geneko

GWR

USER MANUAL

GWR High Speed Cellular Router Series

Document version: 1.0.3
Date: November 2016

Document History

Date	Description	Author	Comments
24.12.2015	User Manual, version 1.0.0	Tanja Savić	Firmware versions: 1.1.2
01.04.2016	User Manual, version 1.0.1	Tanja Savić	Firmware versions: 1.3.0
19.09.2016	User Manual, version 1.0.2	Tanja Savić	Firmware versions: 2.0.0
04.11.2016	User Manual, version 1.0.2	Tanja Savić	Firmware versions: 2.0.0

Document Approval

The following report has been accepted and approved by the following:

Signature	Printed Name	Title	Date
	Dragan Marković	Executive Director	24.12.2015
	Dragan Marković	Executive Director	01.04.2016
	Dragan Marković	Executive Director	19.09.2016
	Dragan Marković	Executive Director	04.11.2016

Trademark

Contents

DOCUMENT APPROVAL 2
TRADEMARK 2
LIST OF FIGURES 5
LIST OF TABLES 8
DESCRIPTION OF THE GWR HIGH SPEED CELLULAR ROUTER SERIES 9
PRODUCTS 10
TYPICAL APPLICATION 11
TECHNICAL PARAMETERS 12
PROTOCOLS AND FEATURES 16
PRODUCT OVERVIEW 20
Front panel 20
Back panel 20
Top Panel 21
PUTTING INTO OPERATION 22
DEVICE CONFIGURATION 22
QUICK START 22
INSERTING SIM CARDS 22
CONNECTING ROUTER 23
ADMINISTRATION WEB PAGE 23
QUICK SETUP 24
TURN LOGGING ON 24
DEVICE CONFIGURATION USING WEB APPLICATION 25
ADD/REMOVE/UPDATE MANIPULATION IN TABLES 25
SAVE/RELOAD CHANGES 25
STATUS INFORMATION 26
Status – General 26
Status – LAN Port Information 27
Status – DHCP 27
Status- WAN Information* 28
Status- ADSL Information 28
Status – Mobile Information 29
Status – Wireless Information 30
Status – Firewall 30
Status –Router Monitoring 31
SETTINGS –WAN PORT* 32
SETTINGS – LAN PORTS 33
SETTINGS – DHCP SERVER 34
SETTINGS – MOBILE SETTINGS 36
SETTINGS-ADSL PORT 41
SETTINGS – WIRELESS SETTINGS 42
SETTINGS – VLANS 43
SETTINGS – ROUTING 43
Gateway Priorities 45
Port forwarding 46
Settings – Demilitarized Zone (DMZ) 47
SETTINGS – VRRP SETTINGS 50
SETTINGS – VPN SETTINGS 51
Generic Routing Encapsulation (GRE) 51

Internet Protocol Security (IPSec) 53
OpenVPN 58
SETTINGS – PPTP 63
SETTINGS – L2TP 64
FILE MANAGEMENT 66
CA Certificate 66
Private Certificate 67
Private Key 68
CRL Certificate 68
Preshared Key Files 69
SETTINGS – FIREWALL – IP FILTERING 70
SETTINGS – FIREWALL – MAC FILTERING 72
SETTINGS – DYNAMIC DNS 72
SETTINGS – SERIAL PORT 1 74
Serial port over TCP/UDP settings 75
Modbus Gateway settings 77
SMS – SMS REMOTE CONTROL 79
SMS – SEND SMS 80
Maintenance 80
Maintenance – System Control 81
Maintenance – Device Identity Settings 81
Maintenance – Authentication 81
Maintenance – Date/Time Settings 83
Maintenance – Diagnostics 84
Maintenance – Update Firmware 84
Maintenance – Import/Export Settings 85
Import Configuration File *85*
Export Configuration File *85*
Maintenance – Default Settings 86
Maintenance – System Reboot 86
MANAGEMENT – DISPLAY SETTINGS 86
MANAGEMENT – TIMED ACTIONS 87
MANAGEMENT – COMMAND LINE INTERFACE 87
MANAGEMENT – REMOTE MANAGEMENT 88
MANAGEMENT – CONNECTION MANAGER 89
Getting started with the Connection Wizard 89
MANAGEMENT – SIMPLE MANAGEMENT PROTOCOL (SNMP) 92
Management – Logs 94
LOGOUT 95
CHROOT 95

CONFIGURATION EXAMPLES 97

GWR ROUTER AS INTERNET ROUTER 97
GRE TUNNEL CONFIGURATION BETWEEN TWO GWR ROUTERS 98
GRE TUNNEL CONFIGURATION BETWEEN GWR ROUTER AND THIRD PARTY ROUTER 102
IPSEC TUNNEL CONFIGURATION BETWEEN TWO GWR ROUTERS 105
#Example 106
IPSEC TUNNEL CONFIGURATION BETWEEN GWR ROUTER AND CISCO ROUTER 114
IPSEC TUNNEL CONFIGURATION BETWEEN GWR ROUTER AND JUNIPER SSG FIREWALL 119
OPENVPN TUNNEL BETWEEN GWR ROUTER AND OPENVNP SERVER 129
PORT FORWARDING EXAMPLE 132
SERIAL PORT – EXAMPLE 134
FIREWALL – EXAMPLE 137
SMS MANAGEMENT – EXAMPLE 145
DEFINING KEEPALIVE FUNCTIONALITY 146

Display 148

APPENDIX 150

Antenna placement 150
Antenna Options 150
KNOWN ISSUES 150

List of Figures

Figure 1 – GWR High Speed Cellular Router Series 9
Figure 2 – GWR Router front panel 20
Figure 3 – GWR Router back panel 20
Figure 4 – GWR Router top panel 21
Figure 5 – Inserting SIM card 23
Figure 6 – User authentication 25
Figure 7 – General router information 26
Figure 8 – LAN Port Information 27
Figure 9 – DHCP Information 27
Figure 10 – WAN Port Information 28
Figure 11 – ADSL Port Information 29
Figure 12 – Mobile Information 29
Figure 13 – Wireless Information 30
Figure 14 – Firewall Information 30
Figure 15 – Router monitoring #1 31
Figure 16 – Router monitoring #2 32
Figure 17 – WAN Ports 32
Figure 18 – LAN Port configuration page 34
Figure 19 – DHCP Server configuration page 36
Figure 20 – Mobile Settings configuration page 36
Figure 21 – ADSL Port Settings 41
Figure 22 – Wireless Settings configuration page 42
Figure 23 – Virtual LAN 43
Figure 24 – Routing configuration page 44
Figure 25 – Gateway priorities 46
Figure 26 – DMZ configuration page 47
Figure 27 – RIP configuration page 48
Figure 28 – Virtual Router Redundancy Protocol 50
Figure 29 – GRE tunnel parameters configuration page 52
Figure 30 – IPSec Summary screen 53
Figure 31 – IPSec Settings 55
Figure 32 – OpenVPN 59
Figure 33 – OpenVPN example 1 59
Figure 34 – OpenVPN Summary screen 60
Figure 35 – PPTP configuration page 63
Figure 36 – PPTP Summary screen 64
Figure 37 – L2TP configuration page 64
Figure 38 – L2TP Summary screen 65
Figure 39 – CA Certificate 66
Figure 40 – Private Certificate 67
Figure 41 – Private Key 68
Figure 42 – CRL Certificate 69
Figure 43 – Preshared Key files management 70

Figure 44 – Firewall configuration page....71
Figure 45 – MAC filtering configuration page....72
Figure 46 – DynDNS settings....73
Figure 47 – Serial Port Settings initial menu....74
Figure 48 – Serial Port configuration page....76
Figure 49 – Modbus gateway configuration page....78
Figure 50 – SMS remote control configuration....80
Figure 51– Send SMS....80
Figure 52 – System control....81
Figure 53 – Device Identity Settings configuration page....81
Figure 54 – Router Management configuration page....82
Figure 55 – Date/Time Settings configuration page....83
Figure 56 – Diagnostic page....84
Figure 57 – Update Firmware page....84
Figure 58 – Export/Import the configuration on the router....85
Figure 59 – Default Settings page....86
Figure 60 – System Reboot page....86
Figure 61 – Display Settings....86
Figure 62 – Timed actions....87
Figure 63 – Command Line Interface....88
Figure 64 – Remote Management....89
Figure 65 – Connection Manager....89
Figure 66 – Connection Wizard – Initial Step....90
Figure 67 – Connection Wizard – Router Detection....91
Figure 68 – Connection Wizard – LAN Settings....91
Figure 69 – Connection Wizard – WAN Settings....92
Figure 70 – SNMP configuration page....93
Figure 71 – SNMP get command....93
Figure 72 – SNMP set command....94
Figure 73 – Syslog configuration page....94
Figure 74 – GWR Router as Internet router....97
Figure 75 – GRE tunnel between two GWR Routers....98
Figure 76 – Network configuration page for GWR Router 1....99
Figure 77 – GRE configuration page for GWR Router 1....99
Figure 78 – Routing configuration page for GWR Router 1....100
Figure 79 – Network configuration page for GWR Router 2....100
Figure 80 – GRE configuration page for GWR Router 2....101
Figure 81 – Routing configuration page for GWR Router 2....101
Figure 82 – GRE tunnel between Cisco router and GWR Router....102
Figure 83 – LAN Port configuration page....103
Figure 84 – GRE configuration page....104
Figure 85 – Routing configuration page....104
Figure 86 – IPSec tunnel between two GWR Routers....105
Figure 87 – LAN Port configuration page for GWR Router 1....106
Figure 88 – IPSEC configuration page I for GWR Router 1....108
Figure 89 – IPSec configuration page II for GWR Router 1....108
Figure 90 – IPSec configuration page III for GWR Router 1....109
Figure 91 – IPSec start/stop page for GWR Router 1....109
Figure 92 – Network configuration page for GWR Router 2....110
Figure 93 – IPSEC configuration page I for GWR Router 2....111
Figure 94 – IPSec configuration page II for GWR Router 2....112
Figure 95 – IPSec configuration page III for GWR Router 2....112
Figure 96 – IPSec start/stop page for GWR Router 2....113
Figure 97 – IPSec tunnel between GWR Router and Cisco Router....114

Figure 98 – LAN Port configuration page for GWR Router 115
Figure 99 – IPSEC configuration page I for GWR Router 116
Figure 100 – IPSec configuration page II for GWR Router 116
Figure 101 – IPSec configuration page III for GWR Router 116
Figure 102 – IPSec start/stop page for GWR Router 117
Figure 103 – IPSec tunnel between GWR Router and Juniper SSG firewall 119
Figure 104 – Network configuration page for GWR Router 120
Figure 105 – IPSec configuration page I for GWR Router 121
Figure 106 – IPSec configuration page II for GWR Router 121
Figure 107 – IPSec configuration page III for GWR Router 121
Figure 108 – IPSec start/stop page for GWR Router 122
Figure 109 – Network Interfaces (list) 123
Figure 110 – Network Interfaces (edit) 123
Figure 111 – AutoKey Advanced Gateway 124
Figure 112 – Gateway parameters 124
Figure 113 – Gateway advanced parameters 125
Figure 114 – AutoKey IKE 125
Figure 115 – AutoKey IKE parameters 126
Figure 116 – AutoKey IKE advanced parameters 126
Figure 117 – Routing parameters 127
Figure 118 – Policies from untrust to trust zone 128
Figure 119 – Policies from trust to untrust zone 128
Figure 120 – Multipoint OpenVPN topology 129
Figure 121 – OpenVPN application settings 130
Figure 122 – OpenVPN GWR settings 131
Figure 123 – Static routes on GWR 132
Figure 124 – Starting OpenVPN application 132
Figure 125 – OpenVPN status on PC 132
Figure 126 – OpenVPN status on GWR 132
Figure 127 – Portforwarding example 133
Figure 128 – GWR port forwarding configuration 133
Figure 129 – Transparent serial connection 134
Figure 130 – GWR Serial port settings 134
Figure 131 – GWR settings for Serial-to-IP conversion 135
Figure 132 – Virtual COM port application 136
Figure 133 – Settings for virtual COM port 136
Figure 134 – Firewall example 138
Figure 135 – Initial firewall configuration on GWR 139
Figure 136 – Filtering of Telnet traffic 139
Figure 137 – Filtering of ICMP traffic 140
Figure 138 – Allowing ICMP traffic 141
Figure 139 – IPSec firewall rules 141
Figure 140 – Allowing WEB access 142
Figure 141 – Outbound rule for WEB access 144
Figure 142 – Complete firewall configuration 145
Figure 143 – Configuration page for SMS management 145
Figure 144 – Configuration page for GSM keepalive 147
Figure 145 – Graphic display 148
Figure 146 – Display 149

List of Tables

Table 1- Legend tag the router's name....10
Table 2 – Technical parameters....15
Table 3 – GWR Router software features....19
Table 4 – WAN parameters....33
Table 5 – LAN parameters....34
Table 6 – DHCP Server parameters....35
Table 7 – Mobile settings parameters....38
Table 8 – Mobile settings (advanced settings) parameters....40
Table 9 – ADSL parameters....41
Table 10 – Wireless parameters....42
Table 11 – VLANs parameters....43
Table 12 – Routing parameters....44
Table 13 – Gateway priorities....45
Table 14 – Port forwarding settings....47
Table 15 – Demilitarized Zone....47
Table 16 – RIP parameters....48
Table 17 – VRRP Parameters....50
Table 18 – GRE parameters....52
Table 19 – IPSec Summary....54
Table 20 – IPSec Parameters....58
Table 21 – OpenVPN parameters....62
Table 22 – PPTP parameters....63
Table 23 – L2TP parameters....65
Table 24 – CA Certificate....66
Table 25 – Private Certificate....67
Table 26 – Private Key....68
Table 27 – CRL Certificate....69
Table 28 – Preshared Key Files....69
Table 29 – Firewall parameters....71
Table 30 – MAC filtering parameters....72
Table 31 – DynDNS parameters....73
Table 32 – Serial port 1 parameters....74
Table 33 – Serial Port over TCP/UDP parameters....76
Table 34 – Modbus gateway parameters....77
Table 35 – Device Identity parameters....81
Table 36 – Router Management....83
Table 37 – Date/time parameters....84
Table 38 – Date/time parameters....87
Table 39 – Command Line Interface parameters....88
Table 40 – Remote Management parameters....89
Table 40 – SNMP parameters....93
Table 42 – Syslog parameters....95

Description of the GWR High Speed Cellular Router Series

GWR routers represent a robust solution designed to provide remote connectivity across cellular networks. Low transmission delay and very high data rates offered by existing cellular networks completely eliminate the need for expensive wired infrastructure. GWR series brings scalability of even most demanding corporate networks on highest possible level. Installing a reliable, high performance backup solution for existing land lines or satellite networks is now a simple task thanks to modern cellular networks. Therefore, no matter if the goal is to provide primary internet access or backup solution for already existing network GWR router series represents a top rated solution.

