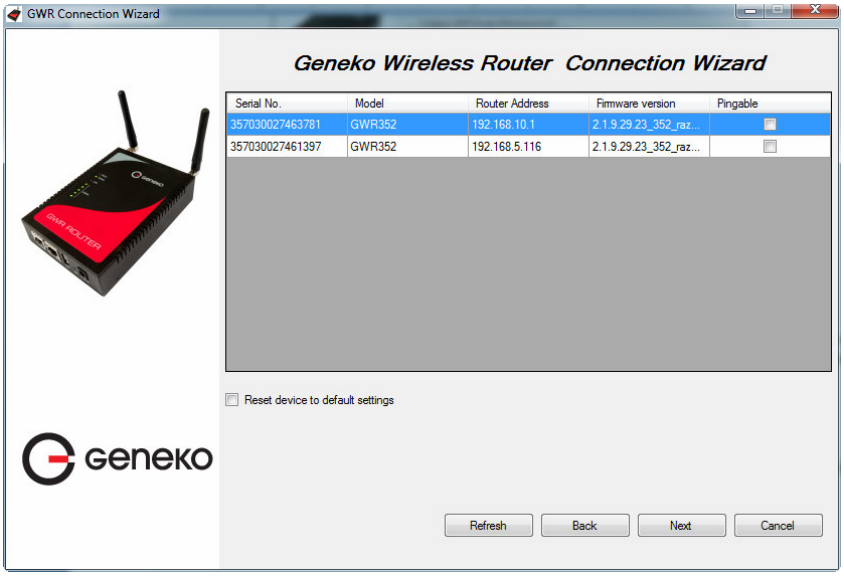


Figure 46 – Connection Wizard – Router Detection

When you select one of the routers from the list and click *Next* you will get to the following screen:

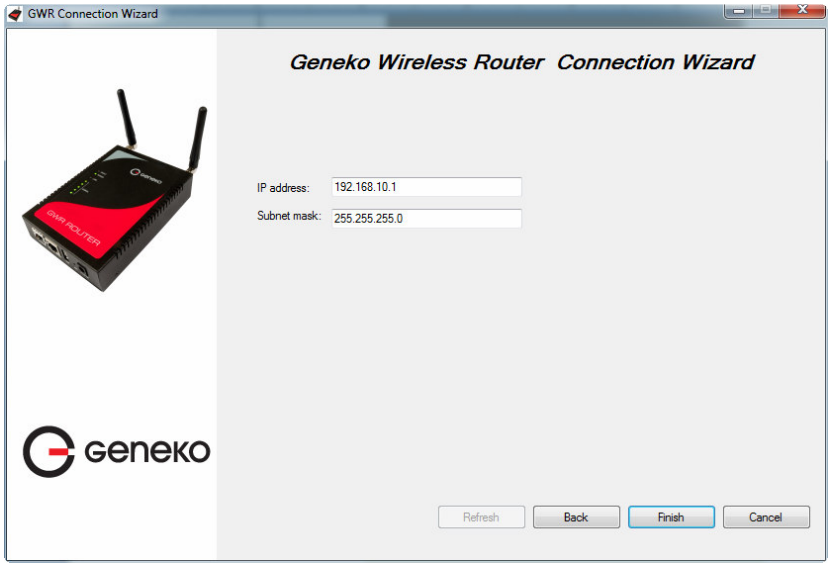


Figure 47 – Connection Wizard – LAN Settings

If you selected to configure LAN and WAN interface click, upon entering LAN information click *Next* and you will be able to setup WAN interface.

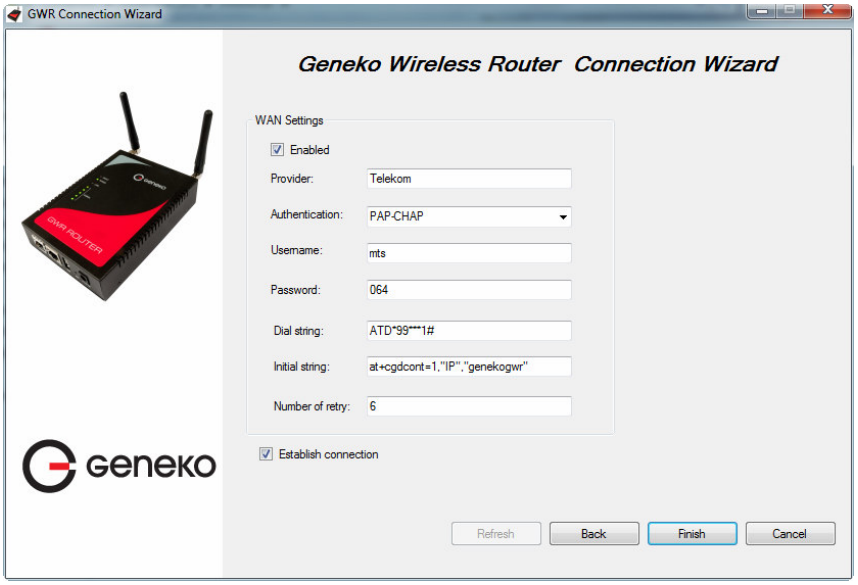


Figure 48 – Connection Wizard – WAN Settings

After entering the configuration parameters if you mark option *Establish connection* router will start with connection establishment immediately when you press *Finish* button. If not you have to start connection establishment manually on the router's web interface.

Management - Simple Management Protocol (SNMP)

SNMP, or Simple Network Management Protocol, is a network protocol that provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network. The Router supports SNMP v1/v2c and all relevant Management Information Base II (MIBII) groups. The appliance replies to SNMP Get commands for MIBII via any interface and supports a custom MIB for generating trap messages.

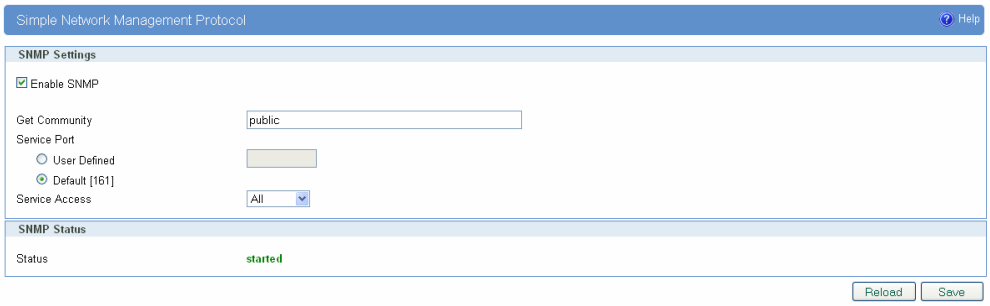


Figure 49 - SNMP configuration page

SNMP Settings	
Label	**Description**
Enable SNMP	SNMP is enabled by default. To disable the SNMP agent, click this option to unmark.
Get Community	Create the name for a group or community of administrators who can view SNMP data. The default is **public**. It supports up to 64 alphanumeric characters.
Service Port	Sets the port on which SNMP data has been sent. The default is 161. You can specify port by marking on user defined and specify port you want SNMP data to be sent.
Service Access	Sets the interface enabled for SNMP traps. The default is Both.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR-I Router and enable/disable SNMP.

Table 26 - SNMP parameters

Management - Logs

Syslog is a standard for forwarding log messages in an IP network. The term "syslog" is often used for both the actual syslog protocol, as well as the application or library sending syslog messages.

Syslog is a client/server protocol: the syslog sender sends a small (less than 1KB) textual message to the syslog receiver. Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

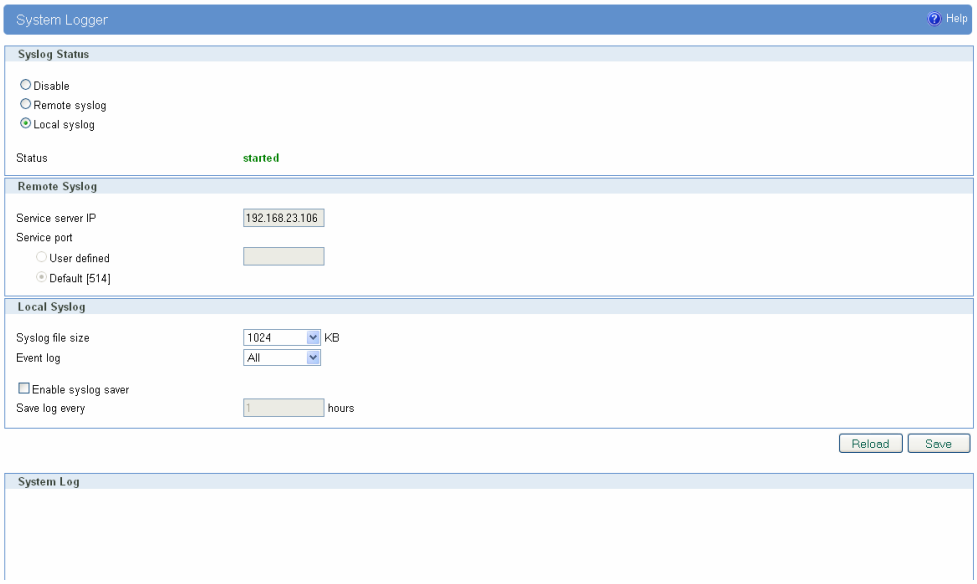


Figure 50 - Syslog configuration page

The GWR-I Router supports this protocol and can send its activity logs to an external server.

Syslog Settings	
Label	**Description**
Disable	Mark this option in order to disable Syslog feature.
Remote syslog	Mark this option in order to enable logging on remote machine.
Local syslog	Start logging facility locally.
Remote Syslog	**Description**
Service Serve IP	The GWR-I Router can send a detailed log to an external Syslog server. The Router's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP service, and number of bytes transferred. Enter the Syslog server name or IP address.
Service Port	Sets the port on which Syslog data has been sent. The default is 514. You can specify port by marking on user defined and specify port you want Syslog data to be sent.
User defined	Set manually port number.
Default	Use standard port number for this service. [514]
Local syslog	**Description**
Syslog file size	Set log size on one of the six predefined values. [10/20/50/100/200/500]kb
Event log	Choose which events to be stored. You can store System, Ipsec events or both of them.
Enable syslog saver	Save logs periodically on filesystem.
Save log every	Set time duration between two saves.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR-I Router and enable/disable Syslog.

Table 27 - Syslog parameters

Logout

The ***Logout*** tab is located on the down left-hand corner of the screen. Click this tab to exit the web-based utility. (If you ex it the web-based utility, you will need to re-enter your User Name and Password to log in and then manage the Router.)

Configuration Examples

GWR-I Router as Internet Router

The GWR-I Routers can be used as *Internet router* for a single user or for a group of users (entire LAN). NAT function is enabled by default on the GWR-I Router. The GWR-I Router uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside world. All outgoing traffic uses the GWR-I Router mobile IP address.

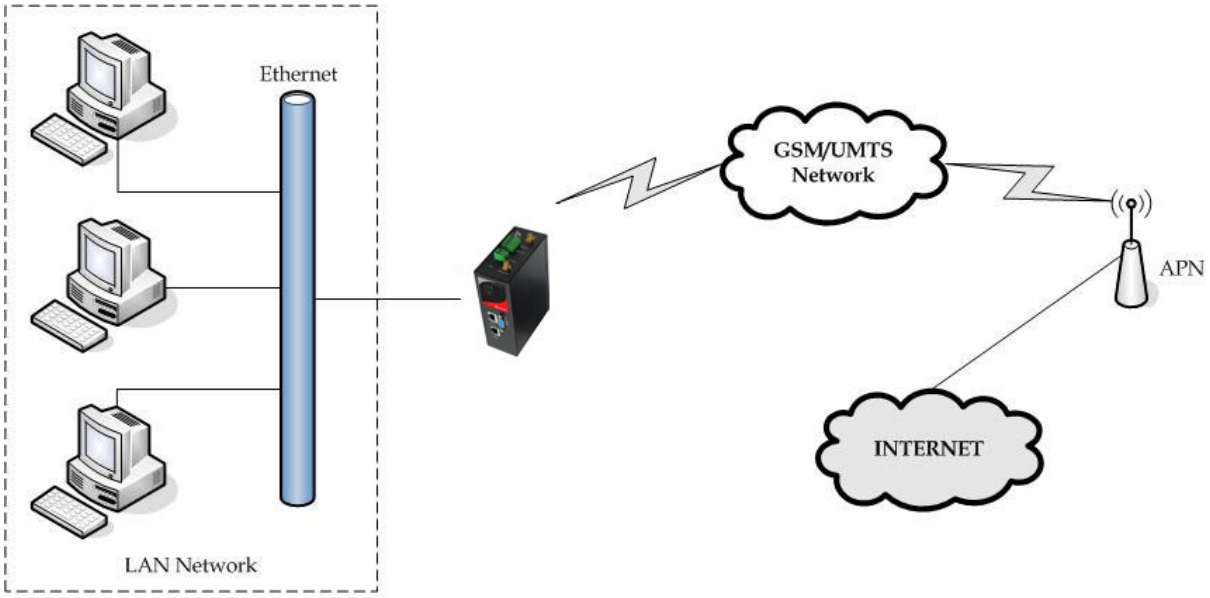


Figure 51 - GWR-I Router as Internet router

- Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP address: 10.1.1.1
  - Netmask: 255.255.255.0
- Press ***Save*** to accept the changes.
- Use SIM card with a dynamic/static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider's network default gateway).
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be provided by your mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Check ***Routing*** Tab to see if there is default route (should be there by default).
- Router will automatically adds default route via *ppp0* interface.
- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.
- Configure the GWR-I Router LAN address (10.1.1.1) as a default gateway address on your PCs. Configure valid DNS address on your PCs.

GRE Tunnel configuration between two GWR-I Routers

GRE tunnel is a type of a VPN tunnel, but it isn't a secure tunneling method. Simple network with two GWR-I Routers is illustrated on the diagram below (*Figure 52*). Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

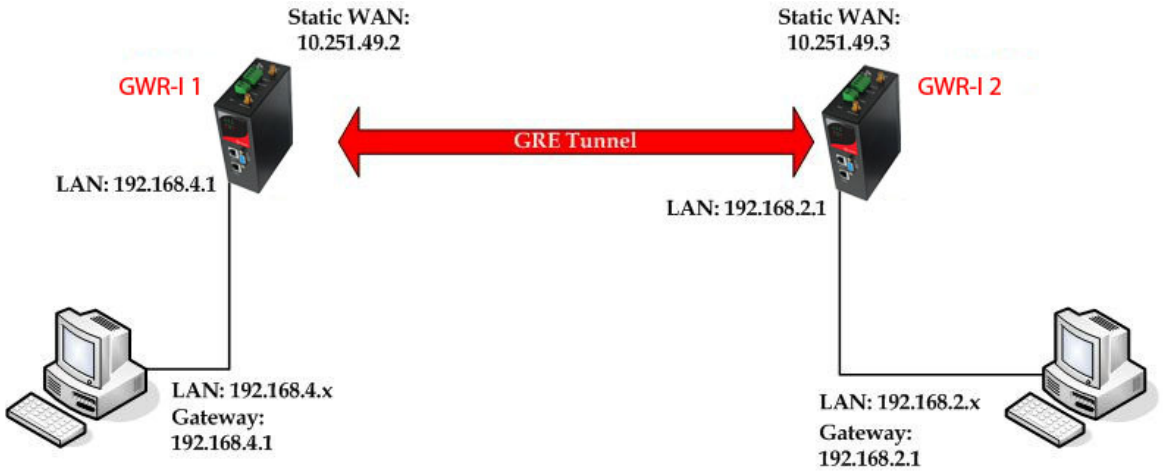


Figure 52 - GRE tunnel between two GWR-I Routers

The GWR-I Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address;
- Source tunnel address should have static WAN IP address;
- Destination tunnel address should have static WAN IP address;

GSM/UMTS APN Type: For GSM/UMTS networks GWR-I Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

The GWR-I Router 1 configuration:

- Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 192.168.4.1
  - Subnet Mask: 255.255.255.0
  - Press ***Save*** to accept the changes.