Figure 1 – GWR High Speed Cellular Router Series

There are practically no limits when it comes to possible application of GWR routers. Wired infrastructure is no longer necessary for building scalable and high performance systems. GWR routers will reduce the costs and speed up the ROI process for each one of possible applications..

Products

The list of most common GWR High Speed Cellular Router Series products is presented bellow.

Devices by model:

GWR-A462-4W-C, GWR-A462-4W-S, GWR-A362-4W-H, GWR-A462-4-C, GWR-A462-4-S, GWR-A362-4-H, GWR-A462-W-C, GWR-A462-W-S, GWR-A362-W-H, GWR-A462-S, GWR-A362-H, GWR462-2W-C, GWR462-2W-S, GWR362-2W-H, GWR462-2-C, GWR462-2-S, GWR362-2-H, GWR462-5W-C, GWR462-5W-S, GWR362-5W-H, GWR462-5-C, GWR462-5-S, GWR362-5-H, GWR-A462-C, GWR462-5-H, GWR462-5W-H, GWR-A462-W-H, GWR-A462-4W-H, GWR-A462-4-H, GWR462-2W-H, GWR462-2-H

	HSPA+	LTE	ADSL2+	RS-232	Eth ports	Wi-Fi
GWR362-2-X	·	–	–	·	2	Optional
GWR362-5-X	·	–	–	·	5	Optional
GWR-A362-X	·	–	·	·	1	Optional
GWR-A362-4-X	·	–	·	·	4	Optional
GWR462-2-X	·	·	–	·	2	Optional
GWR462-5-X	·	·	–	·	5	Optional
GWR-A462-X	·	·	·	·	1	Optional
GWR-A462-4-X	·	·	·	·	4	Optional

Table 1- Legend tag the router's name

-X at the end of Part Number denotes GSM module. Following manufacturers are available:

- S - Sierra Wireless
- C – Cinterion (Gemalto)
- H – Huawei

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

Wireless Interfaces – WWAN Sierra Wireless MC7710 or MC7304 (available on 4G models)	
LTE	DD800/900/1800/2100/2600 MHz Transfer rate (max): 100 Mbps down, 50 Mbps up
UMTS/HSPA+/DC-HSPA+	900/2100MHz Transfer rate (max): 21.1 Mbps down, 5.76 Mbps up
GSM/GPRS/EDGE	900/1800/1900 MHz Transfer rate (max): 236.8 Kbps down, 236.8 Kbps up
Connector	2 x 50 Ω SMA (Center pin: female)
SIM Slots	2 x Push-Push
Wireless Interfaces – WWAN Huawei ME909u-521 (available on 4G models)	
LTE	800/850/900/1800/1900/2100/2600 MHz Transfer rate (max): 100 Mbps down, 50 Mbps up
UMTS/HSPA+/DC-HSPA+	850/900/1900/2100 MHz Transfer rate (max): 42 Mbps down, 5.76 Mbps up
GSM/GPRS/EDGE	850/900/1800/1900 MHz Transfer rate (max): 236.8 Kbps down, 236.8 Kbps up
Connector	2 x 50 Ω SMA (Center pin: female)
SIM Slots	2 x Push-Push
Wireless Interfaces – WWAN Huawei MU609 (available on 3G models)	
UMTS/HSPA+	850/900/1900/2100 MHz Transfer rate (max): 14.4 Mbps down, 5.76 Mbps up
GSM/GPRS/EDGE	850/900/1800/1900 MHz Transfer rate (max): 236.8 Kbps down, 236.8 Kbps up
Connector	2 x 50 Ω SMA (Center pin: female)
SIM Slots	2 x Push-Push
Wireless Interfaces – Wi-Fi (available on Wi-Fi models)	
Standard	802.11b/g/n

Modes	Access point, Client
Transmit Power	18.1 dBm max
Receive Sensitivity	54 Mbps / -75.7 dBm and 11 Mbps / -88.7 dBm
Security	64/128/256-bit WEP, TKIP or AES keys; WPA and WPA2
Connector	1 x 50 Ω RP-SMA (Center pin: male)
Wired Interfaces – DSL (available on ADSL models)	
Technology	ADSL2+ Annex A (ADSL over POTS) or Annex B (ADSL over ISDN)
Standards	ANSI T1.413 Issue 2, ITU-T G.992.1 (G.dmt), ITU-T G.992.2 (G.lite), ITU-T G.992.3 (G.dmt.bis/ADSL2), ITU-T G.992.5 (ADSL2plus)
Connector	RJ-11 6P2C
Wired Interfaces – Ethernet	
Ports	1, 2, or 5, depending on a model
Standard/Physical Layer	IEEE 802.3; 10/100 Base-T
Data Rate/Mode/Interface	10/100 Mbit/s; Full or Half duplex; Auto MDI/MDIX
Connector	RJ-45
Wired Interfaces – RS232	
Ports	1
Standard	RS-232
DTE/DCE	DCE
Signal Support	TXD, RXD, RTS, CTS
Flow Control	Software XON/XOFF, Hardware CTS/RTS
Connector	RJ-45
Wired Interfaces – USB	
Ports	1 Host
Standard	USB 2.0
Signaling	High Speed
Connector	Type A
User Interface	

LCD view port	67 mm x 39 mm (W x H)
LCD viewing angle	6 o'clock
LCD background color	Black
LCD segment colors	White, green, red, yellow
LCD information	Present SIM's, active SIM, GSM provider, SMS available, roaming, signal strength, GSM technology, interfaces, uptime, IP addresses, firmware version
LCD navigation	One button used to select interface for which IP is displayed
Device reset	One reset button, also used for reset-to-factory-settings
LED's	Link/Activity LED's on Ethernet connectors
Power	
Input	12 VDC, 2A
Consumption	tbd
Connector	Barrel connector
DC Power Cord	Barrel connector to bare wire
AC Power Supply	100-240 VAC 50/60 Hz; Option of standard temperature or extended temperature
Physical	
Dimensions (L x W x H)	160 mm x 100 mm x 31.5 mm (L x W x H)
Weight	up to 0.6 kg depending on a model
Material	Plastic coated 0.8 mm steel sheet
Mounting	Desktop, DIN rail sold separately
Environmental	
Operating Temperature	-20° C to +70° C
Storage Temperature	-40° C to +85° C
Relative Humidity	5% to 95% (non-condensing)
IP rating	IP30
Ethernet Isolation	1.5 kV RMS
Serial Port Protection (ESD)	15 kV

Approvals	
Safety	EN 60950-1:2006 + A1:2010 + A2:2013 + A11:2009 + A12:2011
EMC	EN 301 489-1 V1.9.2, EN 301 489-7 V1.3.1, EN 301 489-17 V2.1.1, EN 301 489-24 V1.5.1
Radio Spectrum	EN 301 511 v9.0.2, EN 301 908-2 v5.2.1, EN 301 908-13 v5.2.1, EN 300 328 v1.8.1

Table 2 – Technical parameters

Protocols and features

Features	*Short description*
Ethernet	
WAN	• Static • DHCP • PPPOe
LAN	• Static • DHCP Client • Alias IP address
DHCP Server: • **Static lease reservation** • **Address exclusions**	DHCP Server support.
WiFi	Geneko router provides possibility for using wireless Internet connection. • Access point • Client
VLANs	VLAN support (802.1Q)
Network	
Routing	Static
RIP	The Routing Information Protocol provides great network stability, guarantying that if one network connection goes down the network can quickly adapt to send packets through another connection.
Gateway priorities	The Gateway priorities is used to manage handling of the default gateway interface (Mobile, Wireless, WAN/DSL) . Only one interface can be the default gateway at one moment of time, for specific routing one can use the static routes. User can handle default gateway priorities using metrics in interface settings web pages.
VRRP	VRRP is a protocol which elects a master server on a LAN and the master answers to a 'virtual IP address'. If it fails, a backup server takes over the IP address. Interfaces which VRRP can be set: WAN/DSL, LAN, Mobile
Port forwarding, NAT	IP, TCP, UDP packets from WAN/DSL, LAN, Mobile, Wireless, to destination IP address.
DMZ support	Demilitarized Zone (DMZ) allows one local IP Address to be exposed to the Internet. Some applications require multiple TCP/UDP/IP ports to be open, DMZ provides this function by forwarding all the ports to one computer at the same time. There is the option of choosing the incoming and outgoing interface: LAN, WAN/DSL, Wireless, Mobile.
SNMP	SNMP (*Simple Network Management Protocol*) is a network protocol that provides network administrators with the ability to monitor the status of the Geneko 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 (Mobile, LAN, WAN/DSL, Wireless) and supports a custom MIB for generating trap messages.
NTP(RFC1305)	The Network Time Protocol is a protocol for synchronizing the clocks of router.
DynDNS	Client for various dynamic DNS services. Interfaces on which DynDNS works: Mobile, WAN/DSL, Wireless.
ADSL	Geneko router provides connecting to high speed ADSL line, configuring ADSL line parameters.
Firewall: • **IP filtering** • **MAC filtering**	IP address / Network filtering
Serial over TCP/UDP	Serial to Ethernet converter
Modbus serial/IP gateway	Translation between Modbus/TCP and Modbus/RTU.
VPN	
GRE	GRE is a tunneling protocol which is used to transport packets from one network to another by opening a tunnel. There is possibility for choose IP, Host or Interface (Mobile, LAN, WAN/ADSL, Wireless) for establishing GRE tunnel.
GRE keepalive	• Keepalive for GRE tunnels, • Cisco compliant.
GRE – max. number of tunnels	15
IPSec pass-through	ESP tunnels.
IPsec	IPsec (*Internet Protocol Security*) is a protocol suite for securing IP communication.
Key Exchange Mode	• IKE with Preshared key • IKE with Preshared key file • IKE with X509 certificates and PSK • IKE with X509 certificates and PSK file
Data integrity	• HMAC-MD5, SHA-1, • Authentication and key management.
Encryption	• 3DES, AES (128/192/256), BLOWFISH(128/192/256)
IPSec IKE failover	Defines number of failed IKE negotiation attempts before failover.
IPSec tunnel failover	Switches to another provider when tunnel performance is bad or one provider is unavailable.
IPSec – max. number of tunnels	15
OpenVPN	OpenVPN is a full-featured SSL VPN solution for securing communications via the Internet. Implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol.
OpenVPN – max. number of tunnels	15
PPTP	PPTP client
PPTP – max. number of tunnels	5
L2TP	The Geneko Router can be used as a L2TP peer. L2TP is suitable for Layer-2 tunneling.
L2TP – max. number of tunnels	5

Certificate management	Certificate management is used to manage certificate files so they can be used for peer authentication. • **CA Certificate** • **Private Certificate** • **Private Key** • **Preshared Key Files** **CRL Certificate** is used to manage Certificate Revocation List certificate files so they can be used for validating certificates.
GSM/UMTS/LTE features	
2G/3G/4G	Support with dual SIM capability.
Dual SIM support	For operator backup.
SIM PIN locking	Enable locking of SIM card with PIN code.
Roaming protection	By enabling this option router will be able to connect to roaming network.
Reset Location information	By enabling this option router will erase LOCI Elementary File in SIM card. This will cause SIM card to scan all available networks when registering.
Authentication	PAP, CHAP, PAP-CHAP
SIM keepalive	Make some traffic periodically in order to maintain connection alive.
SIM Priority	SIM1, SIM2
Reboot after failed connections	Reboot gateway after 'n' consecutive failed connection attempts.
Persistent connection	Keep connection alive, try to reopen the connection if it is broken.
Management	
User-friendly WEB GUI	HTTP based.
CLI: • **SSH** • **telnet** • **serial**	Remote management over SSH. Remote management over Telnet. Custom AT scripting to modem
Timed Actions	Create a schedule of actions to be performed in a certain time of the day. There is a possibility to add more actions for each day of the week.
Traffic and event log	Log tracing.
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.
Remote Management	Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of Geneko Routers. In order for it to work, it must be enabled on the router and installed on a Windows computer. It is a Geneko TM application.

Update Firmware	• Over WEB interface • Over CLI
Maintenance	
Diagnostics	Ping utility. It is possible to choose interface (LAN, Mobile, WAN, Wireless) and type (IP address or hostname).
Authentication	Used for activating and deactivating device access system through Username and Password mechanism. It is possible to activate or deactivate function for authentication via remote radius server.
Date/Time Settings	Current Date and Time Date and Time Setup: • Manually • Automatically
Device Identity Settings	There is an option to define name, location of device and description of device function. These data are kept in device permanent memory.
Import/Export settings	Import or Export of configuration (Possibility of selecting type of configuration to export).
Factory default settings	External taster and configuration application.
Customization Options	
Chroot environment	Support for shell scripts, LUA, Python. Perl and compiled C/C++ executables. Allowed access to device peripherals from user space.

Table 3 – GWR Router software features

Product Overview

Front panel

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

- One or four RJ45 connector(s) – Ethernet port for connection into local computer network
- One RJ45 connector for RS232 serial communication (ADSL or WAN)
- Power supply connector

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.

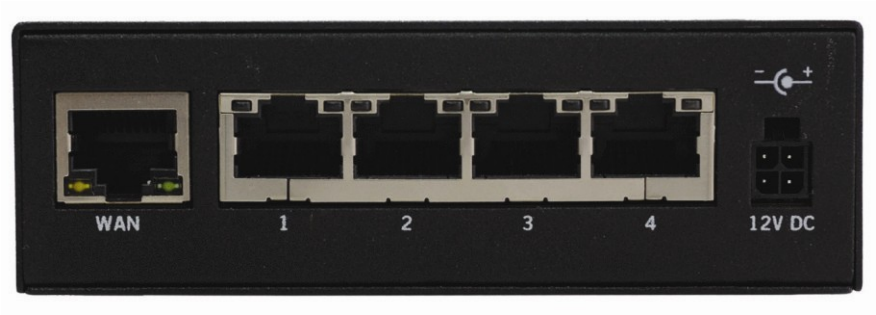


Figure 2 – GWR Router front panel

Back panel

On the back panel of device (*Figure 3*) the following connectors are located:

- Slot for SIM cards (SIM1 and SIM2)
- SMA connector for connection of the GSM/UMTS/LTE antennas (main, WI-FI, AUX)
- Reset button,
- One USB connector,
- one RJ45 connector for RS232 serial communication
- Display button

Figure 3 – GWR Router back panel

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

Warm reset: If the GWR 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 Router, hold the RESET button pressed for a few seconds. Restoration of the default configuration will be signaled by writing messages on the display and changing network status. This will restore the factory defaults and clear all custom settings of the GWR Router. You can also reset the GWR Router to factory defaults using the Maintenance > Default Settings screen.