Figure 53 - Network configuration page for GWR-I Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS

provider's network default gateway).

- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > GRE*** to configure GRE tunnel parameters:
  - Enable: yes
  - Local Tunnel Address: 10.10.10.1
  - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252)
  - Tunnel Source: 10.251.49.2 (select HOST from drop down menu if you want to use host name as peer identifier)
  - Tunnel Destination: 10.251.49.3 (select HOST from drop down menu if you want to use host name as peer identifier)
  - KeepAlive enable: no
  - Period:(none)
  - Retries:(none)
  - Press ADD to put GRE tunnel rule into GRE table.
  - Press ***Save*** to accept the changes.

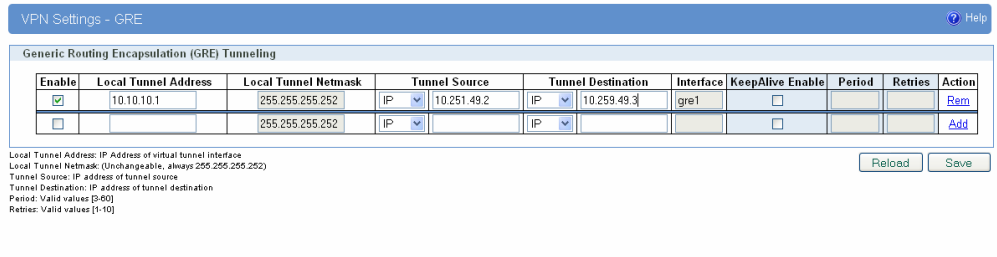


Figure 54 - GRE configuration page for GWR-I Router 1

- Click **Routing** on **Settings** Tab to configure GRE Route. Parameters for this example are:
  - Destination Network: 192.168.2.0
  - Netmask: 255.255.255.0
  - Interface: gre_x

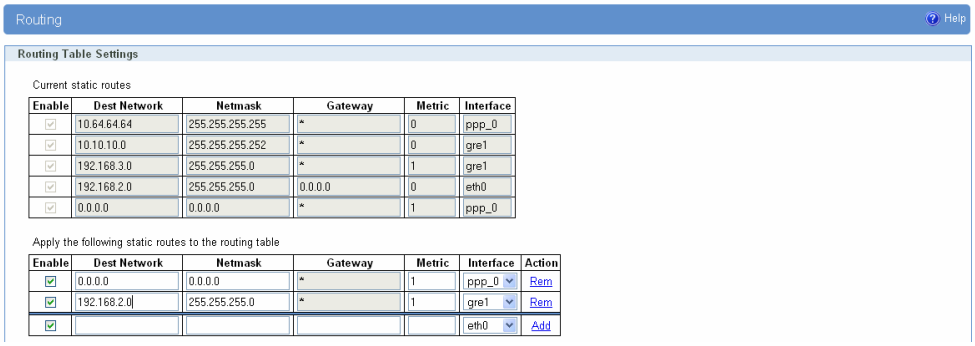


Figure 55 - Routing configuration page for GWR-I Router 1

- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.
- On the device connected on GWR-I router 1 setup default gateway 192.168.4.1

The GWR-I Router 2 configuration:

- Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 192.168.2.1

- Subnet Mask: 255.255.255.0
- Press ***Save*** to accept the changes.

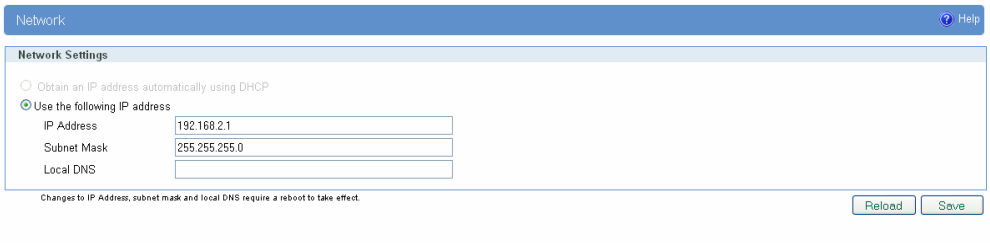


Figure 56 - Network configuration page for GWR-I Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider's network default gateway).
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > GRE*** to configure GRE tunnel parameters:
  - Enable: yes
  - Local Tunnel Address: 10.10.10.2
  - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252)
  - Tunnel Source: 10.251.49.3 (select HOST from drop down menu if you want to use host name as peer identifier)
  - Tunnel Destination: 10.251.49.2 (select HOST from drop down menu if you want to use host name as peer identifier)
  - KeepAlive enable: no
  - Period:(none)
  - Retries:(none)
  - Press ADD to put GRE tunnel rule into GRE table.
  - Press ***Save*** to accept the changes.

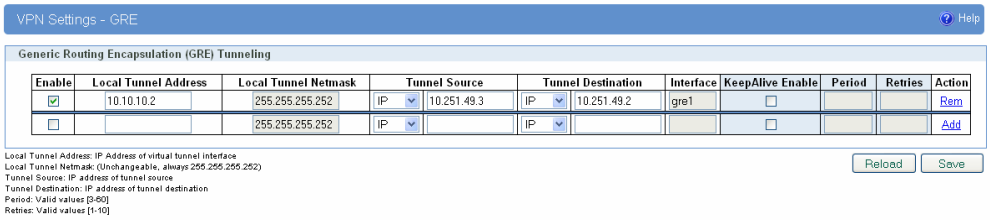


Figure 57 - GRE configuration page for GWR-I Router 2

- Configure GRE Route. Click ***Routing*** on ***Settings*** Tab. Parameters for this example are:
  - Destination Network: 192.168.4.0
  - Netmask: 255.255.255.0

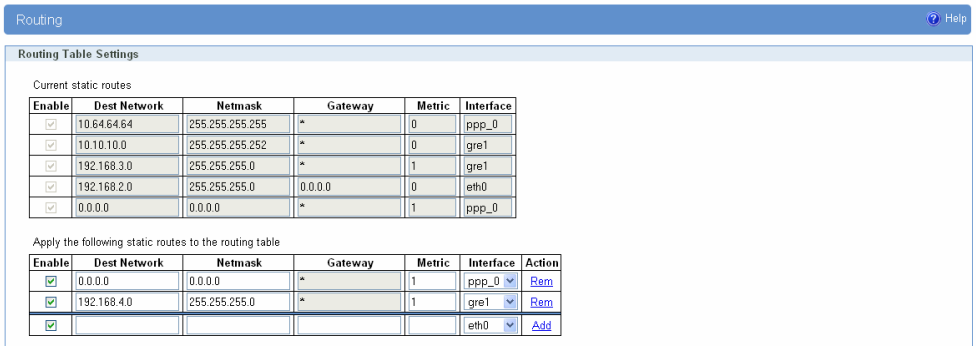


Figure 58 - Routing configuration page for GWR-I Router 2

- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.
- On the device connected on GWR-I router 2 setup default gateway 192.168.2.1

GRE Tunnel configuration between GWR-I Router and third party router

GRE tunnel is a type of a VPN tunnels, but it isn't a secure tunneling method. However, you can encrypt GRE packets with an encryption protocol such as IPSec to form a secure VPN.

On the diagram below (*Figure 59*) is illustrated simple network with two sites. Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

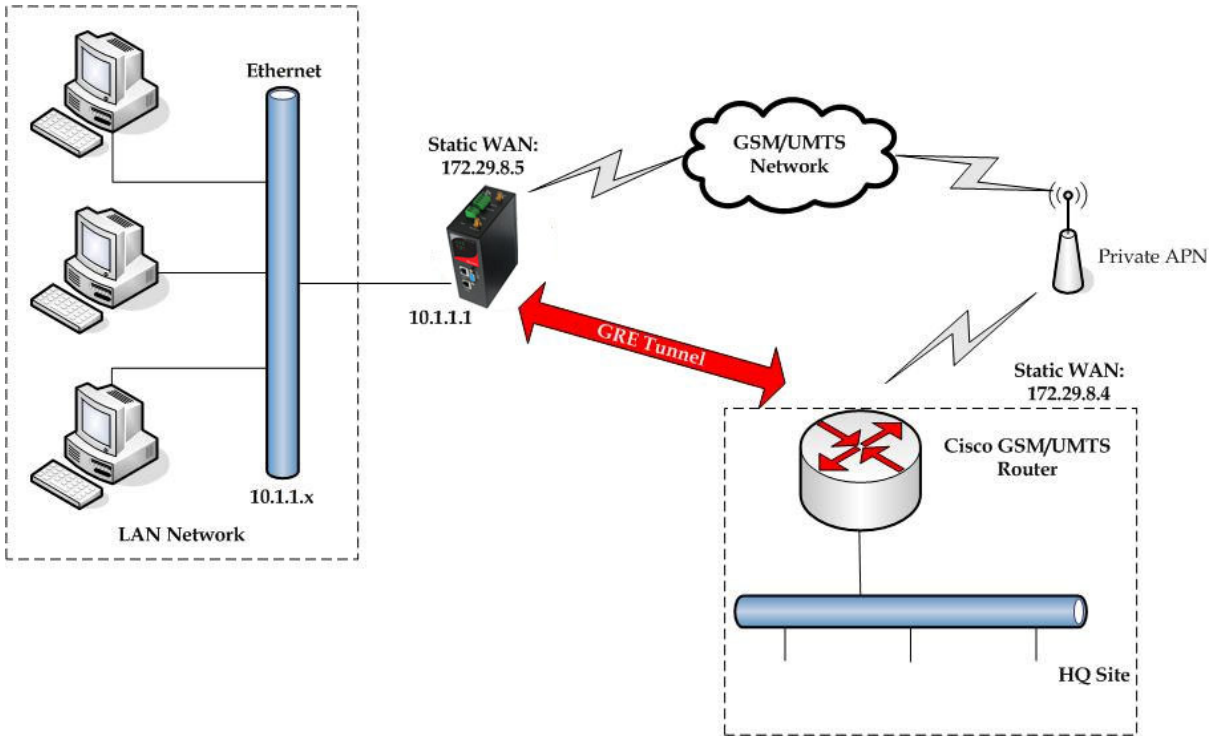


Figure 59 - GRE tunnel between Cisco router and GWR-I Router

GRE tunnel is created between Cisco router with GRE functionality on the HQ Site and the GWR-I Router on the Remote Network. In this example, it is necessary for both routers to create tunnel interface (virtual interface). This new tunnel interface is its own network. To each of the routers, it appears that it has two paths to the remote physical interface and the tunnel interface (running through the tunnel). This tunnel could then transmit unroutable traffic such as NetBIOS or AppleTalk.

The GWR-I Router uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside. All outgoing traffic uses the GWR-I Router WAN/VPN mobile IP address. HQ Cisco router acts like gateway to remote network for user in corporate LAN. It also performs function of GRE server for termination of GRE tunnel. The GWR-I Router act like default gateway for Remote Network and GRE server for tunnel.

1. HQ router requirements:
   - HQ router require static IP WAN address;
   - Router or VPN appliance have to support GRE protocol;
   - Tunnel peer address will be the GWR-I Router WAN's mobile IP address. For this reason, a static mobile IP address is preferred on the GWR-I Router WAN (GPRS) side;
   - Remote Subnet is remote LAN network address and Remote Subnet Mask is subnet of remote LAN.

2. The GWR-I Router requirements:

- Static IP WAN address;
- Peer Tunnel Address will be the HQ router WAN IP address (static IP address);
- Remote Subnet is HQ LAN IP address and Remote Subnet Mask is subnet mask of HQ LAN.

GSM/UMTS APN Type: For GSM/UMTS networks GWR-I Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

Cisco router sample Configuration:

```
Interface FastEthernet 0/1
ip address 10.2.2.1 255.255.255.0
description LAN interface

interface FastEthernet 0/0
ip address 172.29.8.4 255.255.255.0
description WAN interface

interface Tunnel0
ip address 10.1.1.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 172.29.8.5

ip route 10.1.1.0 255.255.255.0 tunnel0
```

The GWR-I Router Sample Configuration:

- Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 10.1.1.1
  - Subnet Mask: 255.255.255.0
  - Press ***Save*** to accept the changes.

Figure 60 - Network configuration page

- Use SIM card with a dynamic/static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider's network default gateway).
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > GRE Tunneling*** to configure new VPN tunnel parameters:
  - Enable: yes
  - Local Tunnel Address: 10.1.1.1
  - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252)
  - Tunnel Source: 172.29.8.5
  - Tunnel Destination: 172.29.8.4

- KeepAlive enable: no
- Period:(none)
- Retries:(none)
- Press ADD to put GRE tunnel rule into VPN table.
- Press ***Save*** to accept the changes.

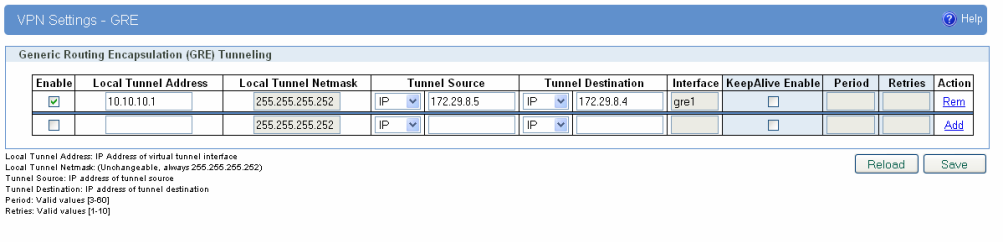


Figure 61 - GRE configuration page

- Configure GRE Route. Click ***Routing*** on ***Settings*** Tab. Parameters for this example are:
  - Destination Network: 10.2.2.0
  - Netmask: 255.255.255.0

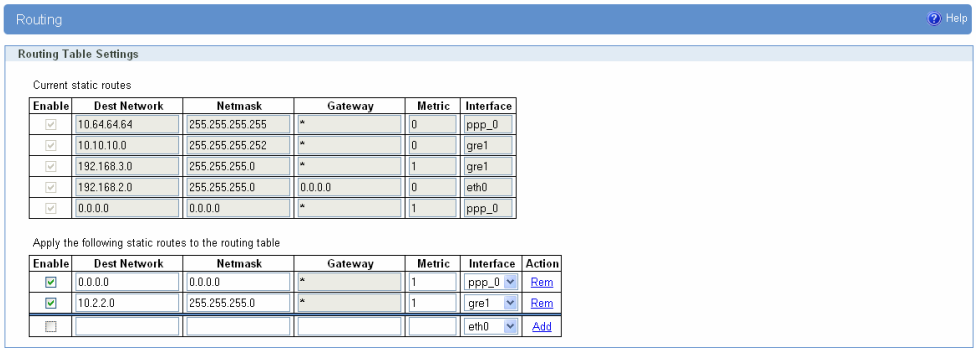


Figure 62 - Routing configuration page

- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.

User from remote LAN should be able to communicate with HQ LAN.