Top Panel

Figure 4 – GWR Router top panel

On the GWR Router top panel is display, where we can read off Present SIM's, active SIM, GSM provider, SMS available, roaming, signal strength, GSM technology, interfaces, uptime, IP addresses, firmware version.

Putting Into Operation

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

- GSM/UMTS/LTE antenna,
- Ethernet cable and
- SIM card must be inserted.

And finally, device should have powered up using power supply adapter.
Power consumption of GWR router is 2W in standby and 3W in burst mode.

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

Device Configuration

There are two methods which can be used to configure the GWR 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 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 Router but still represents a very powerful tool when it comes to router setup and monitoring. Another document deals with CLI commands and instructions.

Quick start

INSERTING SIM CARDS

Warning: do not insert or eject SIM cards while router is powered on. Make sure to disconnect router from AC/DC adapter before inserting or ejecting SIM cards.

* Put the SIM CARD 1 in SIM CARD 1 HOLDER.
*When you want to remove SIM CARD from the SIM CARD HOLDER, press SIM CARD first to get out from the HOLDER, then you can get it.
* Repeat these steps for second SIM, if needed.

Figure 5 – Inserting SIM card

CONNECTING ROUTER

Warning: Use only the router's box power supply.

* Connect antennas to router. Make sure to tighten antennas so that they are not loose.
* Plug AC/DC adapter cable into POWER CONNECTOR on your router.
* Plug AC/DC adapter into wall power socket.
* Display will turn on.
* Wait approximately 43-45 seconds for router to become fully operational.
* Plug one side of ETHERNET CABLE to ETHERNET CONNECTOR on a router.
* Plug other side of ETHERNET CABLE to Ethernet port on your computer.
*You will see on the screen if SIM card is present, cellular network types, signal level, current firmware version (or IP address), uptime, number of LAN ports.

ADMINISTRATION WEB PAGE

* Add network 192.168.1.0/24 to the interface on your PC
* Optional: Ping 192.168.1.1 to check is the GWR router reachable
* Open your Web browser (e.g. Firefox, Chrome, Safari, Opera, or Internet Explorer) and open following address: http://192.168.1.1
* When prompted for your login credentials, use "admin" (without quotes) for both username and password.
* After logging in you should be able to see administration web page, which allows you to easily setup the router.

QUICK SETUP

* Once logged in to administration web page, click on SETTINGS ->MOBILE SETTINGS link from the menu on the left side of the screen.
* If SIM card is present, ENABLED check box will be checked. Otherwise, you need to insert SIM card as explained in "Inserting SIM cards" chapter.
* Your GSM operator should provide you with PROVIDER, USERNAME (optional), PASSWORD (optional), APN and PIN (optional) information. Make sure you enter this into corresponding fields, and then click on SAVE button.
* After a few minutes when your GWR router is connected, connection status will be accomplished.
* Click on SETTINGS -> ETHERNET SETTINGS ->LAN PORTS link from the menu on the left side of the screen
* Set IP Address and Subnet Mask and click on SAVE button
* Add a new network to the interface on your PC
* Ping new IP address
* When the GWR router is accessible, insert new IP address in a Web browser
* Click on MAINTENANCE » DATE/TIME SETTINGS link from the menu on the left side of the screen.
* Click on SYNC CLOCK button. GWR Router will sync DATE and TIME fields with your computer's current date and time. Now click on SAVE button.

TURN LOGGING ON

When troubleshooting router make sure logs are turned on.
You should send logs to Geneko when submitting support request.

* Click on MANAGEMENT -> LOGS link from the menu on the left side of the screen.
* Click on LOCAL SYSLOG radio button, and then click on SAVE button.
* Set appropriate log size and click on SAVE button.
* Log is now available for download from router to your computer when you click on EXPORT LOG button.

Device configuration using web application

The GWR 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 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 Username 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.

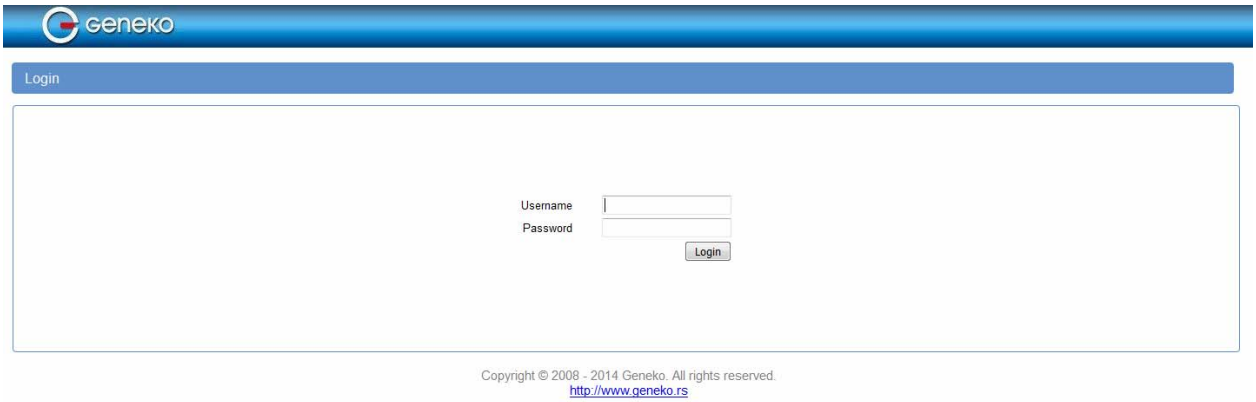


Figure 6 – User authentication

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

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

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 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
- Lan Port Information
- DHCP
- WAN Information* or ADSL Information
- Mobile
- Wireless
- Firewall
- Routes
- Router Monitoring

* functionality at GWR462-5-S, GWR462-5-H, GWR462-5W-S, GWR462-5W-H, GWR462-2-S, GWR462-2-H, GWR462-2W-S, GWR362-5-H, GWR362-5W-H, GWR362-2-H, GWR362-2W-H, GWR462-2W-C,GWR462-2-C, GWR462-5W-C, GWR462-5-C, GWR462-2W-H

Status – General

General Information Tab provides general information about device type, device firmware version, kernel version, CPU vendor, Uptime since last reboot, hardware resources utilization and MAC address of LAN port. Screenshot of General Router information is shown at *Figure 7*. 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.

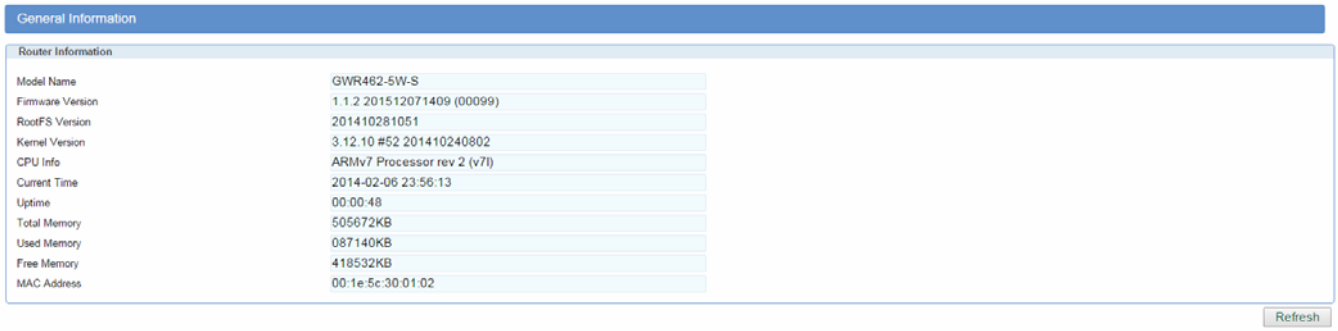


Figure 7 – General router information

Status – LAN Port Information

Lan Port Information Tab provides information about Ethernet port and Ethernet traffic statistic. Screenshot of Lan Port Information is shown in *Figure 8*.

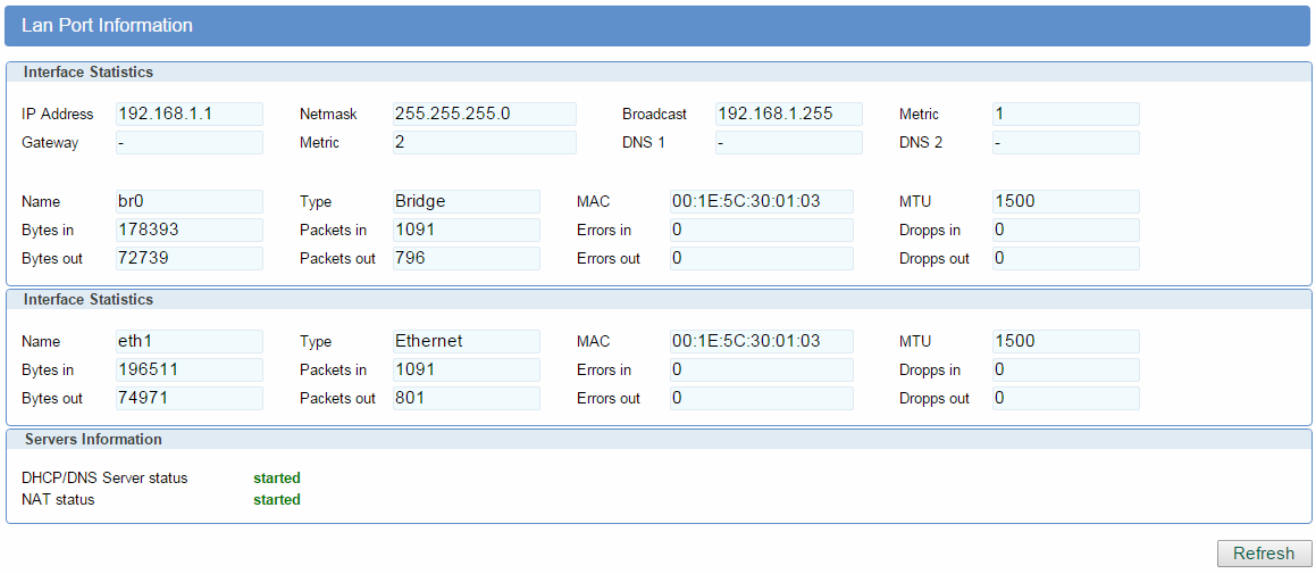


Figure 8 – LAN Port Information

Status – DHCP

DHCP Information Tab provides information about DHCP clients with IP addresses gained from DHCP server, MAC addresses, expiration period, and lease status.

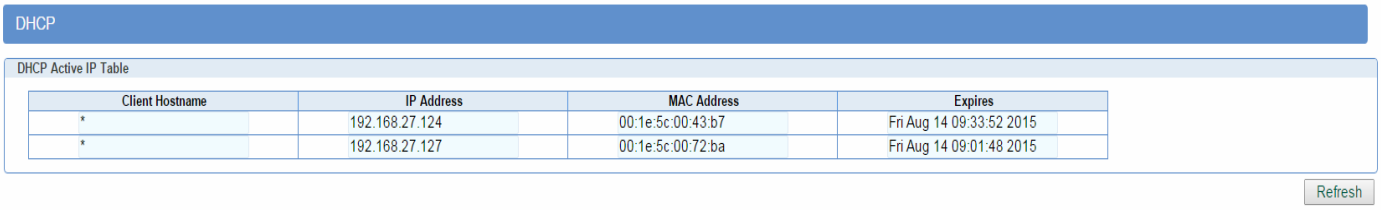


Figure 9 – DHCP Information

Status- WAN Information*

WAN Port Information Tab provides information about WAN port and WAN traffic statistics (IP address, netmask, Broadcast address, Gateway, WAN traffic statistics (in bytes) etc.).
Screenshot of WAN Port Information is shown in *Figure 10*.