IPSec Tunnel configuration between two GWR-I Routers

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. Simple network with two GWR-I Routers is illustrated on the diagram below *Figure 63*. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

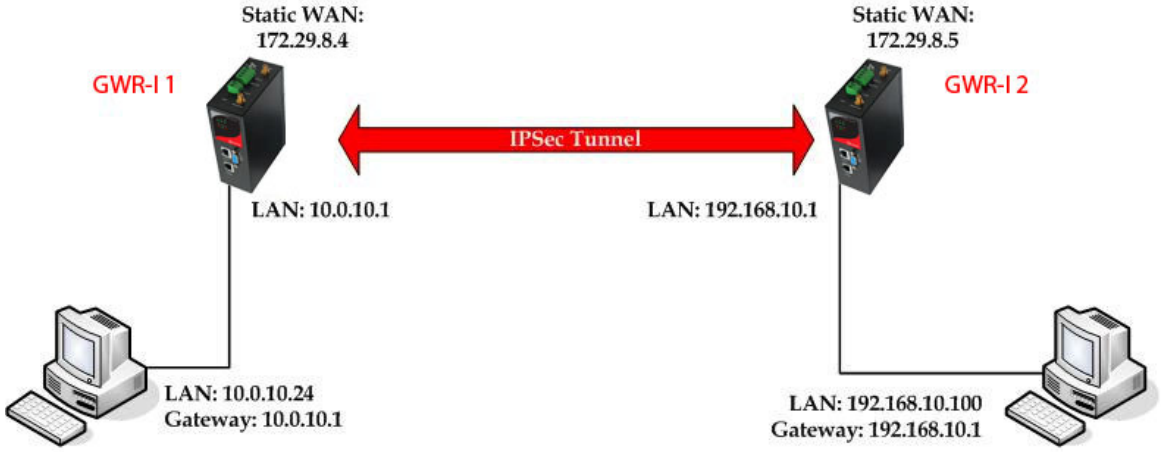


Figure 63 - IPSec tunnel between two GWR-I Routers

The GWR-I Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address
- Dynamic IP WAN address must be mapped to hostname with DynDNS service (for synchronization with DynDNS server SIM card must have internet access)

GSM/UMTS APN Type: For GSM/UMTS networks GWR-I Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs

For the purpose of detailed explanation of IPSec tunnel configuration , two scenarios will be examined and network illustrated in the *Figure* 63 will be used for both scenarios.

Scenario #1

Router 1 and Router 2 , presented in the *Figure* 63, have firmware version that provides three modes of negotiation in IPSec tunnel configuration process:

- Aggressive
- Main
- Base

In this scenario, aggressive mode will be used. Configurations for Router 1 and Router 2 are listed below.

The GWR-I Router 1 configuration:

Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask:

- IP Address: 10.0.10.1
- Subnet Mask: 255.255.255.0
- Press ***Save*** to accept the changes.

Figure 64 - Network configuration page for GWR-I Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > IPSEC*** to configure IPSEC tunnel parameters. Click ***Add New Tunnel*** button to create new IPSec tunnel. Tunnel parameters are:
  - ***Add New Tunnel***
    - Tunnel Name: test
    - Enable: true
  - ***IPSec Setup***
    - Keying Mode: IKE with Preshared key
    - Phase 1 DH group: Group 2
    - Phase 1 Encryption: 3DES
    - Phase 1 Authentication: MD5
    - Phase 1 SA Life Time: 28800
    - Perfect Forward Secrecy: true
    - Phase 2 DH group: Group 2
    - Phase 2 Encryption: DES
    - Phase 2 Authentication: MD5
    - Phase 2 SA Life Time: 3600
    - Preshared Key: 1234567890
  - ***Local Group Setup***
    - Local Security Gateway Type: SIM card
    - IP Address From: SIM 1 (WAN connection is established over SIM 1)
    - Local ID Type: IP Address
    - Local Security Group Type: Subnet
    - IP Address: 10.0.10.0
    - Subnet Mask: 255.255.255.0
  - ***Remote Group Setup***
    - Remote Security Gateway Type: IP Only
    - IP Address: 172.29.8.5
    - Remote ID Type: IP Address
    - Remote Security Group Type: IP
    - IP Address: 192.168.10.1

Failover

- Enable Tunnel Failover: false

- ***Advanced***
  - Negotiation Mode: Aggressive
  - Compress(Support IP Payload Compression Protocol(IPComp)): false
  - Dead Peer Detection(DPD): false
  - NAT Traversal: true
  - Send Initial Contact: true

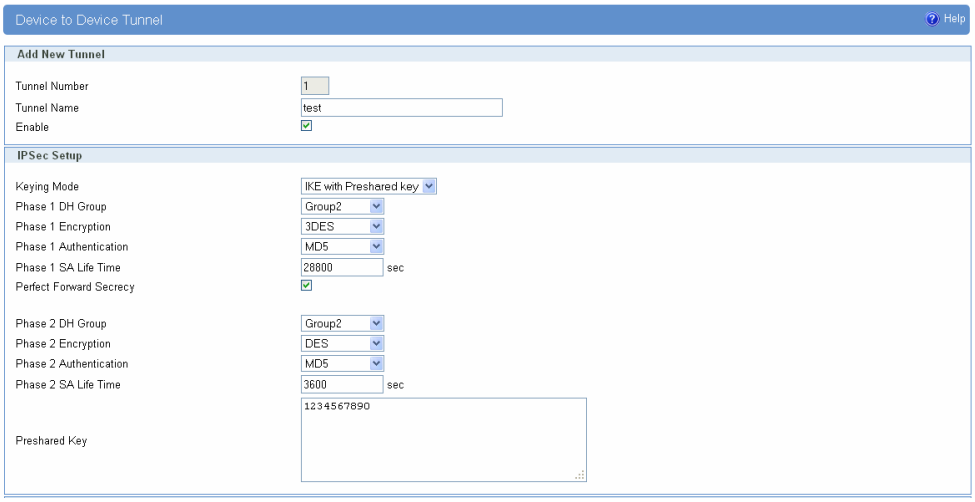


Figure 65 - IPSEC configuration page I for GWR-I Router 1

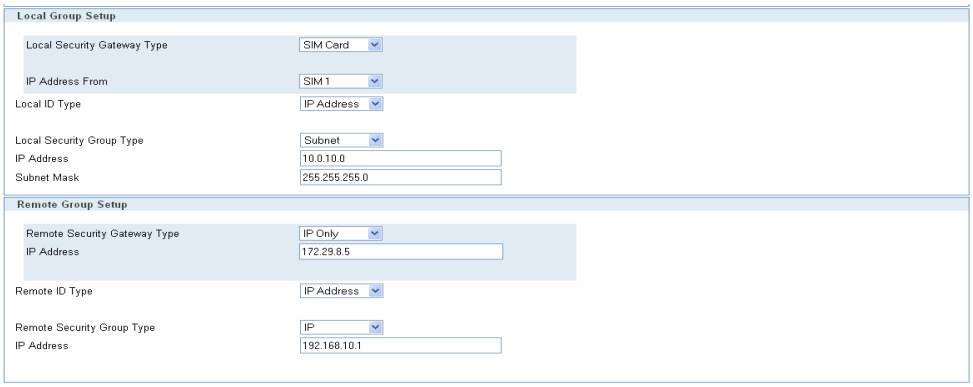


Figure 66 - IPSec configuration page II for GWR-I Router 1

NOTE : If option NAT Traversal is selected Aggressive mode is predefined.

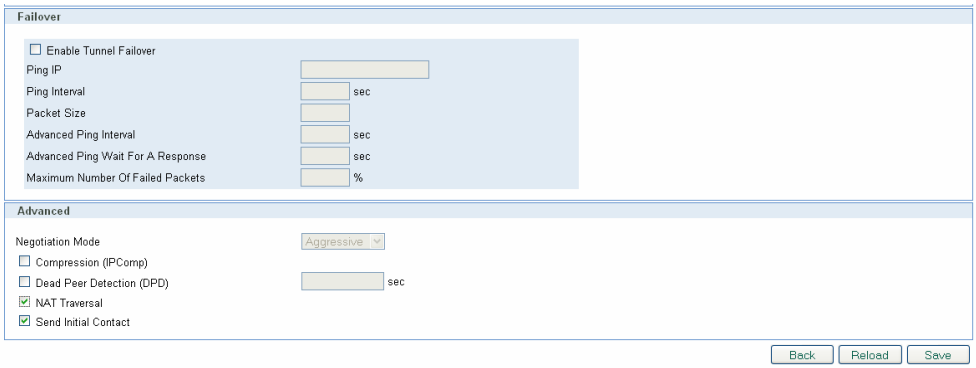


Figure 67 - IPSec configuration page III for GWR-I Router 1

- Click ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel

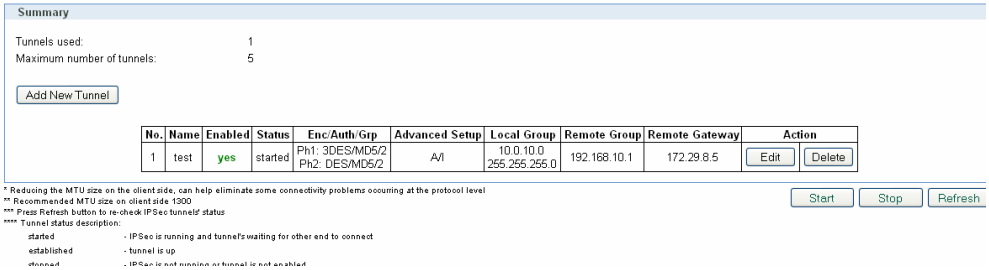


Figure 68 – IPSec start/stop page for GWR-I Router 1

- On the device connected on GWR-I router 1 setup default gateway 10.0.10.1

The GWR-I Router 2 configuration:

- Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 192.168.10.1
  - Subnet Mask: 255.255.255.0

  Press ***Save*** to accept the changes.

Figure 69 - Network configuration page for GWR-I Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > IPSEC*** to configure IPSEC tunnel parameters. Click ***Add New Tunnel*** button to create new IPSec tunnel. Tunnel parameters are:
  - ***Add New Tunnel***
    - Tunnel Name: test
    - Enable: true
  - ***IPSec Setup***
    - Keying Mode: IKE with Preshared key
    - Phase 1 DH group: Group 2
    - Phase 1 Encryption: 3DES
    - Phase 1 Authentication: MD5
    - Phase 1 SA Life Time: 28800
    - Perfect Forward Secrecy: true
    - Phase 2 DH group: Group 2
    - Phase 2 Encryption: DES
    - Phase 2 Authentication: MD5
    - Phase 2 SA Life Time: 3600
    - Preshared Key: 1234567890

  - ***Local Group Setup***
    - Local Security Gateway Type: SIM card
    - IP Address From: SIM 1 (WAN connection is established over SIM 1)
    - Local ID Type: IP Address
    - Local Security Group Type: IP
    - IP Address: 192.168.10.1
  - ***Remote Group Setup***
    - Remote Security Gateway Type: IP Only
    - IP Address: 172.29.8.4
    - Remote ID Type: IP Address
    - Remote Security Group Type: Subnet
    - IP Address: 10.0.10.0
    - Subnet: 255.255.255.0

  - ***Failover***
    - Enable Tunnel Failover: false
  - ***Advanced***
    - Negotiation Mode: Aggressive
    - Compress(Support IP Payload Compression Protocol(IPComp)): false
    - Dead Peer Detection(DPD): false
    - NAT Traversal: true
    - Send Initial Contact: true

    Press ***Save*** to accept the changes.

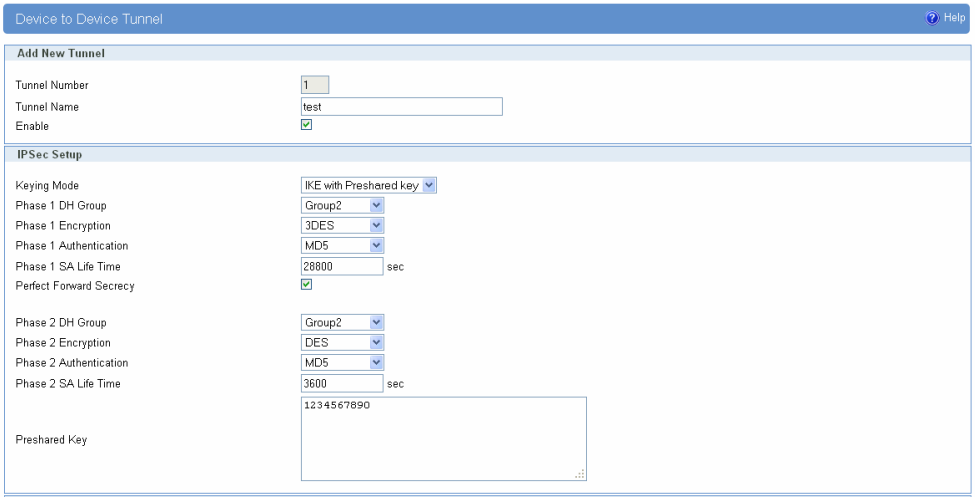


Figure 70 - IPSEC configuration page I for GWR-I Router 2

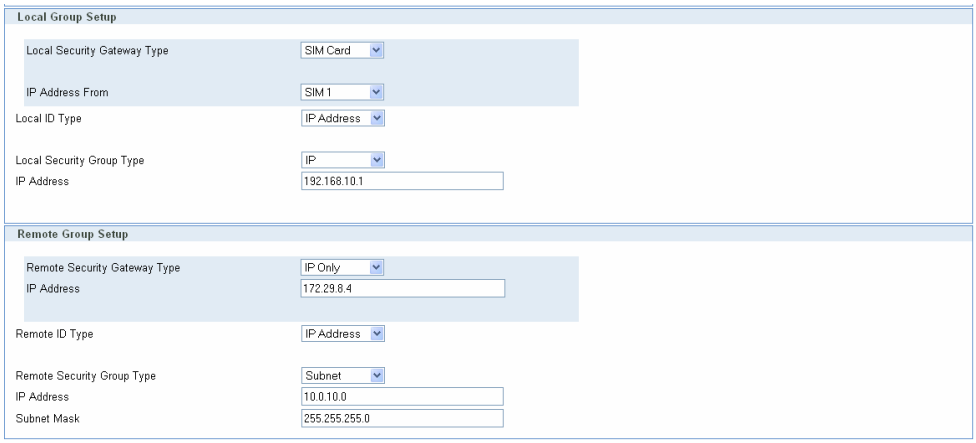


Figure 71 - IPSec configuration page II for GWR-I Router 2

NOTE : If option NAT Traversal is selected Aggressive mode is predefined.

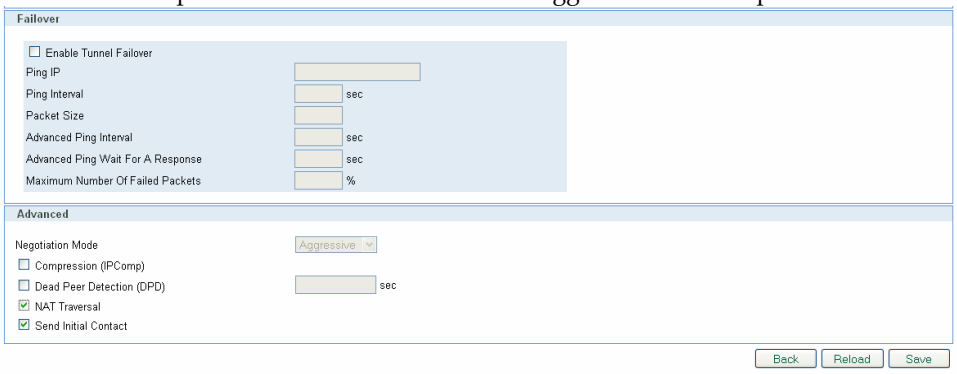


Figure 72 - IPSec configuration page III for GWR-I Router 2

- Click ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel

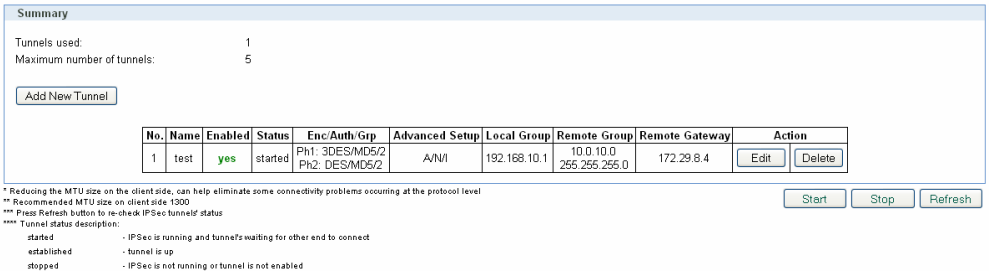


Figure 73 – IPSec start/stop page for GWR-I Router 2

- On the device connected on GWR-I router 2 setup default gateway 192.168.10.1.

Scenario #2

Router 1 and Router 2, presented in the Figure 63, have firmware version that provides single mode of negotiation in IPSec tunnel configuration process – Main mode. Considering this, both routers will be in main mode and there will not be displayed option for Negotiation mode in IPSec configurations.

Configurations for Router 1 and Router 2 are listed below.

The GWR-I Router 1 configuration:

Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask:

- IP Address: 10.0.10.1
- Subnet Mask: 255.255.255.0
- Press ***Save*** to accept the changes.

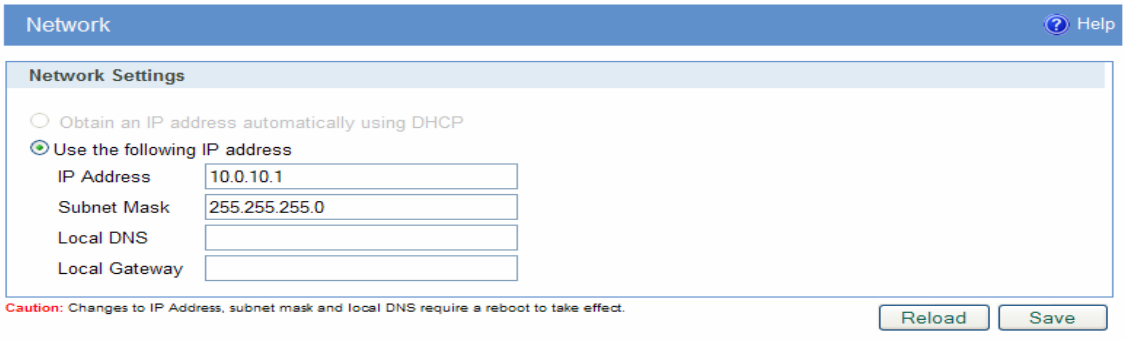


Figure 74 - Network configuration page for GWR-I Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > IPSEC*** to configure IPSEC tunnel parameters. Click ***Add New Tunnel*** button to create new IPSec tunnel. Tunnel parameters are:
    - ***Add New Tunnel***
        - Tunnel Name: test
        - Enable: true
    - ***IPSec Setup***
        - Keying Mode: IKE with Preshared key
        - Phase 1 DH group: Group 2
        - Phase 1 Encryption: 3DES
        - Phase 1 Authentication: MD5
        - Phase 1 SA Life Time: 28800
        - Perfect Forward Secrecy: true
        - Phase 2 DH group: Group 2
        - Phase 2 Encryption: DES
        - Phase 2 Authentication: MD5
        - Phase 2 SA Life Time: 3600
        - Preshared Key: 1234567890

    - ***Local Group Setup***
        - Local Security Gateway Type: SIM card
        - IP Address From: SIM 1 (WAN connection is established over SIM 1)
        - Custom Peer ID: false
        - Local Security Group Type: Subnet
        - IP Address: 10.0.10.0
        - Subnet Mask: 255.255.255.0
    - ***Remote Group Setup***
        - Remote Security Gateway Type: IP Only
        - IP Address: 172.29.8.5
        - Custom Peer ID: false
        - Remote Security Group Type: IP
        - IP Address: 192.168.10.1
    - ***Failover***
        - Eanble IKE failover: false
        - Enable Tunnel Failover: false
    - ***Advanced***
        - Compress(Support IP Payload Compression Protocol(IPComp)): false
        - Dead Peer Detection(DPD): false
        - NAT Traversal: true
        - Send Initial Contact: true

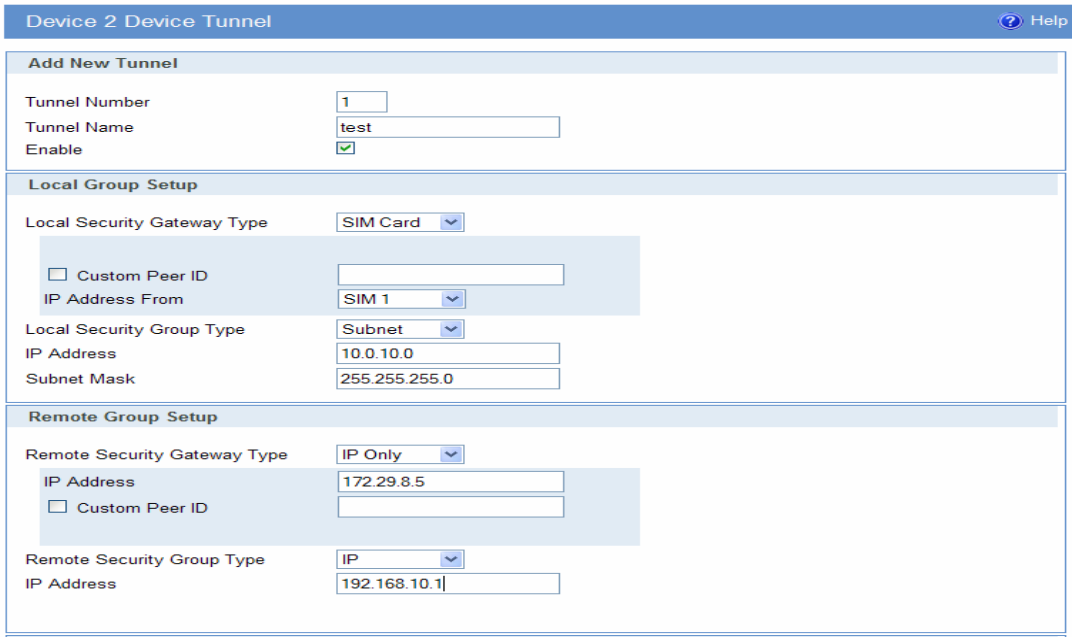


Figure 75 - IPSEC configuration page I for GWR-I Router 1

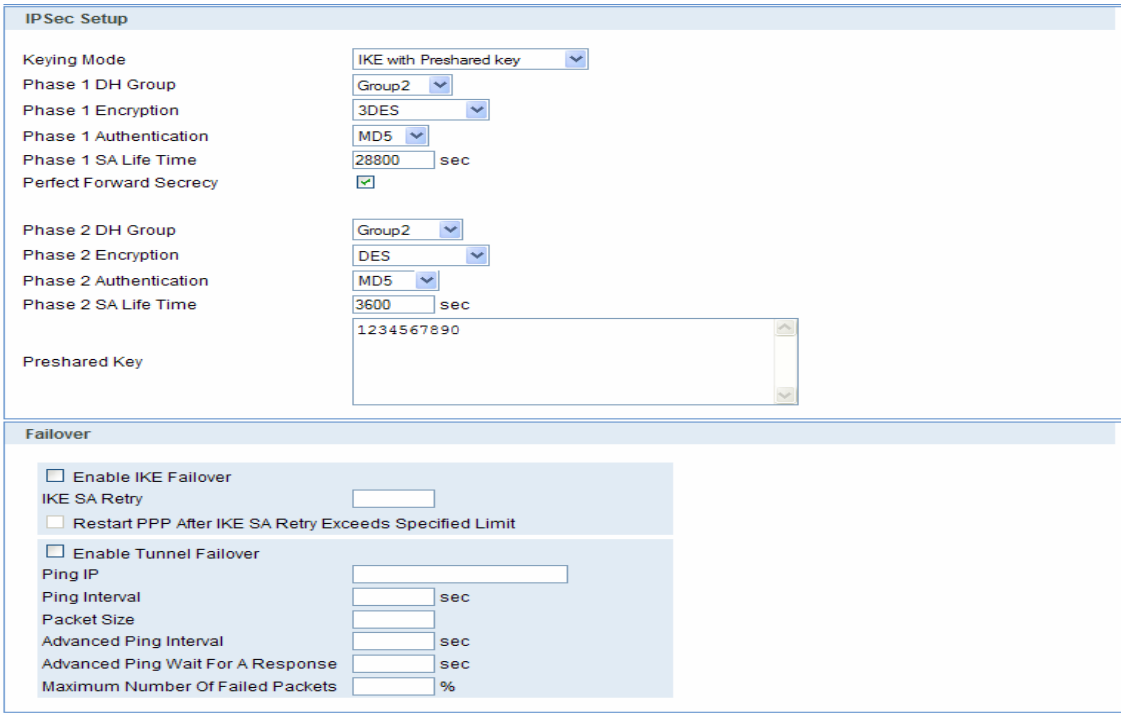


Figure 76 - IPSEC configuration page II for GWR-I Router 1

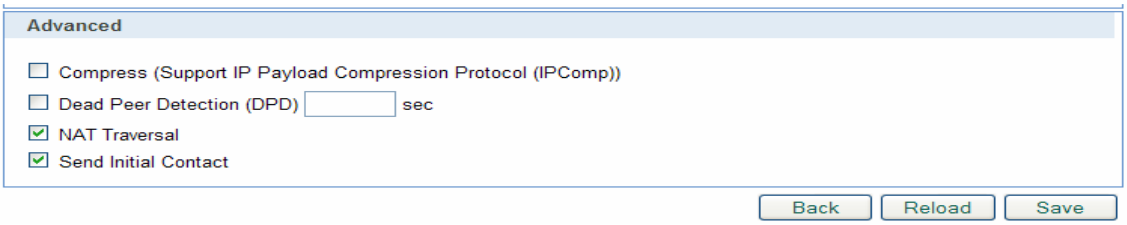


Figure 77 - IPSEC configuration page III for GWR-I Router 1

***NOTE**: Firmware version used in this scenario also provides options for Connection mode of IPSec tunnel.*

If connection mode Connect is selected that indicates side of IPSec tunnel which sends requests for establishing of the IPSec tunnel.

If connection mode Wait is selected that indicates side of IPSec tunnel which listens and responses to IPSec establishing requests from Connect side.

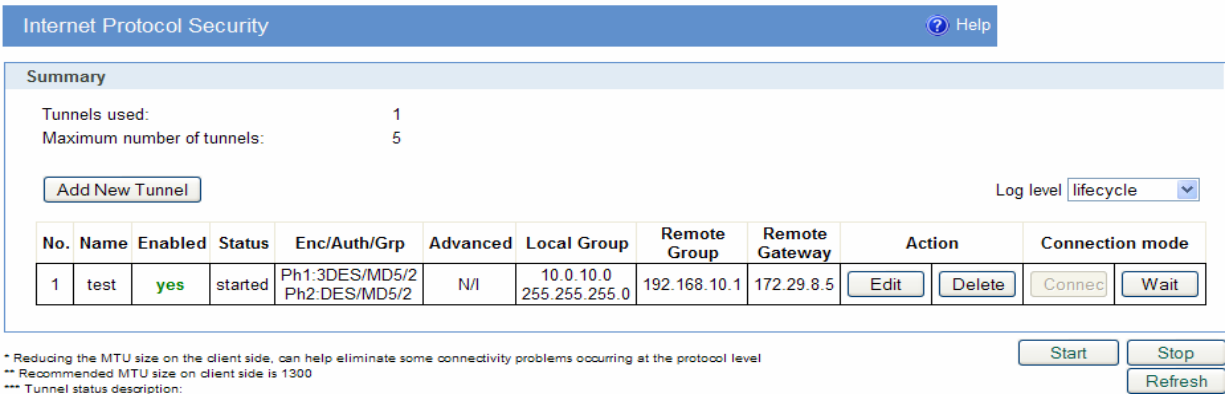


Figure 78 – IPSec start/stop page for GWR-I Router 1

Click ***Connect*** button and after that ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel

- On the device connected on GWR-I router 1 setup default gateway 10.0.10.1

The GWR-I Router 2 configuration:

- Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 192.168.10.1
  - Subnet Mask: 255.255.255.0

  Press ***Save*** to accept the changes.

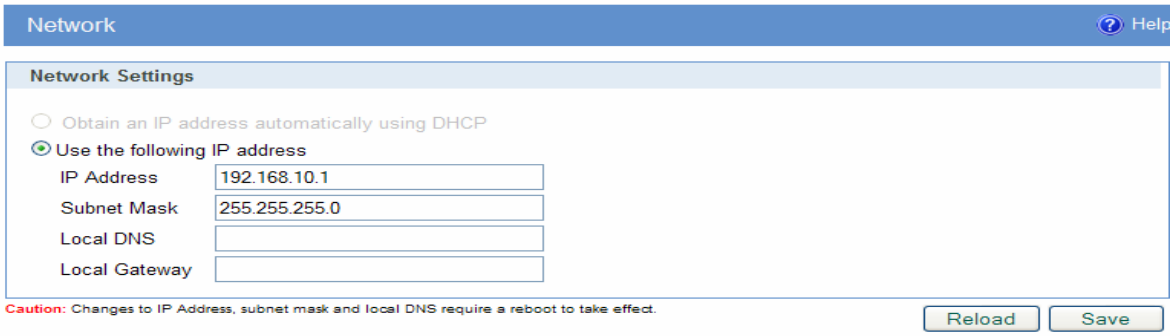


Figure 79 - Network configuration page for GWR-I Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > IPSEC*** to configure IPSEC tunnel parameters. Click ***Add New Tunnel*** button to create new IPSec tunnel. Tunnel parameters are:
  - ***Add New Tunnel***
    - Tunnel Name: test
    - Enable: true
  - ***IPSec Setup***
    - Keying Mode: IKE with Preshared key
    - Phase 1 DH group: Group 2
    - Phase 1 Encryption: 3DES
    - Phase 1 Authentication: MD5
    - Phase 1 SA Life Time: 28800
    - Perfect Forward Secrecy: true
    - Phase 2 DH group: Group 2
    - Phase 2 Encryption: DES
    - Phase 2 Authentication: MD5
    - Phase 2 SA Life Time: 3600
    - Preshared Key: 1234567890
  - ***Local Group Setup***
    - Local Security Gateway Type: SIM card
    - IP Address From: SIM 1 (WAN connection is established over SIM 1)
    - Custom Peer ID: false
    - Local Security Group Type: IP
    - IP Address: 192.168.10.1
  - ***Remote Group Setup***
    - Remote Security Gateway Type: IP Only
    - IP Address: 172.29.8.4
    - Custom Peer ID: false
    - Remote Security Group Type: Subnet

- IP Address: 10.0.10.0
- Subnet: 255.255.255.0

- ***Failover***
  - Enable IKE failover: false
  - Enable Tunnel Failover: false
- ***Advanced***
  - Compress(Support IP Payload Compression Protocol(IPComp)): false
  - Dead Peer Detection(DPD): false
  - NAT Traversal: true
  - Send Initial Contact: true

  Press ***Save*** to accept the changes.