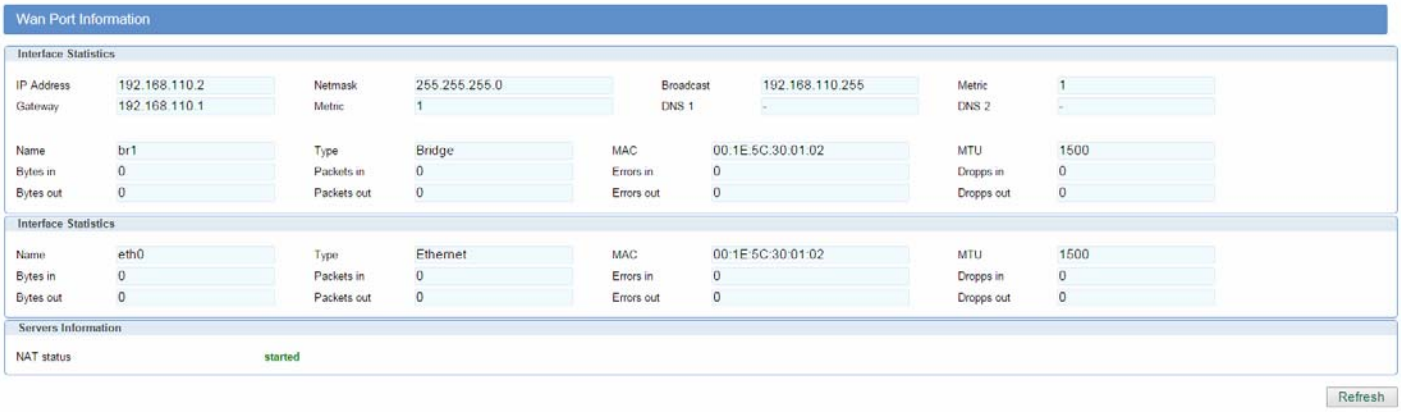
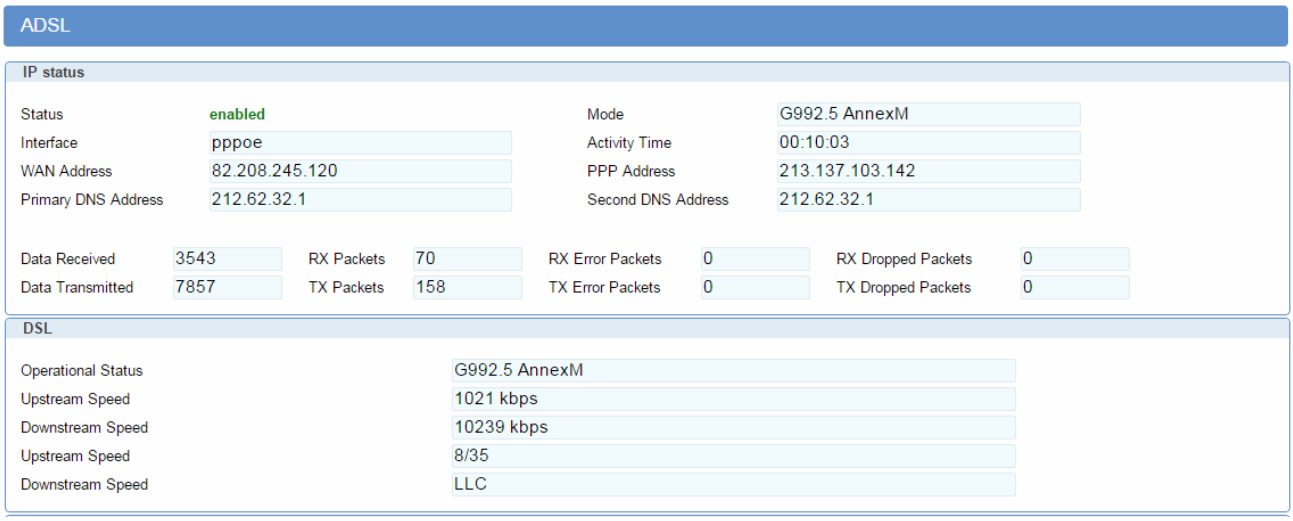
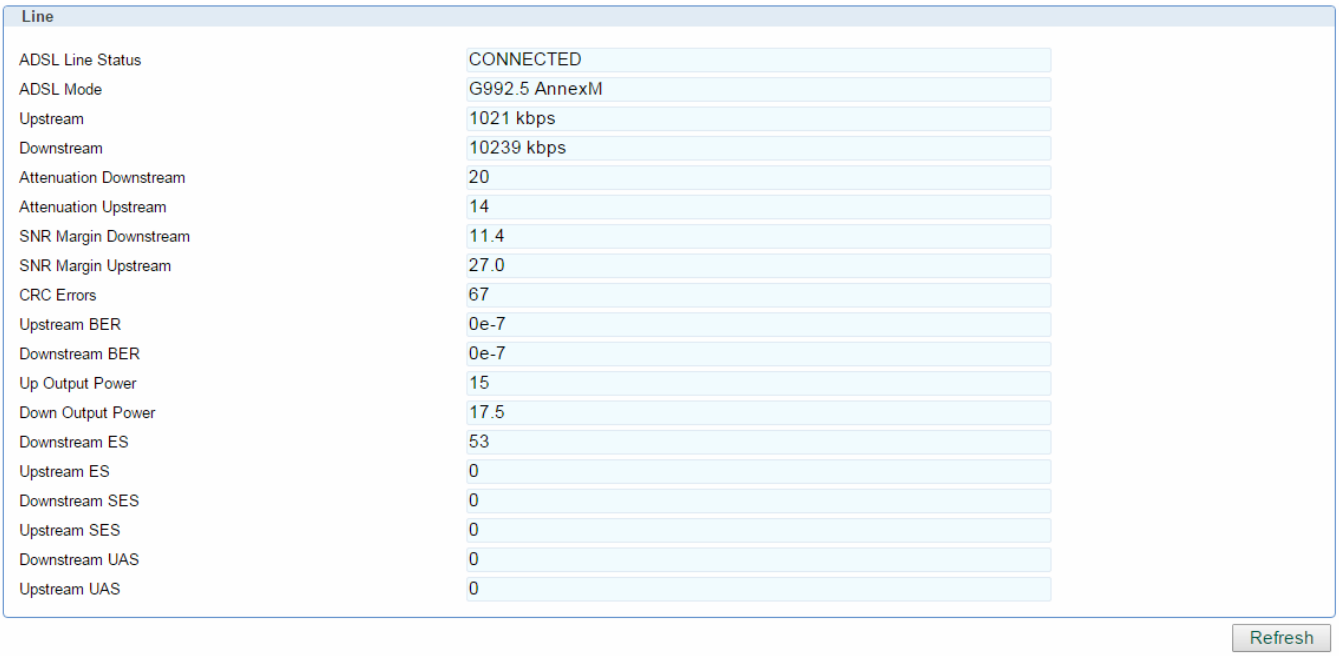


Figure 10 – WAN Port Information

Status- ADSL Information

ADSL Port Information Tab provides IP status information about interface, WAN address, primary DNS address, DSL information about upstream speed and downstream speed and Line information. Line information display ADSL line status, ADSL mode, upstream speed, downstream speed.
Screenshot of ADSL Information is shown in *Figure 11*.





Line

ADSL Line Status	CONNECTED
ADSL Mode	G992.5 AnnexM
Upstream	1021 kbps
Downstream	10239 kbps
Attenuation Downstream	20
Attenuation Upstream	14
SNR Margin Downstream	11.4
SNR Margin Upstream	27.0
CRC Errors	67
Upstream BER	0e-7
Downstream BER	0e-7
Up Output Power	15
Down Output Power	17.5
Downstream ES	53
Upstream ES	0
Downstream SES	0
Upstream SES	0
Downstream UAS	0
Upstream UAS	0

Refresh

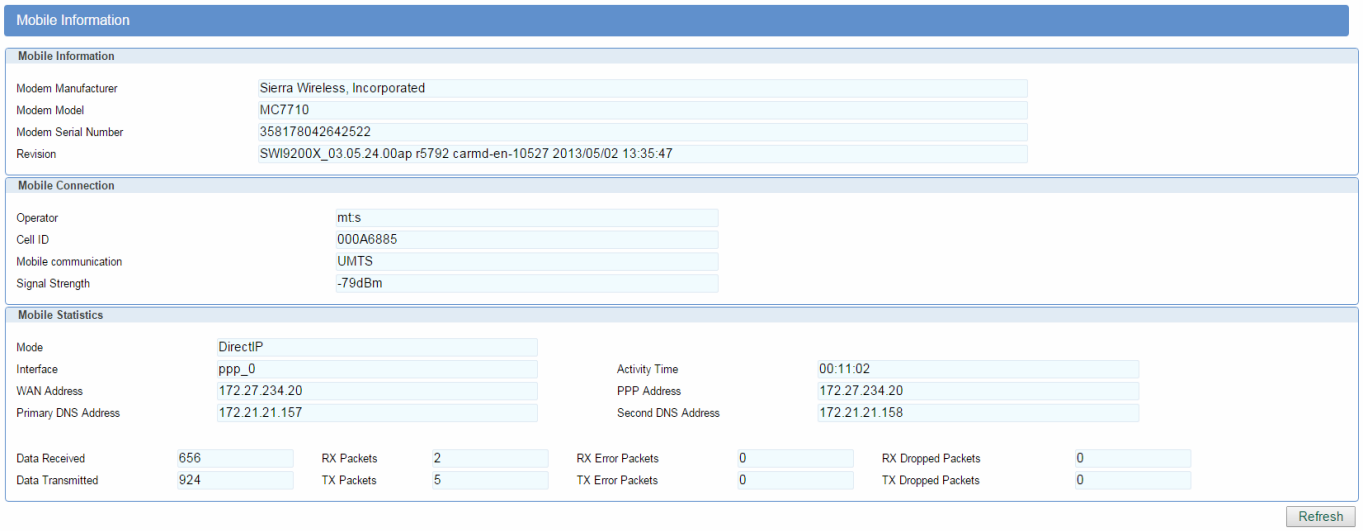
Figure 11 – ADSL Port Information

Status – Mobile Information

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

- GPRS/EDGE/HSPA/HSPA+/LTE mobile module(manufacturer and model),
- Mobile operator and signal quality,
- Mobile traffic statistics (in bytes)

Screenshot of Mobile information from the router is shown in *Figure 12*.



Mobile Information

Mobile Information

Modem Manufacturer	Sierra Wireless, Incorporated
Modem Model	MC7710
Modem Serial Number	358178042642522
Revision	SWI9200X_03.05.24.00ap r5792 carmd-en-10527 2013/05/02 13:35:47

Mobile Connection

Operator	mt:s
Cell ID	000A6885
Mobile communication	UMTS
Signal Strength	-79dBm

Mobile Statistics

Mode	DirectIP		
Interface	ppp_0	Activity Time	00:11:02
WAN Address	172.27.234.20	PPP Address	172.27.234.20
Primary DNS Address	172.21.21.157	Second DNS Address	172.21.21.158

Data Received	656	RX Packets	2	RX Error Packets	0	RX Dropped Packets	0
Data Transmitted	924	TX Packets	5	TX Error Packets	0	TX Dropped Packets	0

Refresh

Figure 12 – Mobile Information

As a primary and secondary DNS are always displayed DNS servers assigned by provider. They are

not necessarily used by the router. If Local DNS is configured it has priority to those DNS servers.

Status – Wireless Information

Wireless Information Tab provides information about Interface Statistics, traffic statistics (in bytes), MAC address, Access Point Status, DHCP/DNS Server status and NAT status. Screenshot of Wireless Information from the router is shown in *Figure 13*.

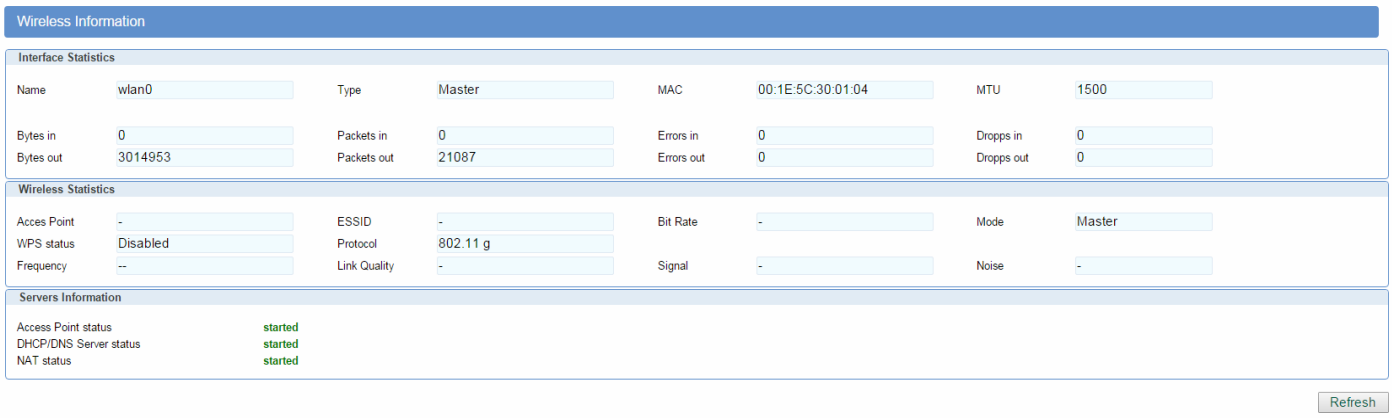


Figure 13 – Wireless Information

Status – Firewall

Firewall Information Tab provides information about active firewall rules divided in three groups: INPUT, FORWARD and OUTPUT chain. Each of these groups has packet counter which can be cleared with one of three displayed button: Reset INPUT, Reset FORWARD and Reset OUTPUT.
Screenshot of Wireless Information from the router is shown in *Figure 14*.

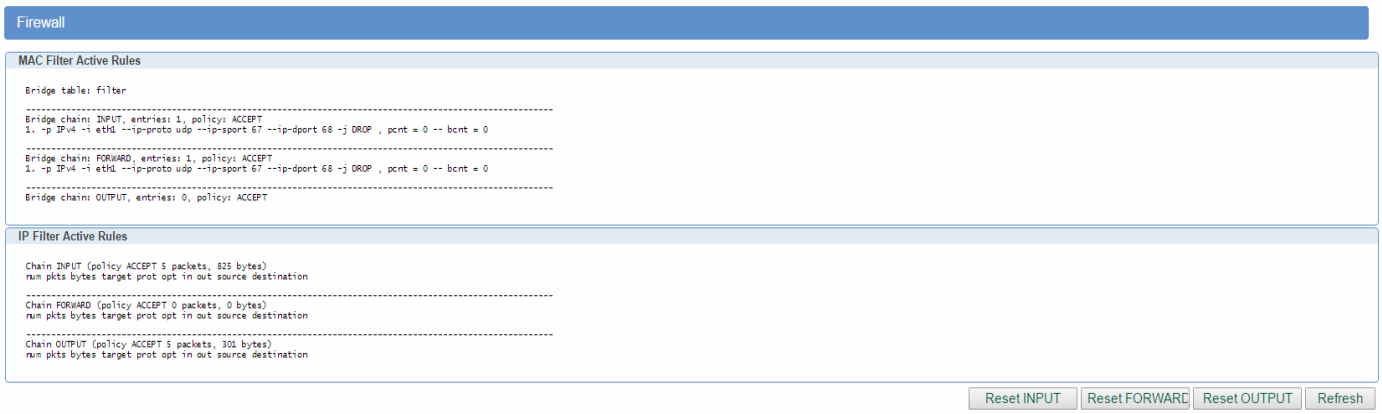
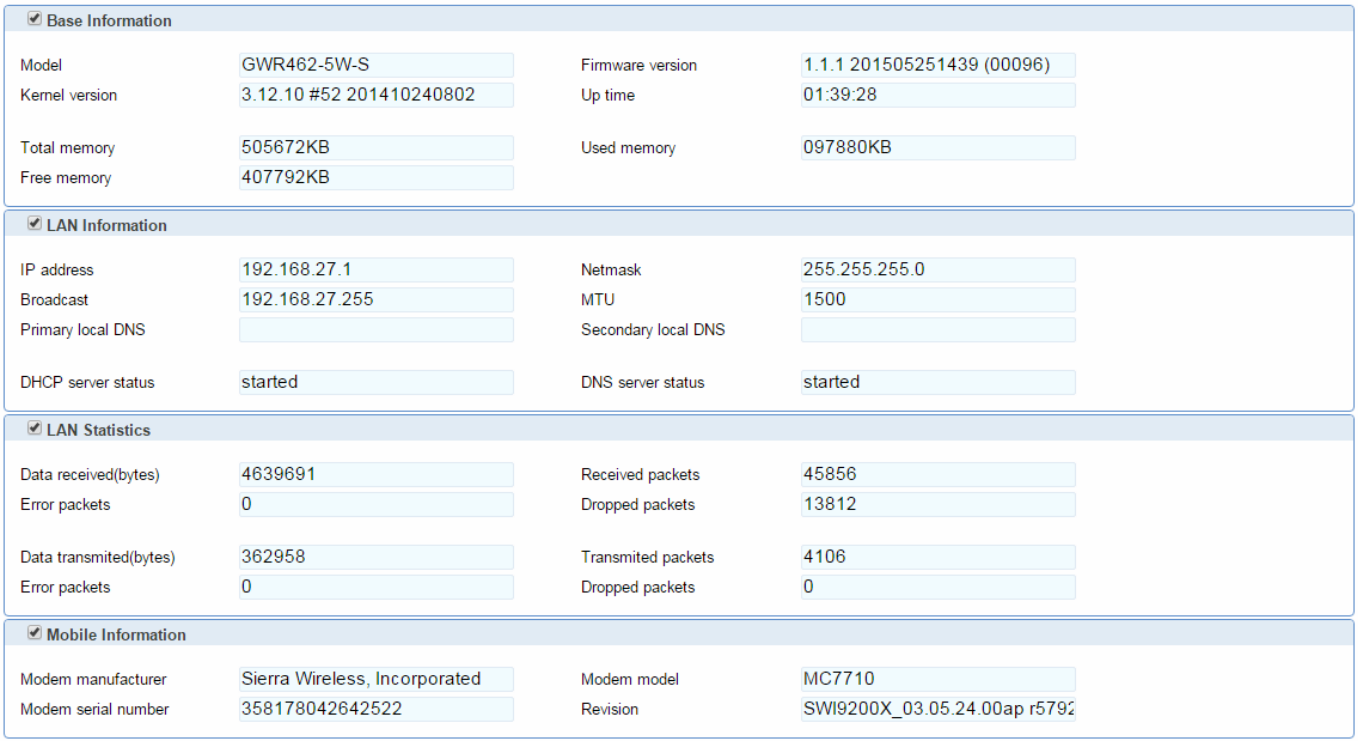