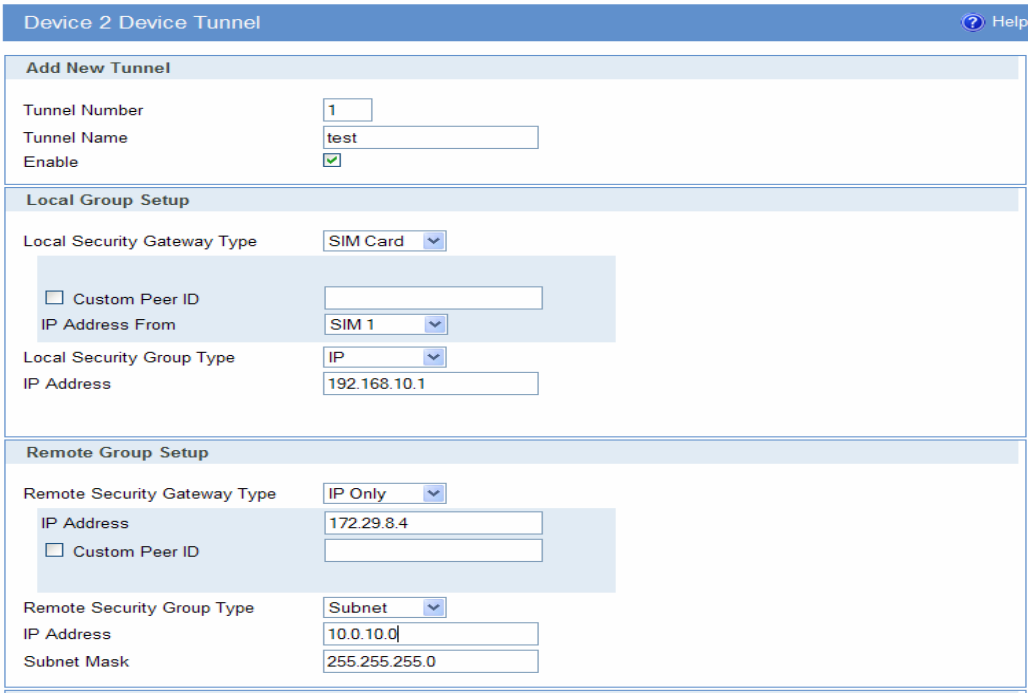


Figure 80 - IPSEC configuration page I for GWR-I Router 2

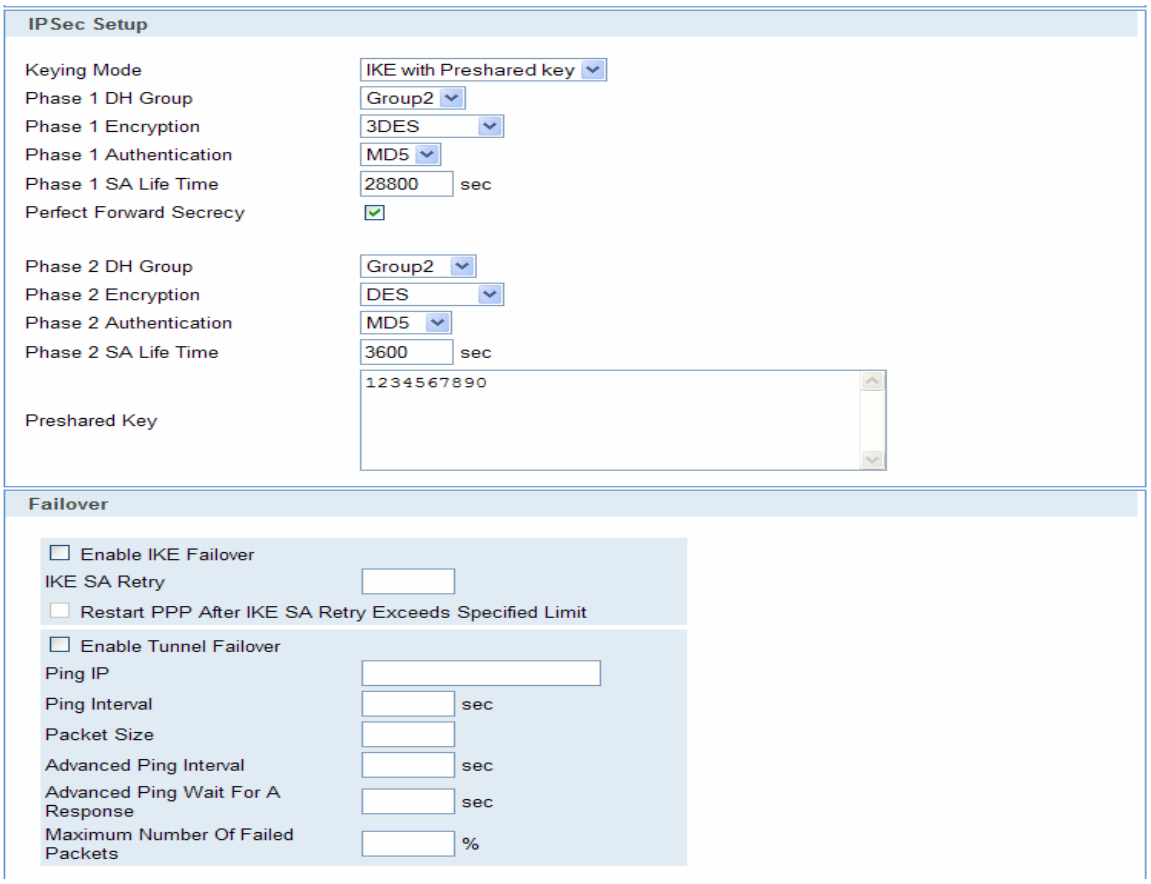


Figure 81 - IPSEC configuration page II for GWR-I Router 2

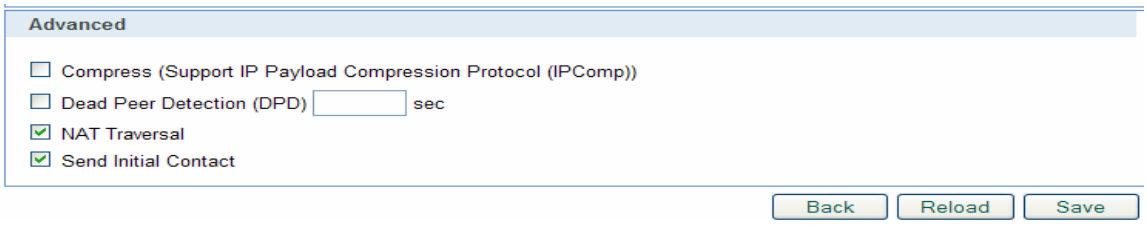


Figure 82 - IPSEC configuration page III for GWR-I Router 2

***NOTE**: Firmware version used in this scenario also provides options for Connection mode of IPSec tunnel.*

If connection mode Connect is selected that indicates side of IPSec tunnel which sends requests for establishing of the IPSec tunnel.

If connection mode Wait is selected that indicates side of IPSec tunnel which listens and responses to IPSec establishing requests from Connect side.

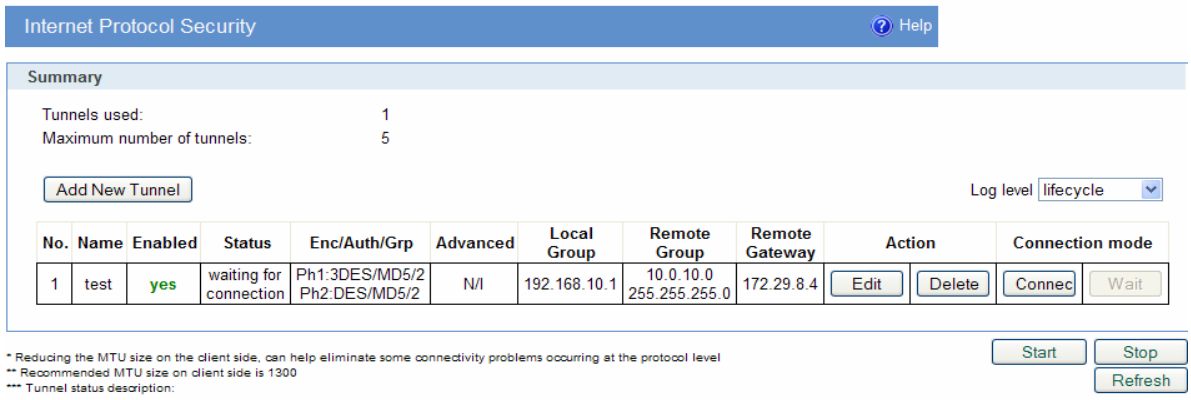


Figure 83 – IPSec start/stop page for GWR-I Router 1

Click ***Wait*** button and after that ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel

- On the device connected on GWR-I router 2 setup default gateway 192.168.10.1.

IPSec Tunnel configuration between GWR-I Router and Cisco Router

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. Diagram below illustrates simple network with GWR-I Router and Cisco Router. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

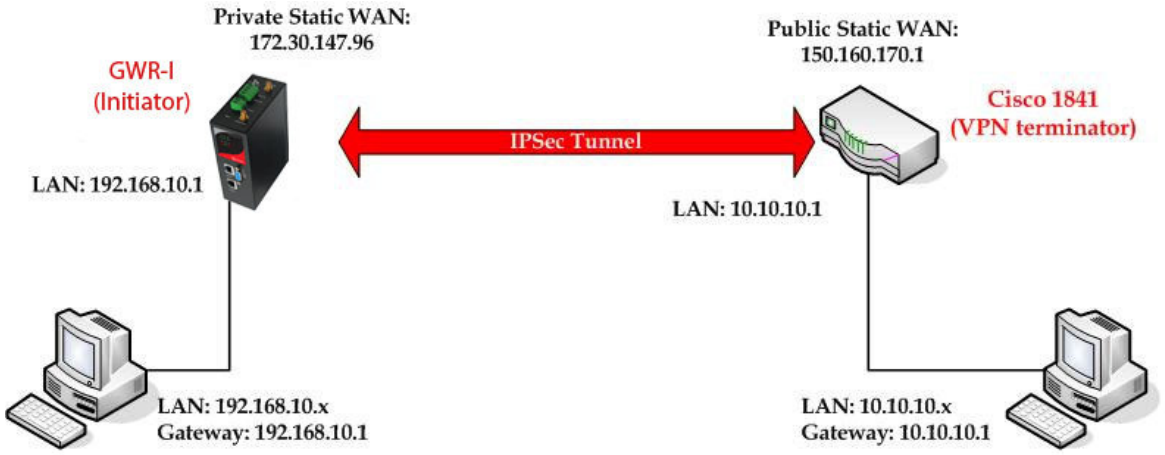


Figure 84 - IPSec tunnel between GWR-I Router and Cisco Router

The GWR-I Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address
- Dynamic IP WAN address must be mapped to hostname with DynDNS service (for synchronization with DynDNS server SIM card must have internet access)

GSM/UMTS APN Type: For GSM/UMTS networks GWR-I Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

The GWR-I Router configuration:

- Click ***Network*** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 192.168.10.1
  - Subnet Mask: 255.255.255.0

  Press ***Save*** to accept the changes.

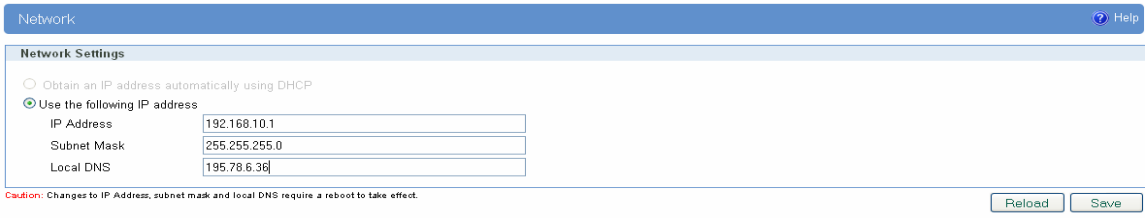


Figure 85 - Network configuration page for GWR-I Router

- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > IPSEC*** to configure IPSEC tunnel parameters. Click ***Add New Tunnel*** button to create new IPSec tunnel. Tunnel parameters are:
    - ***Add New Tunnel***
        - Tunnel Name: test
        - Enable: true
    - ***IPSec Setup***
        - Keying Mode: IKE with Preshared key
        - Phase 1 DH group: Group 2
        - Phase 1 Encryption: 3DES
        - Phase 1 Authentication: SHA
        - Phase 1 SA Life Time: 28800
        - Perfect Forward Secrecy: true
        - Phase 2 DH group: Group 2
        - Phase 2 Encryption: 3DES
        - Phase 2 Authentication: SHA1
        - Phase 2 SA Life Time: 3600
        - Preshared Key: 1234567890

    - ***Local Group Setup***
        - Local Security Gateway Type: SIM card
        - IP Address From: SIM 1 (WAN connection is established over SIM 1)
        - Local ID Type: IP Address
        - Local Security Group Type: Subnet
        - IP Address: 192.168.10.0
        - Subnet Mask: 255.255.255.0
    - ***Remote Group Setup***
        - Remote Security Gateway Type: IP Only
        - IP Address: 150.160.170.1
        - Remote ID Type: IP Address
        - Remote Security Group Type: Subnet
        - IP Address: 10.10.10.0
        - Subnet Mask: 255.255.255.0
    - ***Failover***
        - Enable Tunnel Failover: false
    - ***Advanced***
        - Negotiation Mode: Aggressive
        - Compress(Support IP Payload Compression Protocol(IPComp)): false
        - Dead Peer Detection(DPD): false
        - NAT Traversal: true
        - Send Initial Contact Notification: true

      Press ***Save*** to accept the changes.

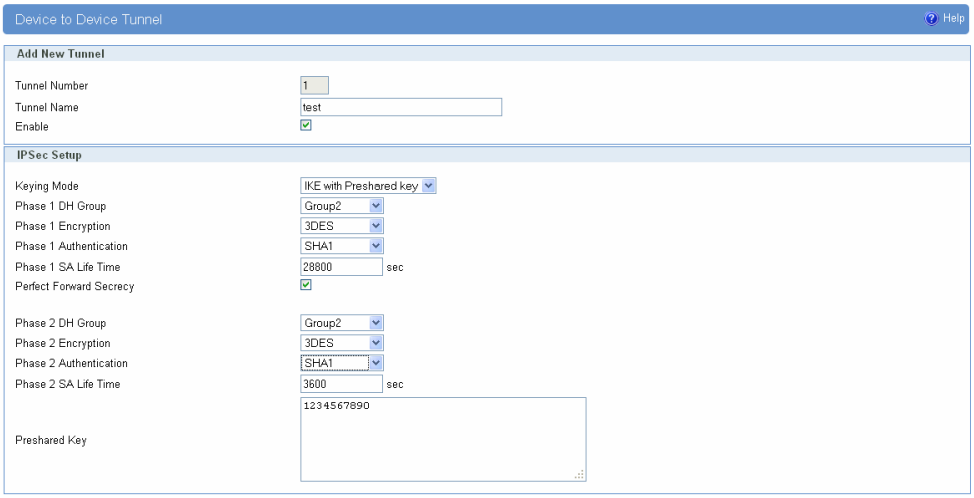


Figure 86 - IPSEC configuration page I for GWR-I Router

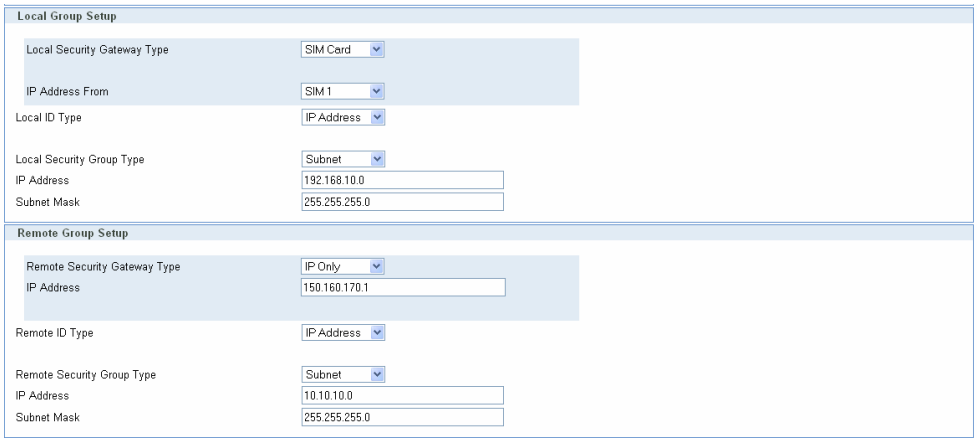


Figure 87 - IPSec configuration page II for GWR-I Router

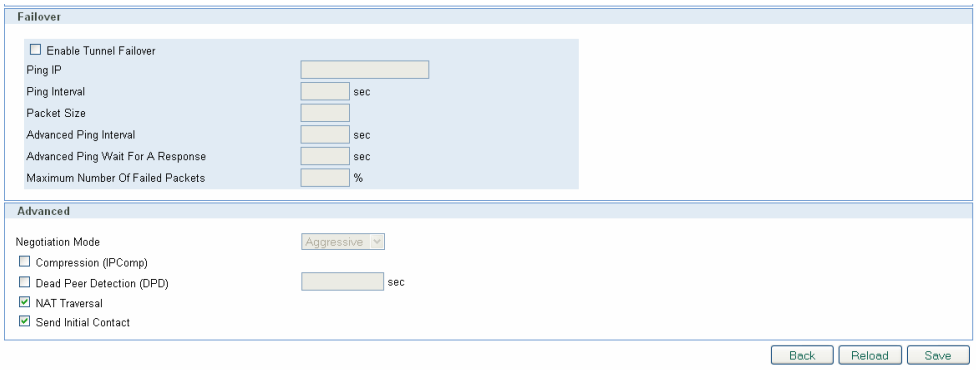


Figure 88 - IPSec configuration page III for GWR-I Router

- Click ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel

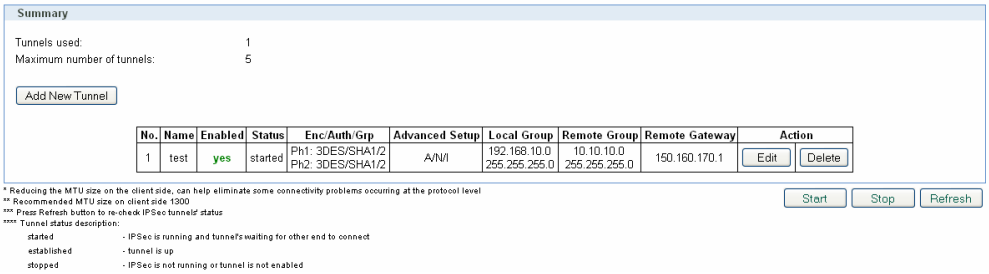


Figure 89 – IPSec start/stop page for GWR-I Router

- On the device connected on GWR-I router setup default gateway 192.168.10.1.

The Cisco Router configuration:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco-Router
!
boot-start-marker
boot-end-marker
!
username admin password 7 ****************
!
enable secret 5 **********************
!
no aaa new-model
!
no ip domain lookup
!
!--- Keyring that defines wildcard pre-shared key.
!
crypto keyring remote
    pre-shared-key address 0.0.0.0  0.0.0.0   key  1234567890
!
!--- ISAKMP policy
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
  lifetime 28800
!
!--- Profile for LAN-to-LAN connection, that references
!--- the wildcard pre-shared key and a wildcard identity
!
crypto isakmp profile L2L
   description LAN to LAN  vpn connection
   keyring remote
   match identity address 0.0.0.0
!
!
crypto ipsec transform-set  testGWR  esp-3des esp-sha-hmac
!
!--- Instances of the dynamic crypto map
!--- reference previous IPsec profile.
!
crypto dynamic-map dynGWR 5
 set transform-set testGWR
 set isakmp-profile L2L
!
!--- Crypto-map only references instances of the previous dynamic crypto map.
!
```

```
crypto map GWR 10 ipsec-isakmp dynamic dynGWR
!
interface FastEthernet0/0
 description WAN INTERFACE
 ip address 150.160.170.1 255.255.255.252
 ip nat outside
no ip route-cache
 no ip mroute-cache
duplex auto
speed auto
 crypto map GWR
!
interface FastEthernet0/1
 description LAN INTERFACE
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0  150.160.170.2
!
ip http server
no ip http secure-server
ip nat inside source list nat_list interface FastEthernet0/0 overload
!
ip access-list extended nat_list
 deny   ip 10.10.10.0  0.0.0.255  192.168.10.0  0.0.0.255
 permit ip 10.10.10.0  0.0.0.255  any
!
access-list 23 permit any
!
line con 0
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

Use this section to confirm that your configuration works properly. Debug commands that run on the Cisco router can confirm that the correct parameters are matched for the remote connections.

- **show ip interface**—Displays the IP address assignment to the spoke router.
- **show crypto isakmp sa detail**—Displays the IKE SAs, which have been set-up between the IPsec initiators.
- **show crypto ipsec sa**—Displays the IPsec SAs, which have been set-up between the IPsec initiators.
- **debug crypto isakmp**—Displays messages about Internet Key Exchange (IKE) events.
- **debug crypto ipsec**—Displays IPsec events.
- **debug crypto engine**—Displays crypto engine events.

IPSec Tunnel configuration between GWR-I Router and Juniper SSG firewall

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. On the diagram below *Figure 90* is illustrated simple network with GWR-I Router and Cisco Router. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

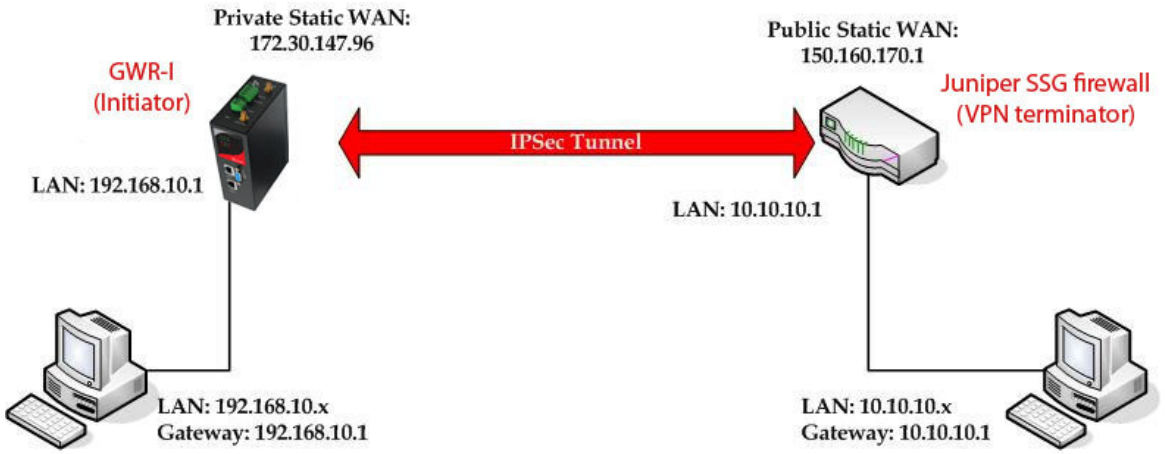


Figure 90 - IPSec tunnel between GWR-I Router and Cisco Router

The GWR-I Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address;
- Source tunnel address should have static WAN IP address;
- Destination tunnel address should have static WAN IP address;

GSM/UMTS APN Type: For GSM/UMTS networks GWR-I Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

The GWR-I Router configuration:

- Click *Network* Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 192.168.10.1
  - Subnet Mask: 255.255.255.0
  - Press ***Save*** to accept the changes.

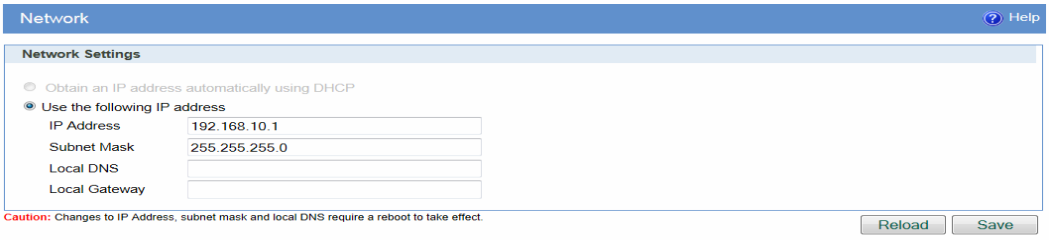


Figure 91 - Network configuration page for GWR-I Router

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***WAN Settings*** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***WAN Settings*** Tab). If disconnected please click ***Connect*** button.

- Click ***VPN Settings > IPSEC*** to configure IPSEC tunnel parameters. Click ***Add New Tunnel*** button to create new IPSec tunnel. Tunnel parameters are:
  - ***Add New Tunnel***
    - Tunnel Name: test
    - Enable: true
  - ***Local Group Setup***
    - Local Security Gateway Type: IP Only
    - IP Address: 172.30.147.96
    - Local ID Type: Custom
    - Custom Peer ID: 172.30.147.96
    - Local Security Group Type: Subnet
    - IP Address: 192.168.10.0
    - Subnet Mask: 255.255.255.0
  - ***Remote Group Setup***
    - Remote Security Gateway Type: IP Only
    - IP Address: 150.160.170.1
    - Remote ID Type: Custom
    - Custom Peer ID: 150.160.170.1
    - Remote Security Group Type: IP
    - IP Address: 10.10.10.0
    - Subnet Mask: 255.255.255.0
  - ***IPSec Setup***
    - Keying Mode: IKE with Preshared key
    - Phase 1 DH group: Group 2
    - Phase 1 Encryption: 3DES
    - Phase 1 Authentication: SHA1
    - Phase 1 SA Life Time: 28800
    - Perfect Forward Secrecy: true
    - Phase 2 DH group: Group 2
    - Phase 2 Encryption: 3DES
    - Phase 2 Authentication: SHA1
    - Phase 2 SA Life Time: 3600
    - Preshared Key: 1234567890
  - ***Advanced***
    - Aggressive Mode: true
    - Compress(Support IP Payload Compression Protocol(IPComp)): false
    - Dead Peer Detection(DPD): false
    - NAT Traversal: true
    - Press ***Save*** to accept the changes.

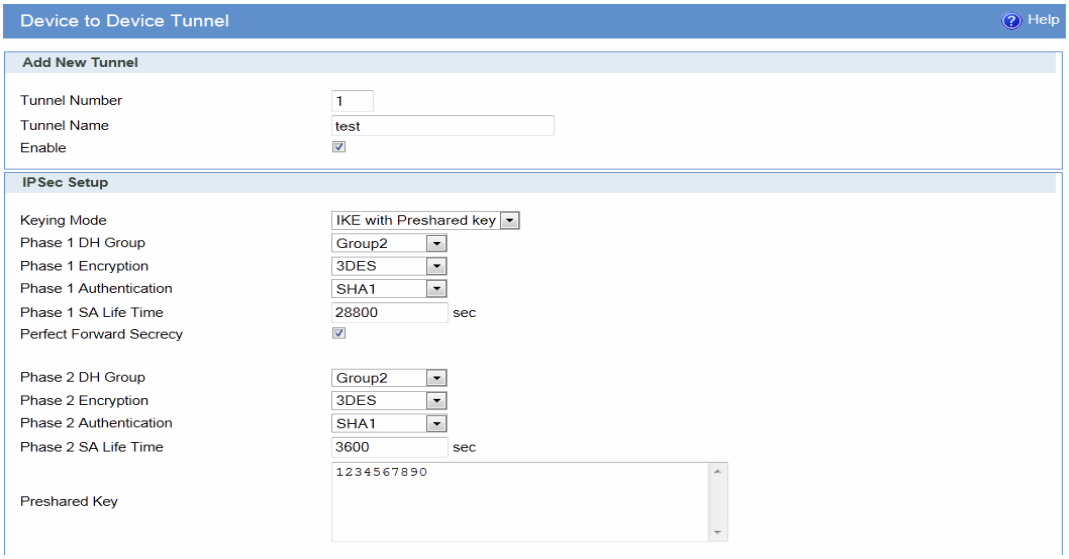


Figure 92 - IPSEC configuration page I for GWR-I Router

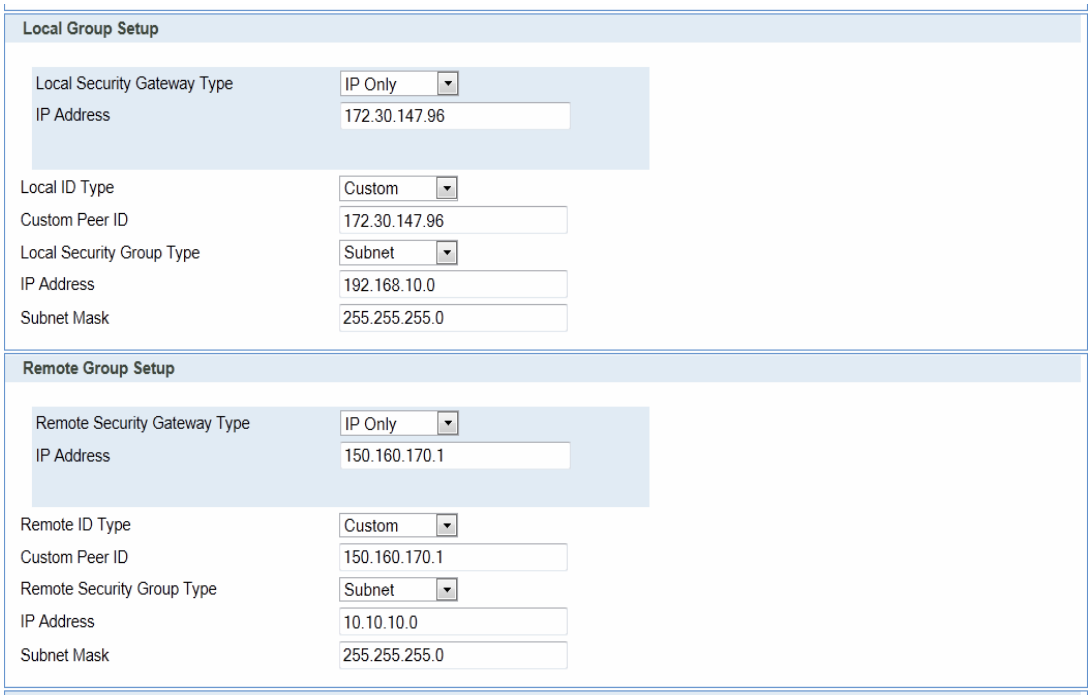


Figure 93 - IPSec configuration page II for GWR-I Router

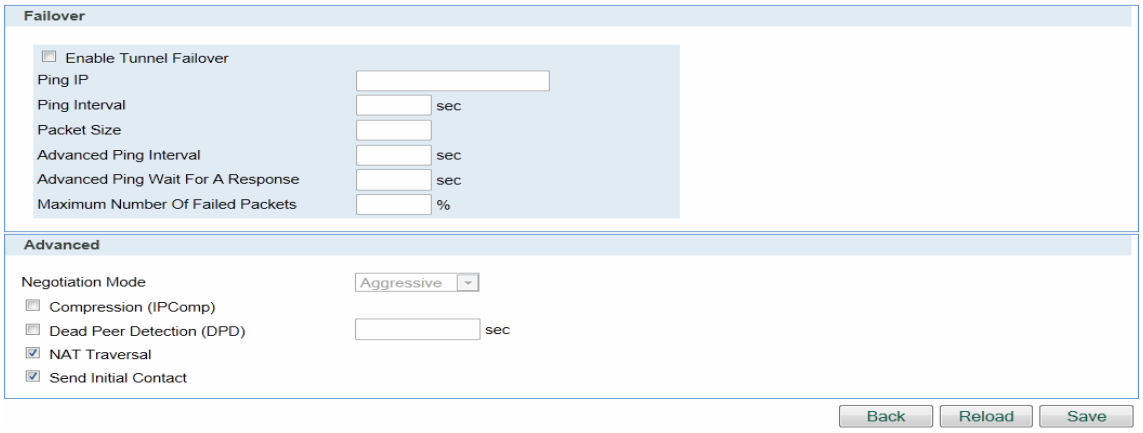


Figure 94 - IPSec configuration page III for GWR-I Router

- Click ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel.