Figure 14 – Firewall Information

Status –Router Monitoring

Router Monitoring tab provides Base information, LAN and Mobile real-time information LAN, Mobile, Wireless statistics and information about Mobile Connection. You can activate Automatic refresh after 5, 10, 15, 30 or 60 seconds.



Base Information

Model	GWR462-5W-S	Firmware version	1.1.1 201505251439 (00096)
Kernel version	3.12.10 #52 201410240802	Up time	01:39:28
Total memory	505672KB	Used memory	097880KB
Free memory	407792KB		

LAN Information

IP address	192.168.27.1	Netmask	255.255.255.0
Broadcast	192.168.27.255	MTU	1500
Primary local DNS		Secondary local DNS	
DHCP server status	started	DNS server status	started

LAN Statistics

Data received(bytes)	4639691	Received packets	45856
Error packets	0	Dropped packets	13812
Data transmited(bytes)	362958	Transmited packets	4106
Error packets	0	Dropped packets	0

Mobile Information

Modem manufacturer	Sierra Wireless, Incorporated	Modem model	MC7710
Modem serial number	358178042642522	Revision	SWI9200X_03.05.24.00ap r5792

Figure 15 – Router monitoring #1

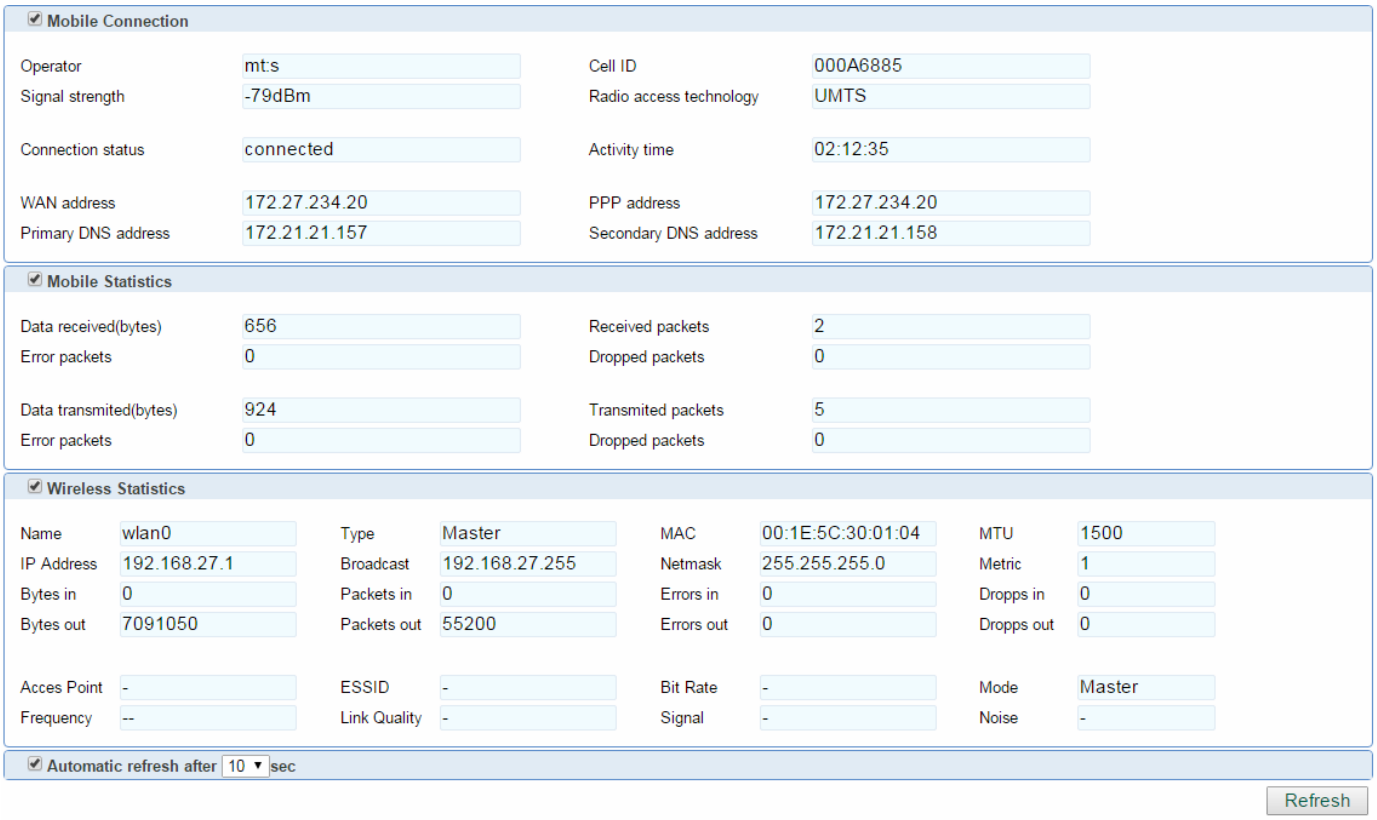


Figure 16 – Router monitoring #2

*Settings –WAN Port**

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

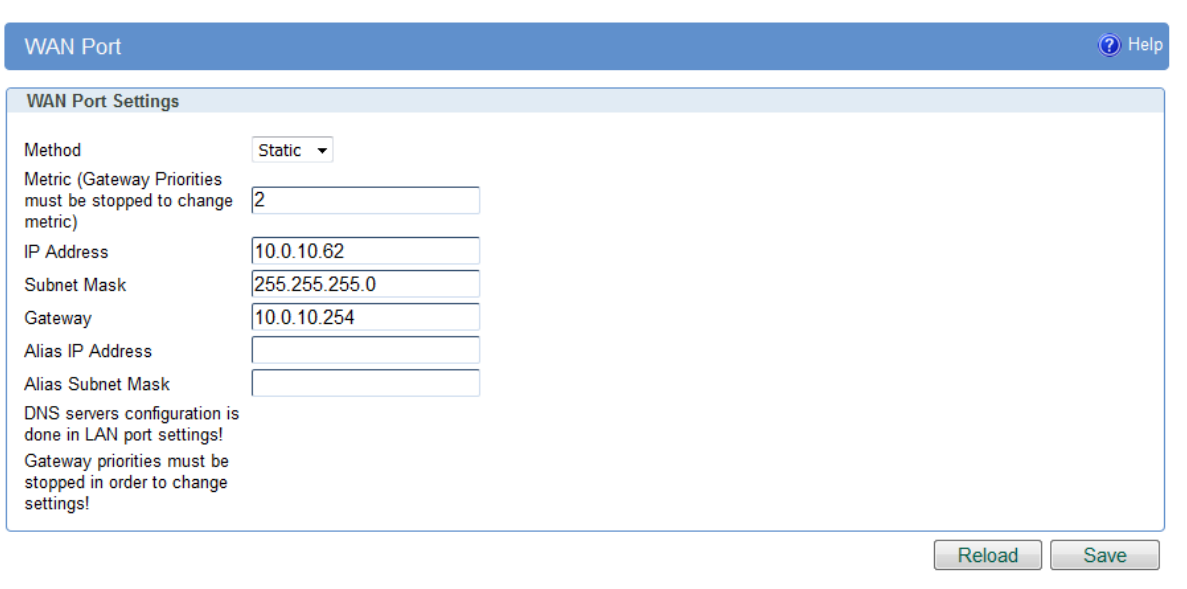


Figure 17 – WAN Ports

WAN Port Parameters	
Label	**Description**
Method	Choose Method Static, DHCP, PPoE
Metric (Gateway Priorities must be stopped to change metric)	Choose metrics to make routing decisions.
IP Address	Type the IP address of your GWR 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 Router support sub–netting. You must specified subnet mask for your LAN TCP/IP settings.
Gateway	All incoming packets are forwarded to IP address defined in this field
Alias IP Address	Secondary IP address of the interface. It, also can be used for communication on the WAN network.
Alias Subnet Mask	Secondary subnet mask of the interface.

Table 4 – WAN parameters

DNS server configuration is done in LAN port settings!

Gateway priorities must be stopped in order to change settings!

Settings – LAN Ports

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

LAN Ports Parameters	
Label	**Description**
Method	Select static or DHCP. With DHP option, the router will obtain an IP address from DHCP server on the LAN.
Metric	This field specifies value which define routing priority.
IP Address	Enter the IP address of your GWR Router in dotted decimal notation. 192.168.1.1 is the factory default IP address.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the IP address of your local gateway. Use Local Gateway option carefully. Gateway becomes unreachable from local subnet when this option is entered.
Alias IP Address	IP address of internal virtual LAN interfaces (secondary).
Alias Subnet Mask	Corresponding subnet mask for this alias.
Primary DNS	Enter the IP address of your primary local DNS server.

Secondary DNS	Enter the IP address of your secondary 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 Router. Whether you make changes or not, router will reboot every time you click ***Save***.

Table 5 – LAN parameters

In the *Figure 18* you can see screenshot of ***LAN Ports*** configuration menu.

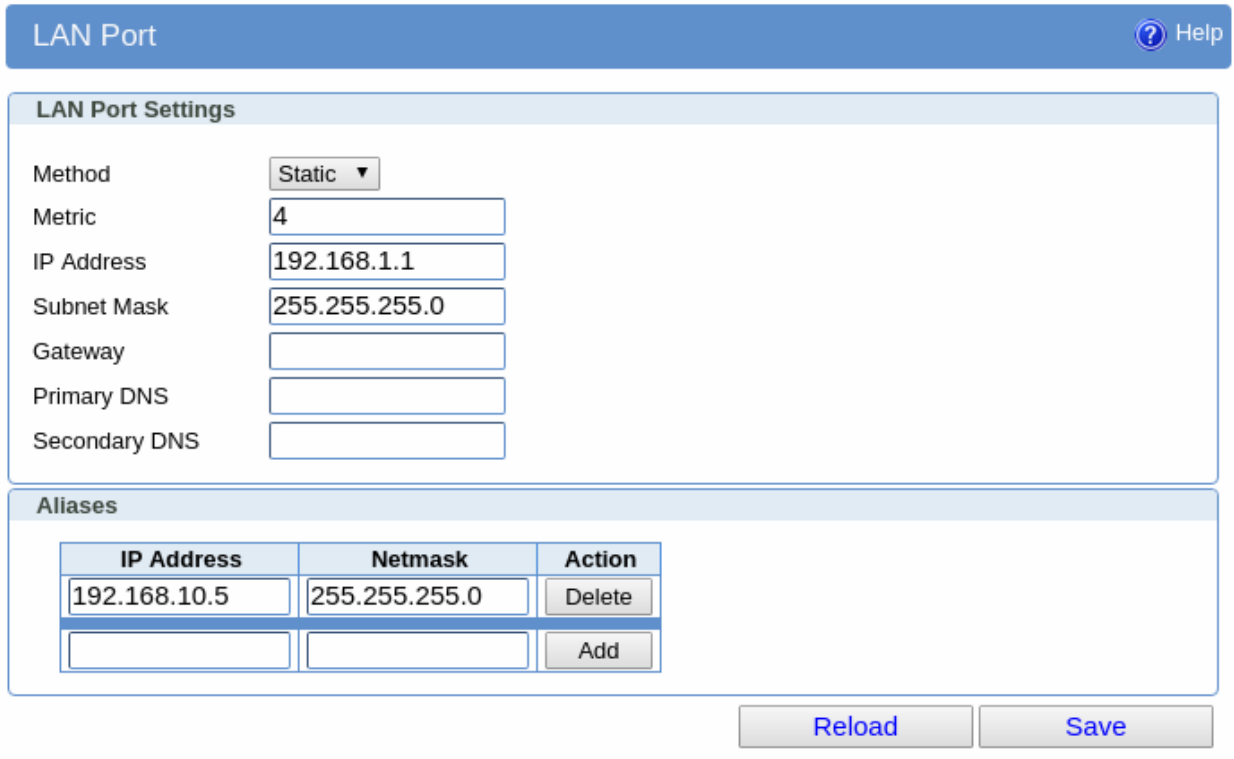


Figure 18 – LAN Port configuration page

Settings – DHCP Server

The GWR 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 Router as your network's DHCP server, click ***DHCP Server*** Tab for DHCP Server setup. The GWR 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 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 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 Address range (From)	This field specifies the IP address pool for assigning IP addresses. **Address range must be in the same network (subnet) as the router's LAN port.**
IP Address range (To)	This field specifies last of the contiguous addresses in the IP address pool.
Lease Duration	This field specifies DHCP session duration time.
Gateway	This field specifies default gateway for DHCP clients. If left blank, router will become the gateway.
Network/netmask	This field shows current network and netmask of the router (DHCP server).
Primary DNS, Secondary DNS	This field specifies IP addresses of DNS (*Domain Name System)* 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 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 ***User Defined*** to have the GWR Router assigns 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 Router.
Remove	Click ***Remove*** to delete selected item from table.
Save	Click ***Save*** to save your changes back to the GWR Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 6 – DHCP Server parameters