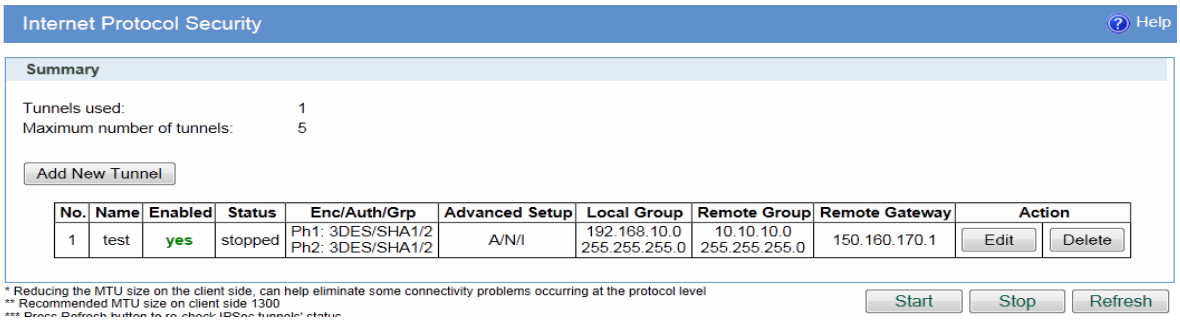


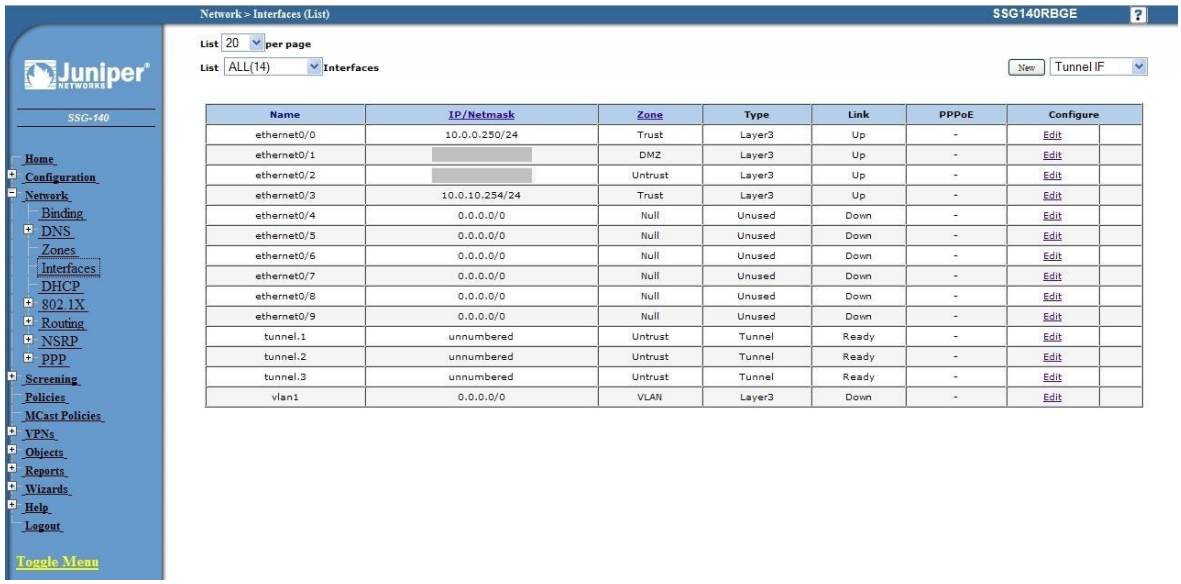
Figure 95 – IPSec start/stop page for GWR-I Router

- On the device connected on GWR-I router setup default gateway 192.168.10.1.

The Juniper SSG firewall configuration:

Step1 – Create New Tunnel Interface

- Click Interfaces on Network Tab.



Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
ethernet0/0	10.0.0.250/24	Trust	Layer3	Up	-	Edit
ethernet0/1	[redacted]	DMZ	Layer3	Up	-	Edit
ethernet0/2	[redacted]	Untrust	Layer3	Up	-	Edit
ethernet0/3	10.0.10.254/24	Trust	Layer3	Up	-	Edit
ethernet0/4	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/5	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/6	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/7	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/8	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/9	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.2	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.3	unnumbered	Untrust	Tunnel	Ready	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Figure 96 - Network Interfaces (list)

- Bind New tunnel interface to Untrust interface (outside int – with public IP addresss).
- Use unnumbered option for IP address configuration.

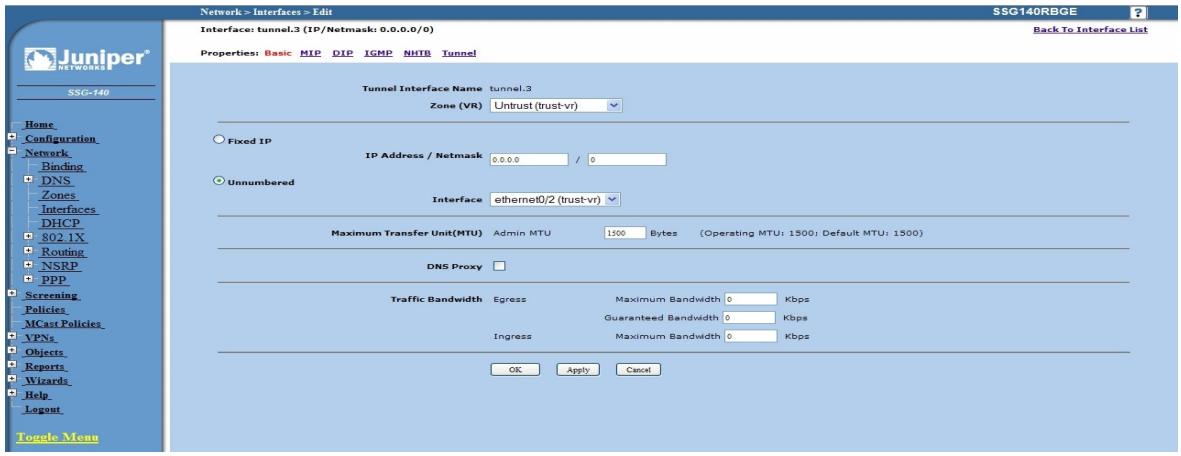


Figure 97 - Network Interfaces (edit)

Step 2 - Create New VPN IPSEC tunnel

- Click ***VPNs*** in main menu. To create new gateway click ***Gateway*** on ***AutoKey Advanced*** tab.

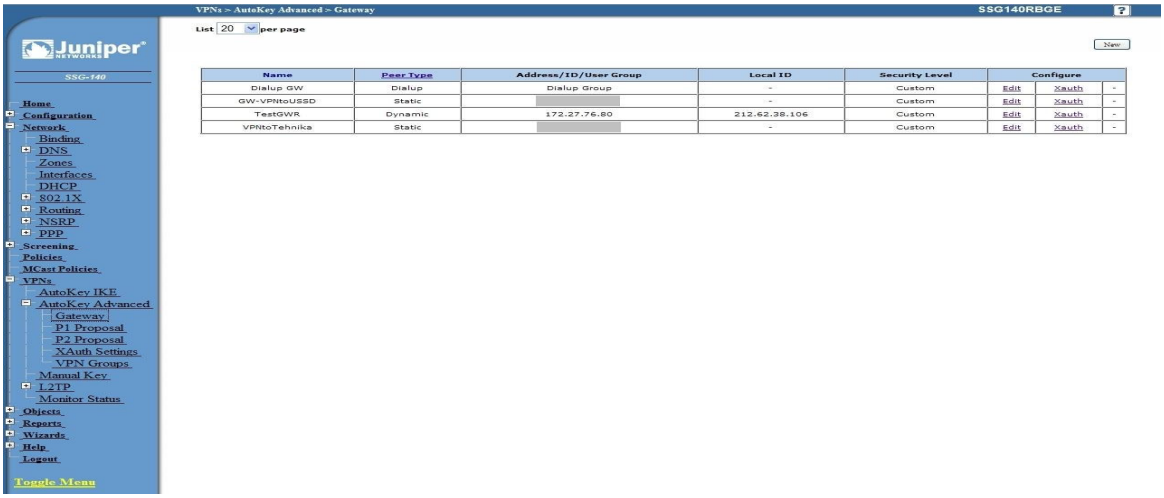


Figure 98 - AutoKey Advanced Gateway

- Click *New* button. Enter gateway parameters:
  - **Gateway name:** TestGWR
  - **Security level:** Custom
  - **Remote Gateway type:** Dynamic IP address(because your GWR-I router are hidden behind Mobile operator router's (firewall) NAT)
  - **Peer ID:** 172.30.147.96
  - **Presharedkey:** 1234567890
  - **Local ID:** 150.160.170.1

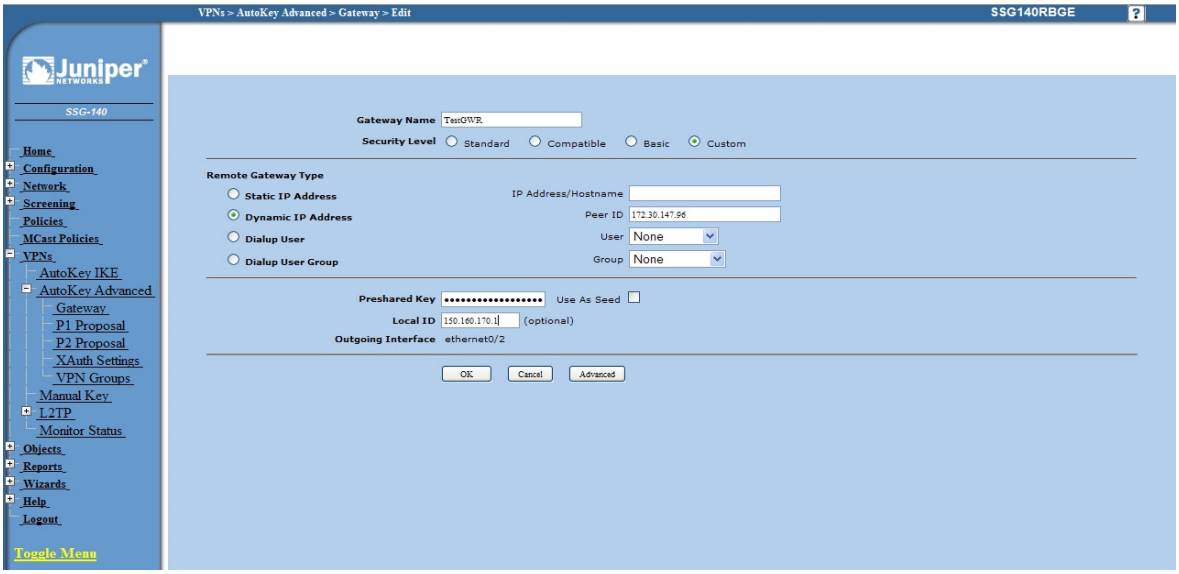


Figure 99 - Gateway parameters

- Click *Advanced* button.
  - **Security level – User Defined:** custom
  - **Phase 1 proposal:** pre-g2-3des-sha
  - **Mode:** Agressive(must be aggressive because of NAT)
  - **Nat-Traversal:** enabled
  - Click ***Return*** and ***OK***.

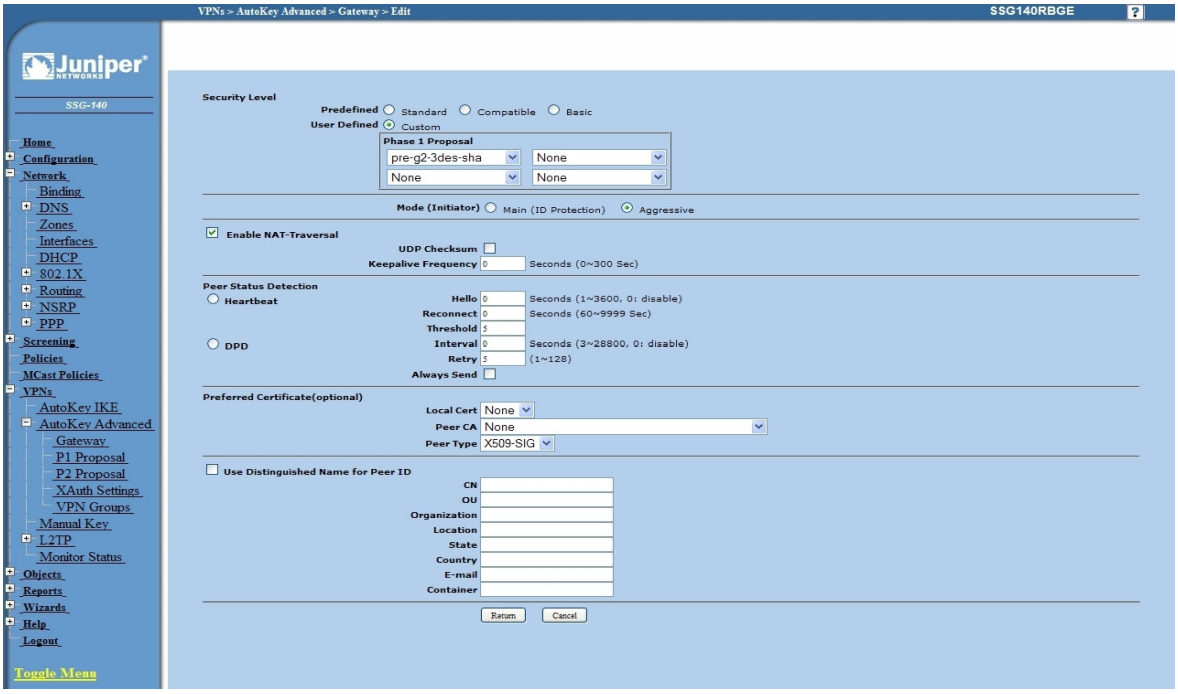


Figure 100 - Gateway advanced parameters

Step 3 - Create AutoKey IKE

- Click ***VPNs*** in main menu. Click ***AutoKey IKE.***
- Click ***New*** button.

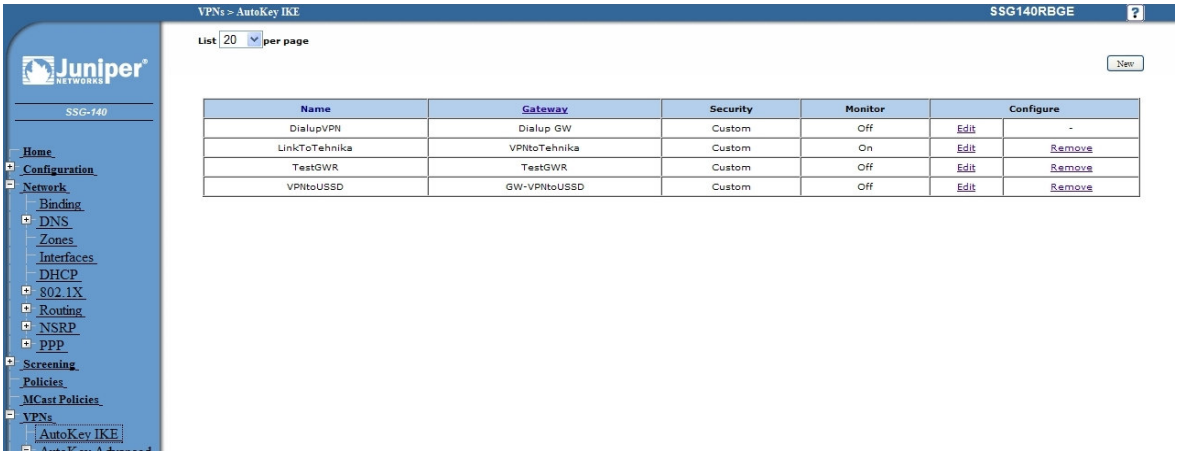


Figure 101 - AutoKey IKE

AutoKey IKE parameters are:

- **VPNname:** TestGWR
- **Security level:** Custom
- **Remote Gateway:** Predefined
- Choose VPN Gateway from step 2

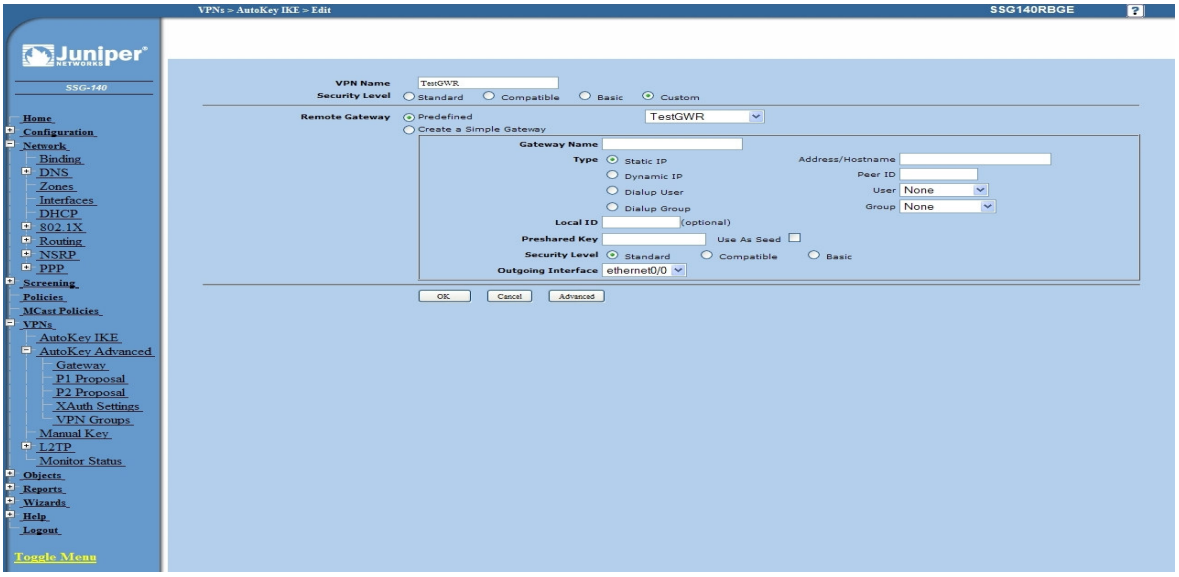


Figure 102 - AutoKey IKE parameters

- Click ***Advanced*** button.
  - **Security level - User defined:** custom
  - **Phase 2 proposal:** pre-g2-3des-sha
  - **Bind to - Tunnel interface:** tunnel.3(from step 1)
  - **Proxy ID:** Enabled
  - **LocalIP/netmask:** 10.10.10.0/24
  - **RemoteIP/netmask:** 192.168.10.0/24
  - Click ***Return*** and ***OK***.

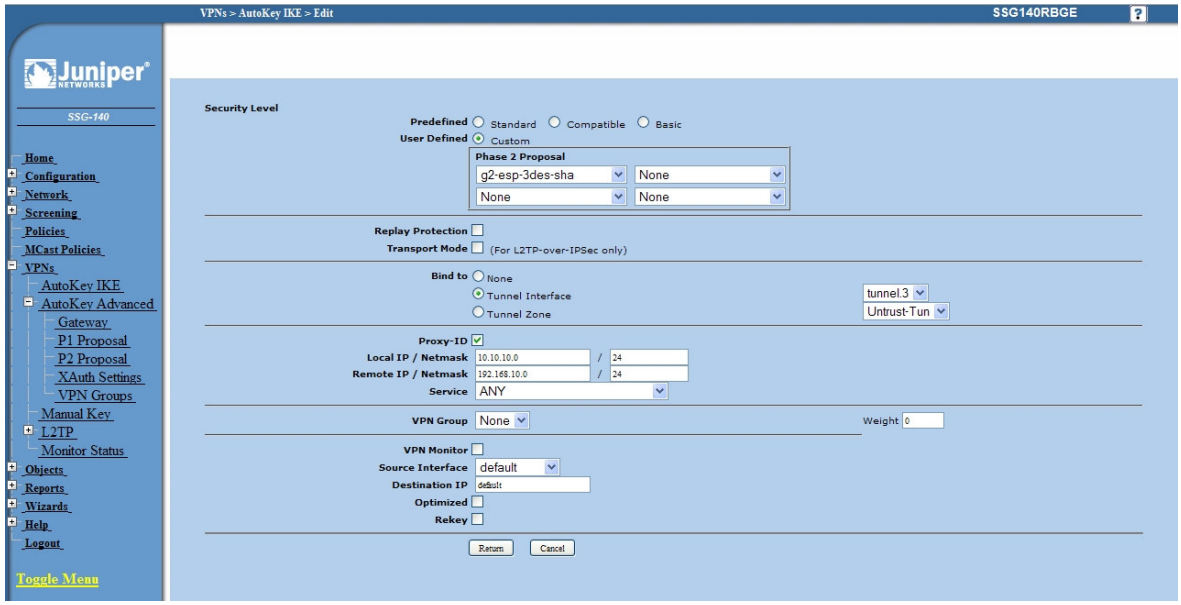


Figure 103 - AutoKey IKE advanced parameters

Step 4 - Routing

- Click ***Destination*** tab on ***Routing*** menu.
- Click **New** button. Routing parameters are:
  - **IP Address:** 192.168.10.0/24
  - **Gateway:** tunnel.3(tunnel interface from step 1)
  - Click ***OK.***

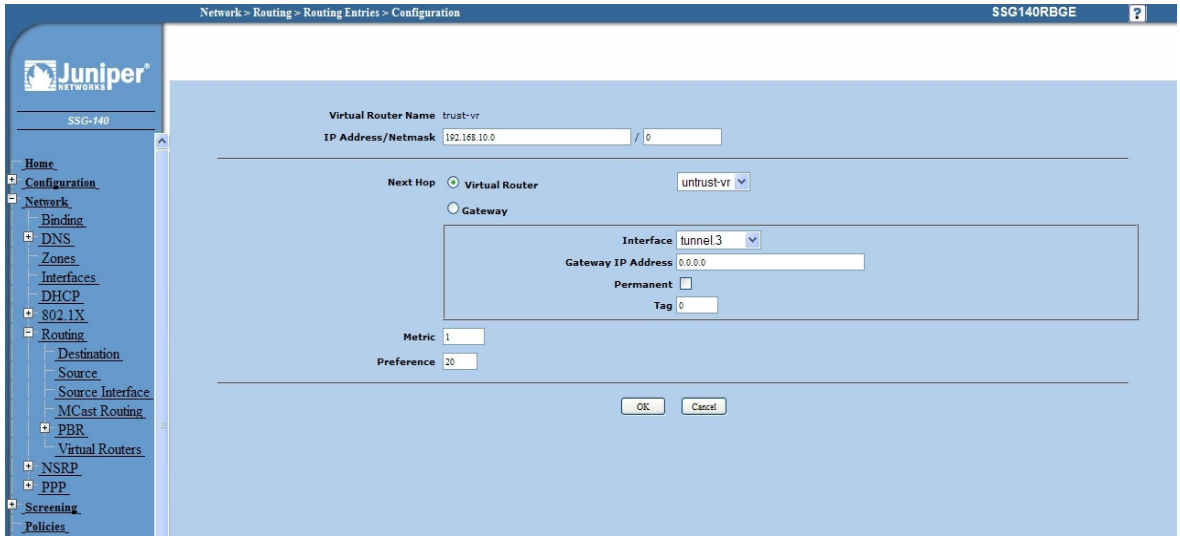


Figure 104 - Routing parameters

Step 5 - Policies

- Click ***Policies*** in main menu.
- Click *New* button (from Untrust to trust zone)
  - **Source Address:** 192.168.10.0/24
  - **Destination Address:** 10.10.10.0/24
  - **Services:** Any
- Click ***OK.***

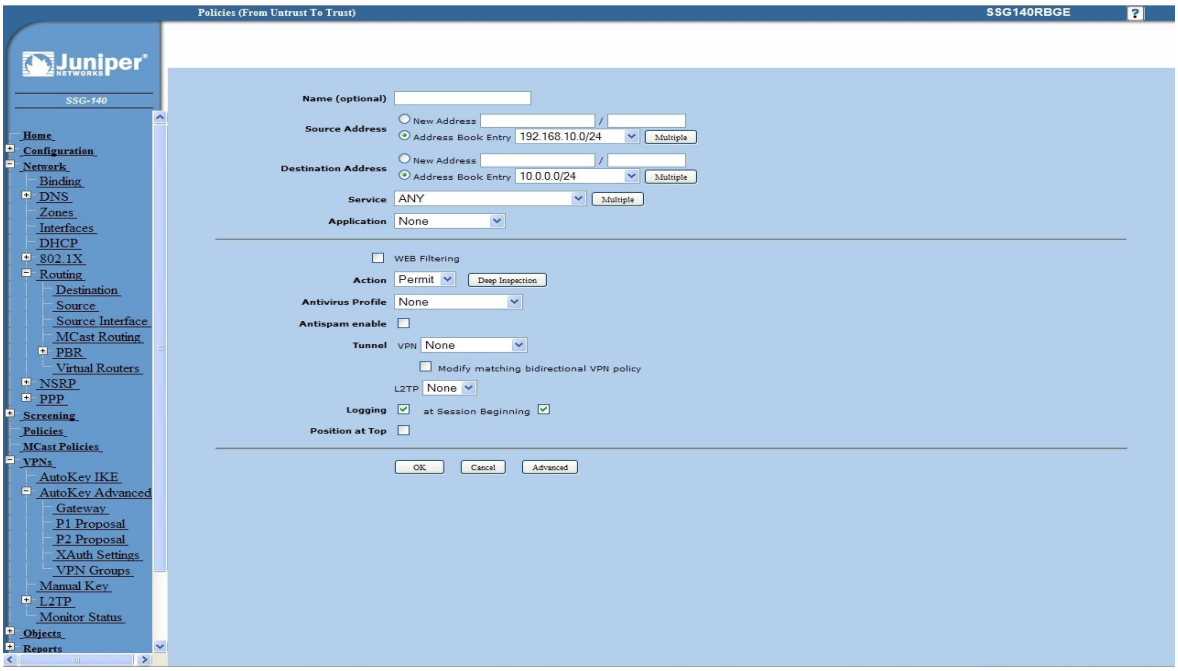


Figure 105 - Policies from untrust to trust zone

- Click ***Policies*** in main menu.
- Click *New* button (from trust to untrust zone)
  - **Source Address:** 10.10.10.0/24
  - **Destination Address:** 192.168.10.0/24
  - **Services:** Any
- Click ***OK.***

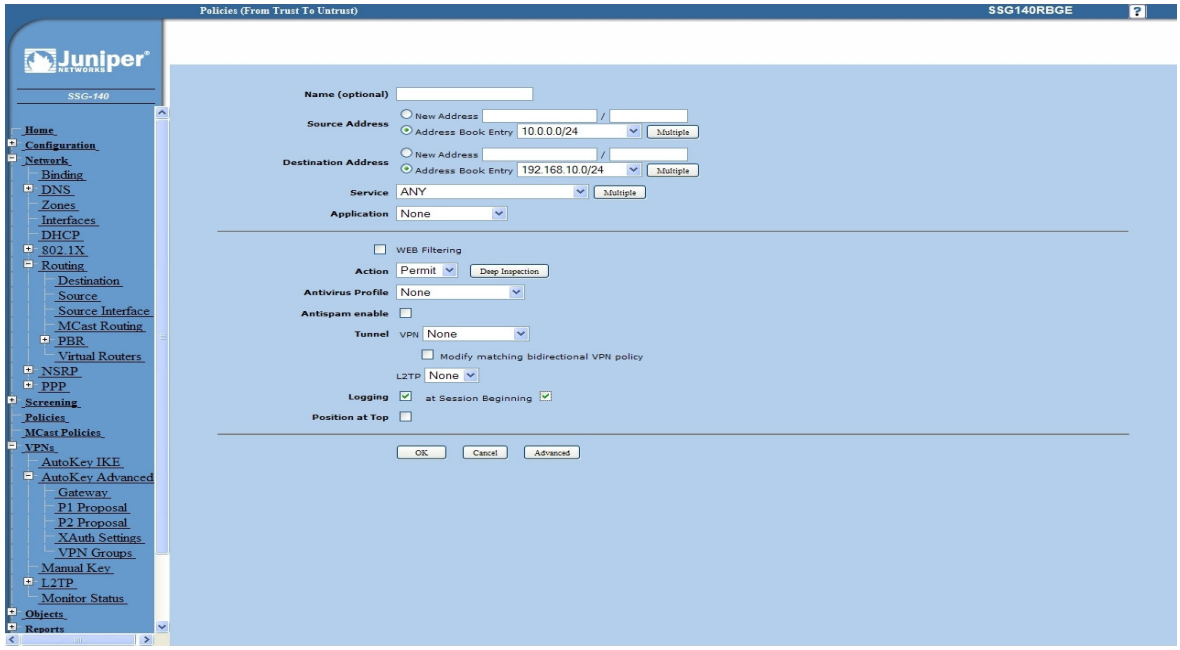


Figure 106 - Policies from trust to untrust zone

Apendix

A. How to Achieve Maximum Signal Strength with GWR-I Router?

The best throughput comes from placing the device in an area with the greatest Received Signal Strength Indicator (RSSI). RSSI is a measurement of the Radio Frequency (RF) signal strength between the base station and the mobile device, expressed in dBm. The better the signal strength, the less data retransmission and, therefore, better throughput.

RSSI information is available from several sources:

- The LEDs on the device give a general indication.
- Via the GWR-I Router local user interface.

Signal strength LED indicator:

- -101 or less dBm = Unacceptable (running LED)
- -100 to -91 dBm = Weak (1 LED)
- -90 to -81 dBm = Moderate (2 LED)
- -80 to -75 dBm = Good (3 LED)
- -74 or better dBm = Excellent (4 LED)
- 0 is not known or not detectable (running LED).

Antenna placement

Placement can drastically increase the signal strength of a cellular connection. Often times, just moving the router closer to an exterior window or to another location within the facility can result in optimum reception.

Another way of increasing throughput is by physically placing the device on the roof of the building (in an environmentally safe enclosure with proper moisture and lightning protection).

- Simply install the GWR-I Router outside the building and run an RJ-45 Ethernet cable to your switch located in the building.
- Keep antenna cable away from interferers (AC wiring).

Antenna Options

Once optimum placement is achieved, if signal strength is still not desirable, you can experiment with different antenna options. Assuming you have tried a standard antenna, next consider:

- Check your antenna connection to ensure it is properly attached.
- High gain antenna, which has higher dBm gain and longer antenna. Many cabled antennas require a metal ground plane for maximum performance. The ground plane typically should have a diameter roughly twice the length of the antenna.

NOTE: Another way of optimizing throughput is by sending non-encrypted data through the device. Application layer encryption or VPN put a heavy toll on bandwidth utilization. For example, IPsec ESP headers and trailers can add 20-30% or more overhead.