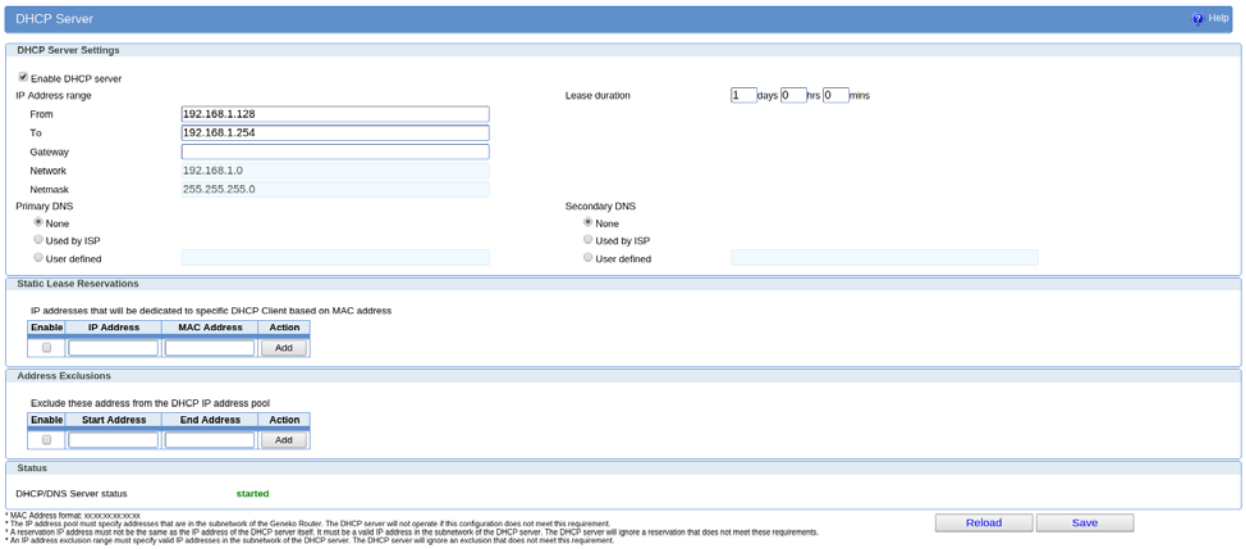


Figure 19 – DHCP Server configuration page

Settings – Mobile Settings

Click ***Mobile Settings*** Tab, to open the Mobile Settings screen. Use this screen to configure the GWR Router GPRS/EDGE/HSPA/HSPA+/LTE parameters (*Figure 20*).

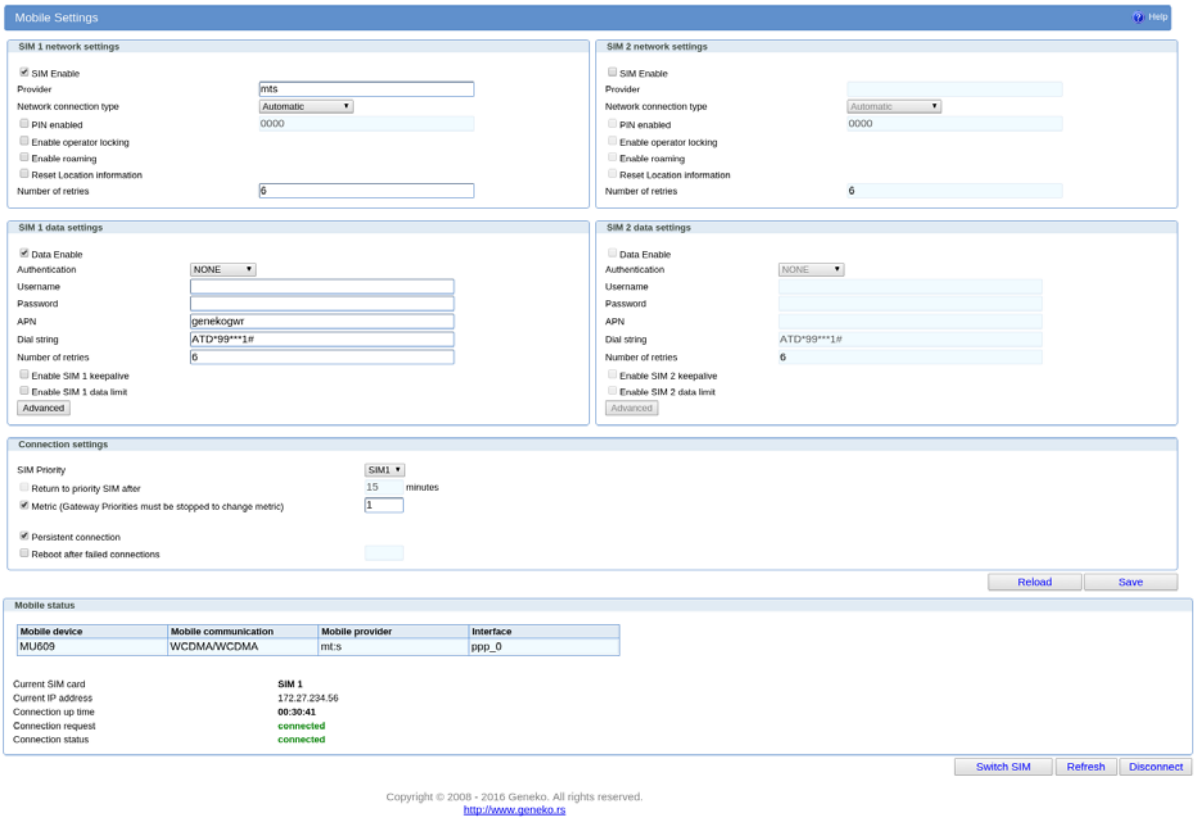


Figure 20 – Mobile Settings configuration page

Mobile Settings	
Label	**Description**
Provider	This field specifies name of GSM/UMTS/LTE ISP. You can setup any name for provider.
Network connection type	This field enables you to choose preferred network (GSM, UMTS and LTE).
PIN enabled	This field enables you to enter PIN code for SIM card if it is enabled on the SIM.
Enable operator locking	This option forces your SIM card to register to predefined PLMN only.
Enable roaming	By enabling this option gateway will be able to connect to roaming network.
Reset Location Information	By enabling this option gateway will erase LOCI Elementary File in SIM card. This will cause SIM card to scan all available networks when registering.
Number of retries	This field specifies number of attempts to establish connection.
Authentication	This field specifies password authentication protocol. From the pop up window choose appropriate protocol (PAP, CHAP, PAP-CHAP).
Username	This field specifies Username for client authentication at GSM/UMTS/LTE network. Mobile provider will assign you specific username for SIM card.
Password	This field specifies Password for client authentication at GSM/UMTS/LTE network. Mobile provider will assign you specific password for SIM card.
APN	This field specifies APN for client authentication at GSM/UMTS/LTE network. Mobile provider will assign you specific APN for SIM card.
Enable SIM keepalive	Make some traffic periodically in order to maintain connection active. You can set keepalive interval value in minutes.
Protocol	Choose which protocol to use for keepalive packets.
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 or 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	If restart PPP option is selected, gateway will restart the PPP connection.
Enable SIM data limit	Enable traffic data limit per SIM.

Traffic limit	Defines maximum data amount transferred over SIM card. When traffic limit is reached SIM card can no longer be used for network connection. Traffic limit can be defined in units of KB (from 1 to 1024), MB (from 1 to 1024) or GB (from 1 to 1024).
Action	Choose switch SIM or disconnect.
Current traffic	Displays amount of traffic that has been transferred over SIM card from the moment of enabling "SIM data limit" option. In order to refresh the displayed value in the "Current traffic" field please click on Refresh button.
Reset current traffic value	Click on Reset button resets a value of the current traffic to zero.
Reset current traffic value on specified day of the month	Every month, on the specified day, a value of the current traffic will be reset to zero. The day of reset is specified by ordinal number.
SIM Priority	Choose SIM1 or SIM2 for establishing connection.
Return to priority SIM after	Set the time to return priority for mobile connection via particular SIM card.
Default Gateway Metric	Set the metric for mobile network interface as the default gateway.
Persistent connection	Keep connection alive, try to reopen the connection if it is broken.
Reboot after failed connections	Reboot gateway after 'n' consecutive failed connection attempts.
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 Router.
Refresh	Click ***Refresh*** to see updated mobile network status.
Connect/ Disconnect	Click ***Connect/Disconnect*** to connect or disconnect from mobile network.

Table 7 – Mobile settings parameters

Figure 20 shows screenshot of GSM/UMTS/LTE tab configuration menu. GSM/UMTS/LTE menu is divided into two parts.

- Upper part provides all parameters for configuration GSM/UMTS/LTE 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/LTE connection (create/maintain/destroy GSM/UMTS/LTE connection). Status line show real–time status: connected/disconnected.

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

Mobile Settings (advanced settings)	
Label	**Description**
Switch to using serial connection	Switch to serial connection with modem device. This is an old fashioned way for establishing PPP connection using pppd application. Note: this is an old way used by old serial modems so maximum bandwidth may not be achieved.
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	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 given, pppd will log the contents of all control packets sent or received in a readable form.
Maximum Transmit Unit	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	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	Inserts the entered domain name 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.
Cancel	Click ***Cancel*** to cancel any changes.
Save	Click ***OK*** to save your changes back to the GWR Router.

Table 8 – Mobile settings (advanced settings) parameters

Settings-ADSL Port

Click ***ADSL Port*** Tab, to open the ADSL Settings screen. Use this screen to configure the username and password parameters *(Figure 21)*. Enable radio button Default route.

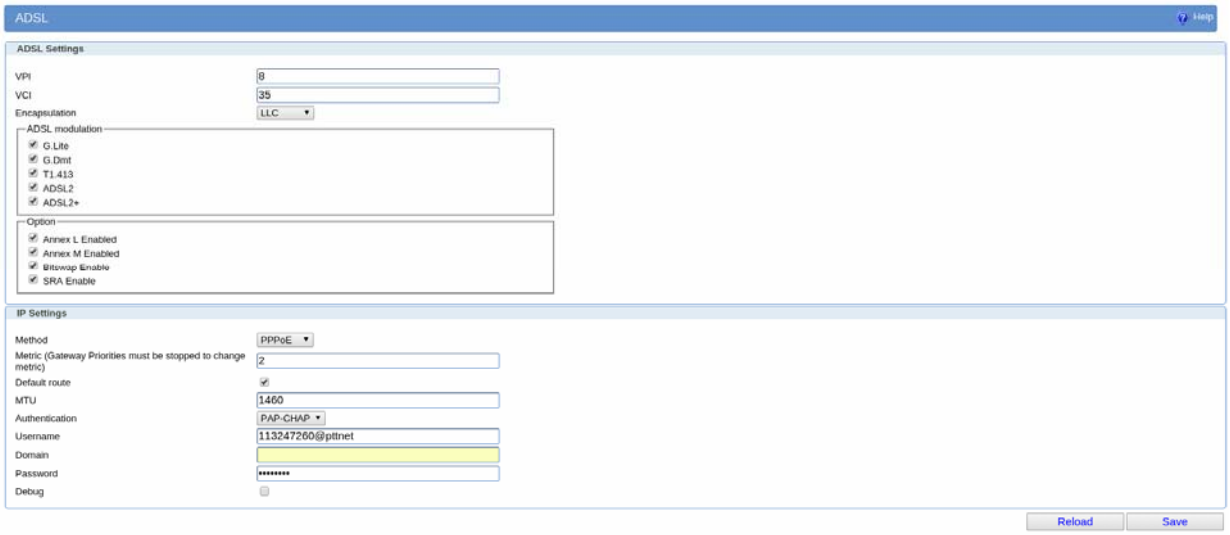


Figure 21 – ADSL Port Settings

ADSL Settings	
Label	**Description**
VPI	Enter Virtual Path Identifier provided by ISP (usually it is 8).
VCI	Enter Virtual Circuit Identifier provided by ISP (usually it is 35).
Encapsulation	Choose LLC or VC MUX encapsulation.
ADSL modulation	Check which ADSL modulations should be used.
Option	Check which options should be used.
Method	Select which method should be used.

Table 9 – ADSL parameters

Settings – Wireless Settings

Wireless settings for GWR router will give you good performance, reliability and security when using Wi-Fi.

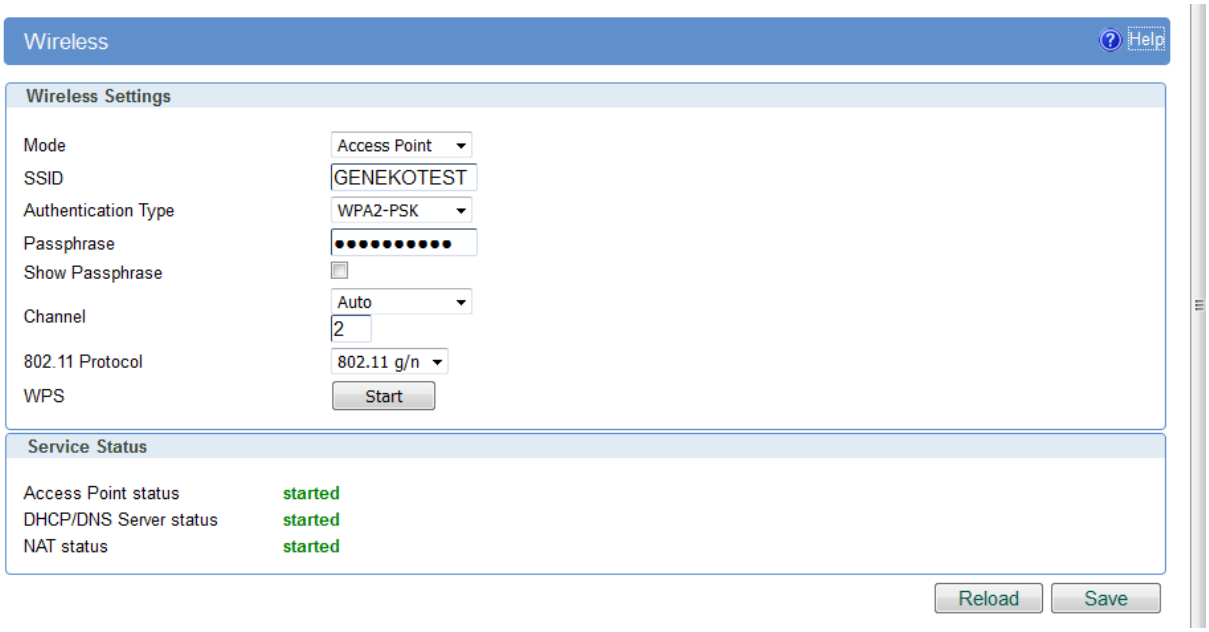


Figure 22 – Wireless Settings configuration page

Wireless Settings	
Label	**Description**
Mode	Select if you want to enable wireless Access Point or Station
SSID	SSID is a case sensitive, up to 32 alphanumeric characters length name that identifies a wireless network.
Authentication Type	Choose Wi-Fi Protected Access II Pre-shared key mode (recommended), or Open access.
Passphrase	Password for WPA2-PSK. Input from 8 to 63 printable characters.
Channel	Select one from list of legally allowed Wireless LAN channels using IEEE 802.11, or Auto for automatic channel selection.
802.11 Protocol	802.11b has a maximum raw data rate of 11 Mbit/s. 802.11bg mixed mode operates at a maximum physical layer bit rate of 54 Mbit/s, or about 22 Mbit/s average throughput. 802.11bgn mixed mode has a maximum raw data rate of 72.2 Mbit/s.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save button to save your changes back to the Geneko Router. Whether you make changes or not, router will reboot every time you click Save.

Table 10 – Wireless parameters

Settings – VLANs

VLAN is a type of local area network that does not have its own dedicated physical infrastructure, but instead uses another LAN to carry its traffic.

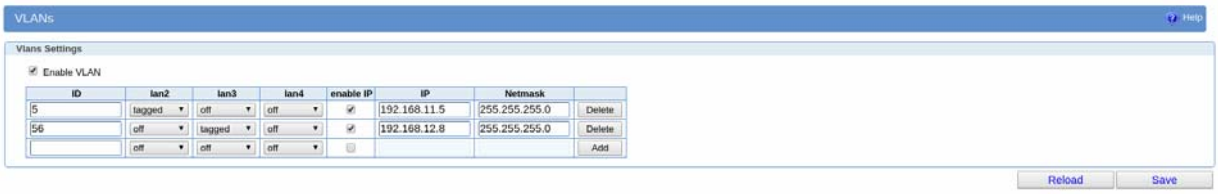


Figure 23 – Virtual LAN

Wireless Settings	
Label	**Description**
Enabled	Select this option to enable VLANs service.
ID	Enter the number of VLAN. Choose any number between 2-4096.
LAN (lan2, lan3…)	Select VLAN off, VLAN tagged or VLAN untagged. Tagged VLAN: Inserting a VLAN ID into a packet header in order to identify which VLAN the packet belongs to. Untagged VLAN: Frame cannot be tagged while travelling from one switch to another switch.
Enable IP	Select this option to enable VLANs IP address.
IP address	Enter the IP address of your VLAN in dotted decimal notation.
Subnet mask	Enter the subnet mask.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save button to save your changes back to the Geneko Router. Whether you make changes or not, router will reboot every time you click Save.

Table 11 – VLANs parameters

Settings – Routing

The static routing function determines the path that data follows over your network before and after it passes through the GWR Router. You can use static routing to allow different IP domain users to access the Internet through the GWR 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 Router to automatically adjust to physical changes in the network's layout.

The GWR Router is a fully functional router with static routing capability. *Figure 23* shows screenshot of Routing page.

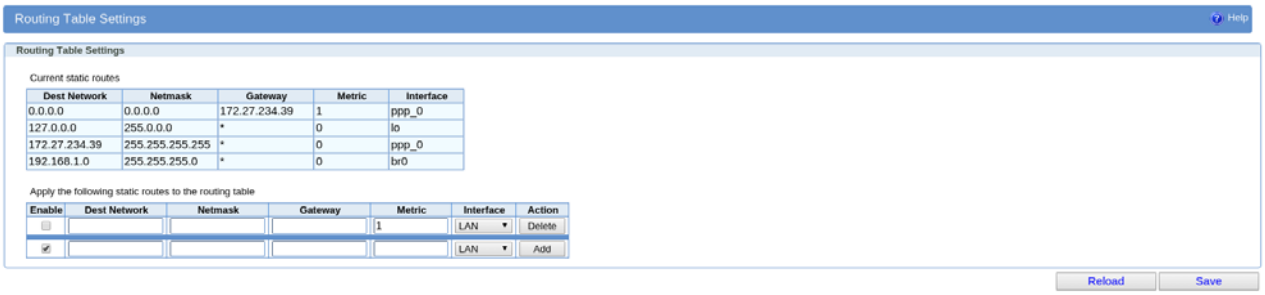


Figure 24 – Routing configuration page

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

- Create/Edit/Remove routes (including default route),
- Reroute GRE and IPSEC packet to dedicated destination at inside network.
- Port translation – Reroute TCP and UDP packets to desired destination inside the network.

Routing Settings	
Label	**Description**
Routing Table	
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 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.
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 does not need to 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 there is possibility to choose LAN, WAN, ADSL and Mobile interface.
Add	Click Add to insert (add) new item in table to the Geneko Router.
Remove	Click Remove to delete selected item from table.

Table 12 – Routing parameters

Gateway Priorities

Gateway Priorities page is used to manage handling of the default gateway interface. Only one interface can be the default gateway at one moment of time, for specific routing one can use the static routes. User can handle default gateway priorities using metrics in interface settings web pages. Be careful not to use same metric for more interfaces because it will cause problems.

For example, one can choose to use the gateways in the following order: 1. mobile 2. WAN (or DSL) 3. WIFI. If mobile works, all traffic except one handled with static routes will go through that network. When mobile doesn't work, WAN (or DSL) is the default gateway, but the router continues to check mobile network, and when it becomes available it will become the default gateway.

Router will check all connections periodically based on the options entered in the table below the list. For checking network connectivity, router uses ping mechanism. User can choose the IP address which will be used for ping, number of pings (ping count), interval in seconds between checks, percentage of successful pings which will be considered valid and packet size.

When choosing which IP address to ping, choose one which will be reachable through the specified interface. Number of pings should be greater than 1 because in networks the first ping sometimes doesn't work because of the missing ARP entry. Interval between checks is how much seconds to wait after the ping is done before pinging again. Time between checks is therefore calculated as how much time it takes for selected number of pings to finish plus interval which is entered in the table. Sometimes ping is not stable, and there are some ping losses, that is when percentage field comes in handy because one can specify the percentage of successful pings which is considered valid. Packet size is the size of data field in IP packet, and that value can be 0 and in that case, traffic which is generated is minimal.

It is very important to know that checking network reachability generates traffic which your provider may charge you!

It is easy to calculate the amount of traffic with formula ping count * (packet size + frame size) to get the amount of traffic in one test. Frame size is around 60 bytes for ping request and 42 bytes for ping reply, when data length is 0. To calculate per hour, day, month one should consider interval between checks and time for pings to complete and this varies from time to time, but in general it can be calculated. For example if one choose 5 pings every minute, with packet size set to 0, if we say that 5 pings takes 5 seconds to complete, that means that every 65 seconds 5*60 bytes will be sent and 5*42 will be received (if network is reachable). That means that in one hour around 13 Kb will be sent and 12.6 Kb will be received (if all pings are successful).

Routing Settings	
Label	**Description**
Routing Table	
Connection	Name of the network connection (network interface card).
IP address	IP address which will be used for pings on that network.
Ping count	Number of pings which will be sent.
Check interval	Interval in seconds for waiting before pinging again.
Successful percentage	Percent of successful pings which is considered valid.
Packet size	Length of IP packet data field.

Table 13 – Gateway priorities

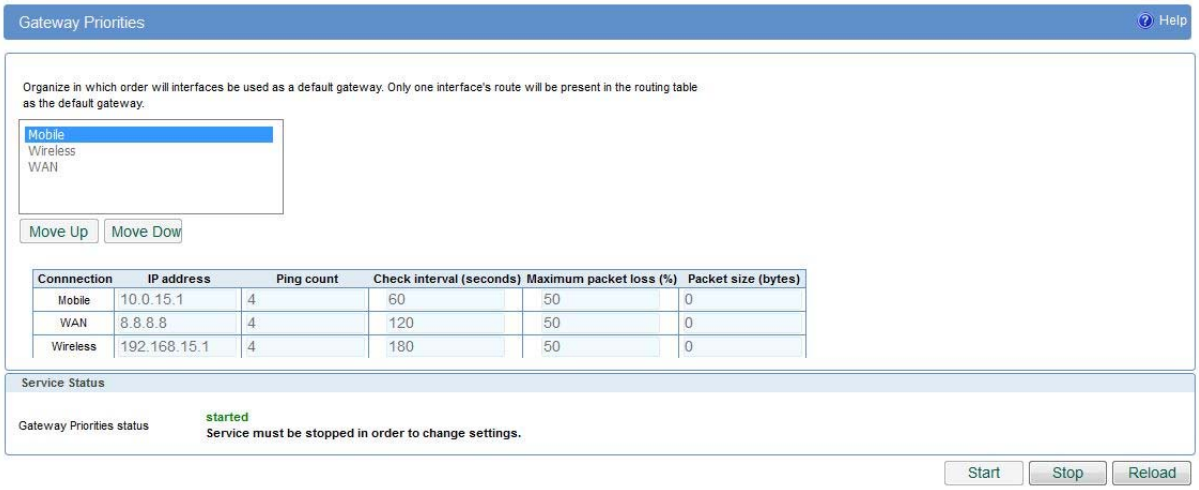


Figure 25 – Gateway priorities

Port forwarding

Port forwarding is an application of NAT (*Network Address Translation*) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway.

For incoming data, the GWR 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 Router.

TCP/UDP Port forwarding	
Enable	This field specifies if NAT is used on the router.
Protocol	This field specifies the IP protocol type.
Source IP	This field specifies incoming IP address for which port forwarding is configured.
Source Netmask	This field specifies incoming IP address netmask for allowed IP subnet.
Source Interface	Select interface where port forwarding is done. Port forwarding settings for source interface include LAN, WAN, ADSL and Mobile interface.
Destination IP	This field specifies destination IP address for which port forwarding is configured.
Destination Netmask	This field specifies destination IP address netmask.
Destination start port	This is the TCP/UDP start port of incoming traffic.
Destination end port	This is the TCP/UDP end port of incoming traffic.
Target IP	This filed specifies IP address where packets should be forwarded.
Target start port	This field specifies starting port for which the traffic will be forwarded.
Target end port	This field specifies ending port for which the traffic will be forwarded.

Add	Click ***Add*** to insert (add) new item in table to the GWR 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 Router. After pressing ***Save*** *button* it make take more than 10 seconds for router to save parameters and become operational again.

Table 14 – Port forwarding settings

Settings – Demilitarized Zone (DMZ)

DMZ (Demilitarized Zone) allows one local 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. Host which will be exposed to the Internet must always have the same IP address, added manually or through DHCP server static lease.

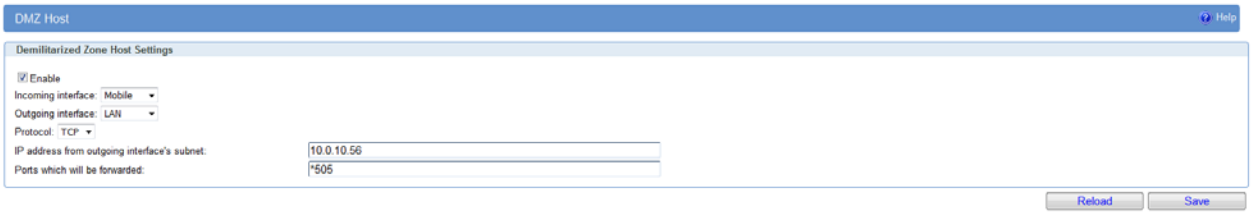


Figure 26 – DMZ configuration page

Demilitarized Zone Host Settings	
Label	**Description**
DMZ Settings	
Enable	This field specifies if DMZ settings is enabled at the Geneko Router.
Incoming Interface	Select through which interface will traffic arrive.
Outgoing Interface	Select through which interface will DMZ be set.
Protocol	Specify if TCP or UDP is used.
IP address from outgoing interface's subnet	IP address which will be exposed to the Internet. This will secure rest of the internal network from external access.
Ports which will be forwarded	Enter port or ports which will be forwarded. One can enter more ports separated by comma, combined with range of ports separated with - or : symbol. For example one can enter 50,500-520,535,600:650.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to save your changes back to the Geneko Router.

Table 15 – Demilitarized Zone

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.
Important: settings must be saved from console in order to be returned after router reboot or export of configuration. It is done with command 'ripd# write' or 'ripd# copy running-config startup-config' Click ***RIP*** Tab, to open the Routing Information Protocol screen. Use this screen to configure the GWR Router RIP parameters *(Figure 27)*.

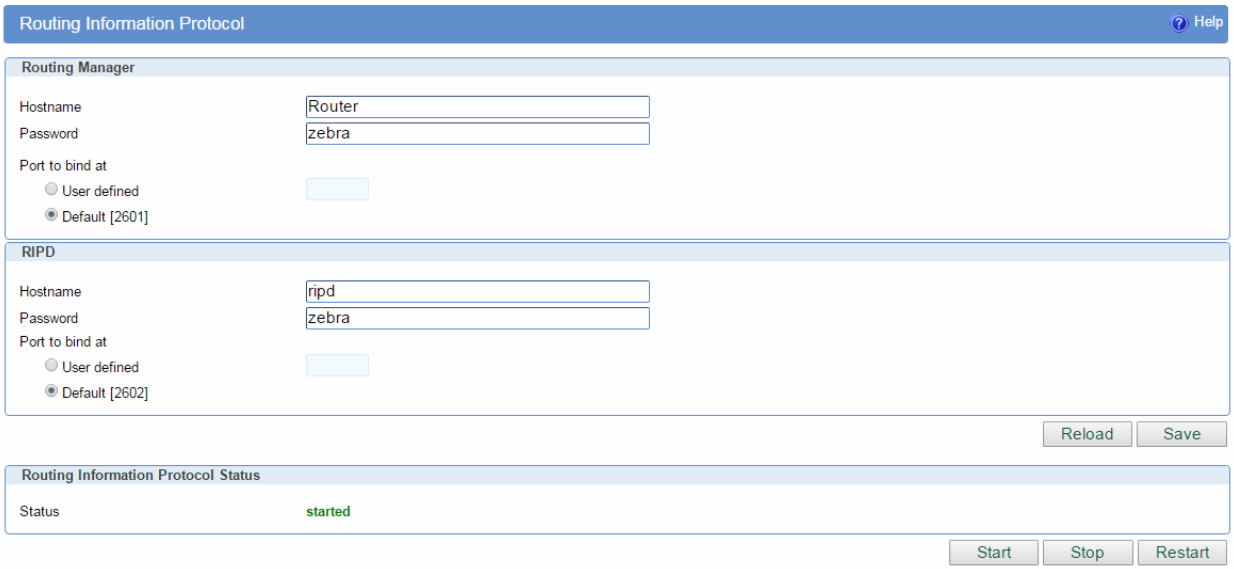


Figure 27 – RIP configuration page

RIP Settings	
Label	**Description**
Routing Manager	
Hostname	Prompt name that will be displayed on telnet console.
Password	Login password.
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 Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 16 – RIP parameters

To enable RIP, click start button under RIP page in the Routing menu.
Use telnet to enter in global configuration mode.

telnet 192.168.1.1 2602 telnet to br0 at TCP port 2602

After telnet, type enable followed by **conf t** and **router rip** to enter RIP configuration mode.

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

ripd(config-router)# **network** [A.B.C.D/Mask]

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

ripd(config-router)# **version** [1|2] // Same as other router //

Disable route redistribution:

ripd(config-router)# **no redistribute kernel**
ripd(config-router)# **no redistribute static**
ripd(config-router)# **no redistribute connected**

Disable RIP update (optional):

ripd(config-router)# **passive-interface br0**
ripd(config-router)# **no passive-interface br0**

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 internet work needs. Use following command to setup RIP timer:

ripd(config-router)#**timers basic** [UPDATE-INTERVAL] [INVALID] [TIMEOUT] [GARBAGE-COLLECT]
ripd(config-router)# **no timers basic**

Configure interface for RIP protocol (first type **exit** if you are at ripd(config-router) to get up from config-router to config mode).

ripd(config)# **interface** greX
ripd(config-if)# **ip rip send version** [VERSION]
ripd(config-if)# **ip rip receive version** [VERSION]

Disable rip authentication at an interface.

ripd(config-if)# **no ip rip authentication mode** [md5|text]

Debug commands:

ripd(config)# **debug rip**
ripd(config)# **debug rip events**
ripd(config)# **debug rip packet**
ripd(config)# **terminal monitor**

Settings – VRRP Settings

VRRP (Virtual Router Redundancy Protocol) is a protocol which elects a master server on a LAN and the master answers to a 'virtual IP address'. If it fails, a backup server takes over the IP address.
VRRP specifies an election protocol to provide the virtual router function described earlier. All protocol messaging is performed using IP multicast datagrams, thus the protocol can operate over a variety of multi-access LAN technologies supporting IP multicast. Each VRRP virtual router has a single well-known MAC address allocated to it.

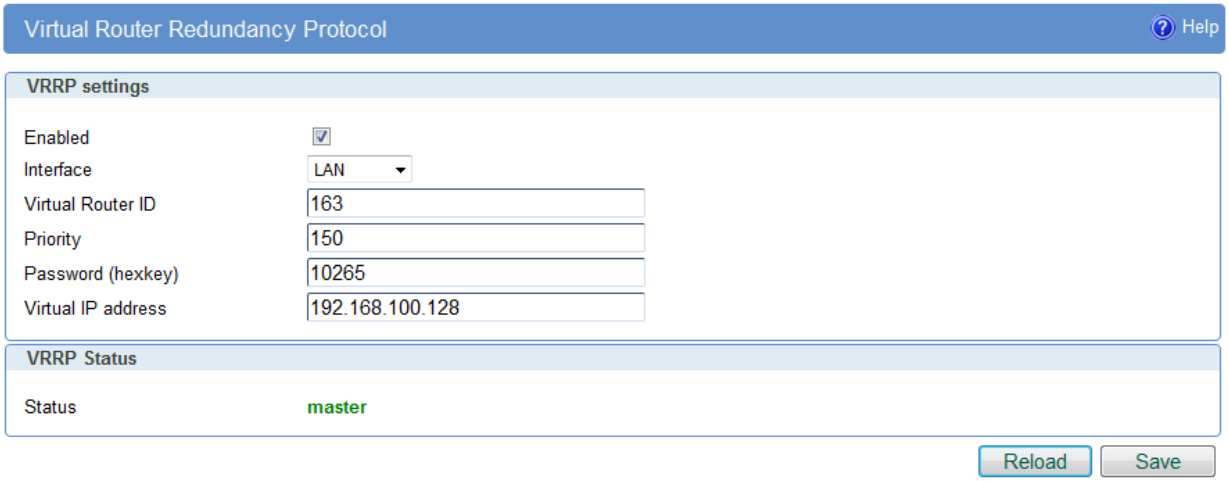


Figure 28 – Virtual Router Redundancy Protocol

VRRP	
Label	**Description**
Enabled	Select this option to enable VRRPD service
Interface	Select on which interface will VRRP be set.
Virtual Router ID	Enter Virtual Router IDentifier (VRID) [1-255], which is the same for all physical routers for virtual router with this ID in the network.
Priority	Routers have a priority of between 1-255 and the router with the highest priority will become the master.
Password	Enter authentication password as hexkey [0-9a-fA-F]+.
Virtual IP address	Enter the IP address(es) of the virtual server
Reload	Click Reload to discard any changes and reload previous settings
Save	Click Save to save changes.

Table 17 – VRRP Parameters

Settings – VPN Settings

VPN (*Virtual private network*) 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 29* 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 Host name of tunnel source.
Tunnel Destination	This field specifies IP address or Host name of tunnel destination.
Interface	This field specifies GRE interface. This field gets from the GWR Router.
Keep Alive Enable	Check for keepalive enable.
Period	Defines the time interval (in seconds) between transmitted keep alive 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 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 Router.

Table 18 – GRE parameters

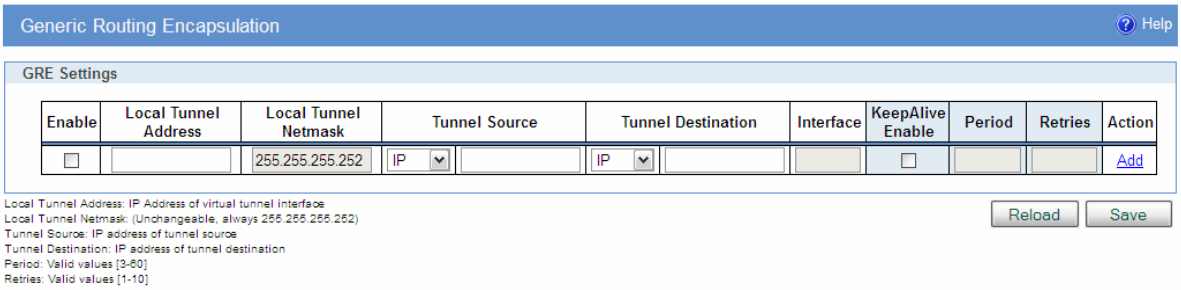


Figure 29 – GRE tunnel parameters configuration page

GRE Keep alive

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)

IPSec (*Internet Protocol Security*) is a protocol suite for securing Internet Protocol communication by authenticating and encrypting each IP packet of a data stream.

Click ***VPN Settings - IPSec***, to open the VPN configuration screen. At the *Figure 30-IPSec Summary screen* you can see IPSec Summary. This screen gathers information about settings of all defined IPSec tunnels.

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.

IPSec Summary and IPSec Settings are briefly displayed in following figures and tables.

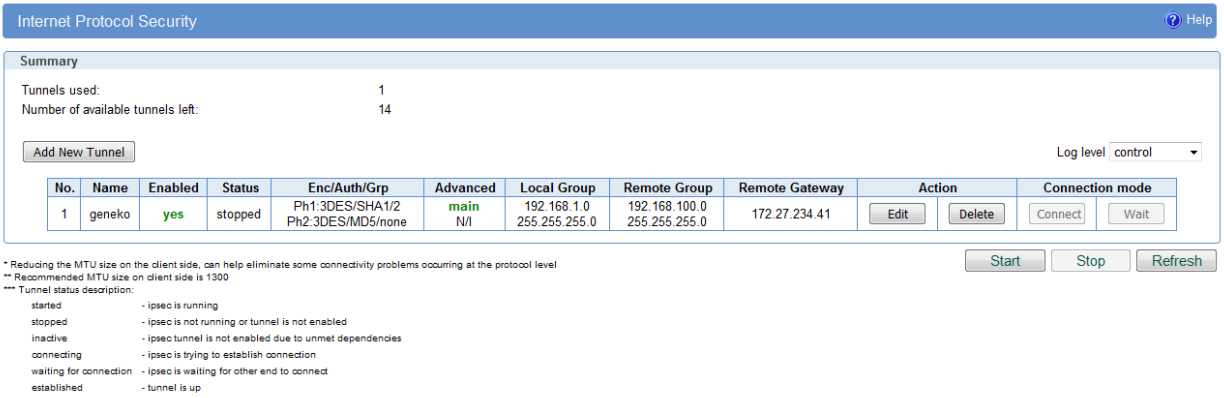


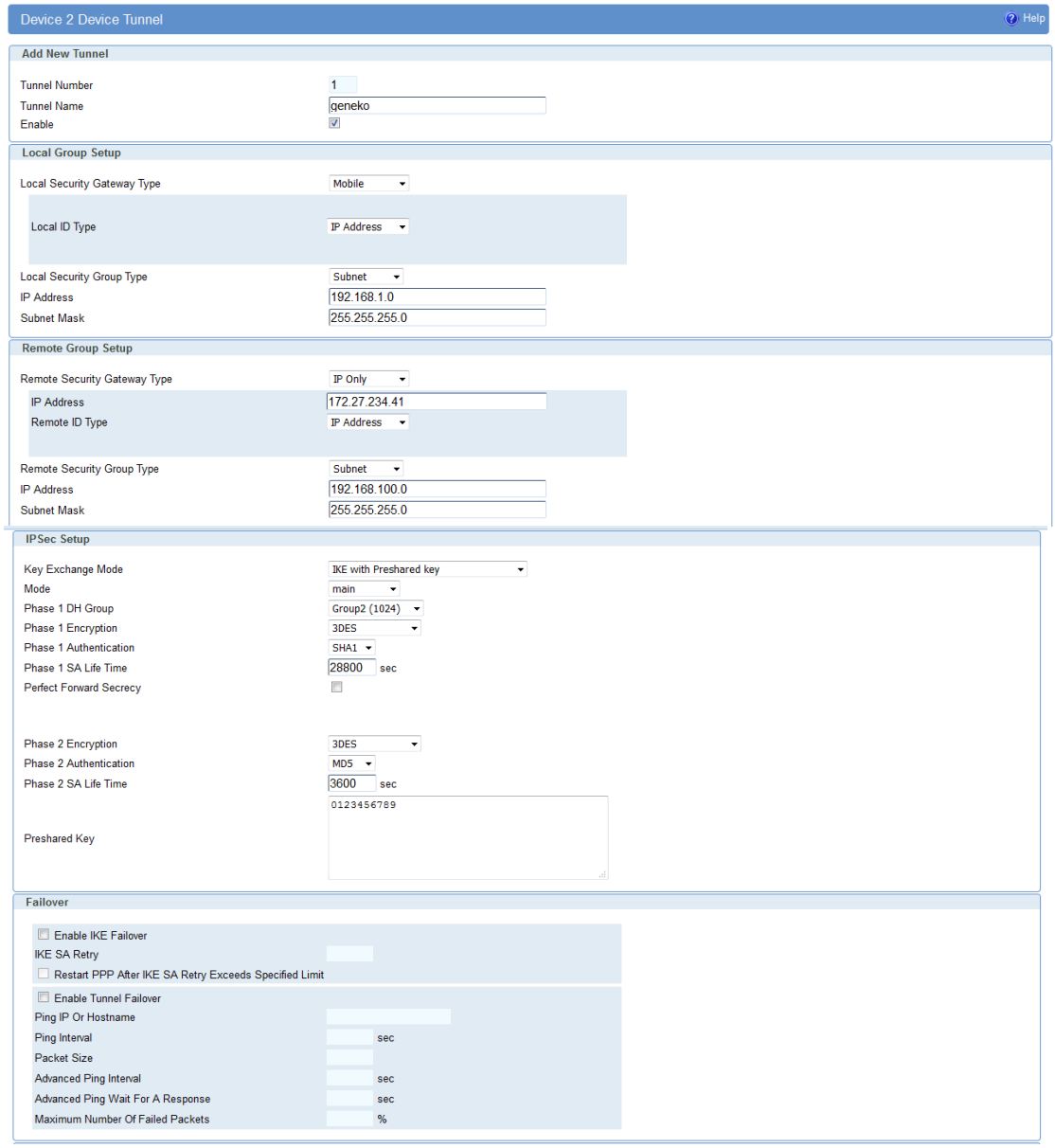
Figure 30 – IPSec Summary screen

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. Maximum number of tunnels is 15.
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.
Action - Edit	This link opens screen where you can change the tunnel's settings.
Action - Delete	Click on this link to delete the tunnel and all settings for that particular tunnel

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.
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 19 – IPSec Summary

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.



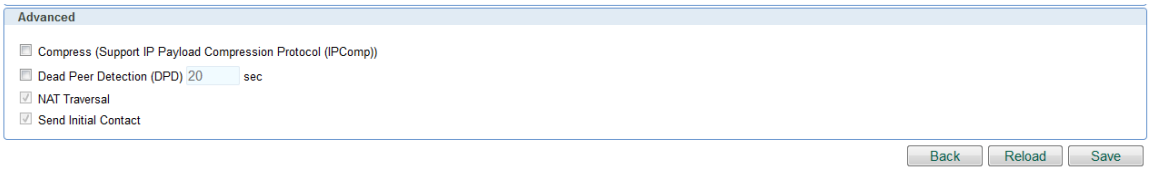


Figure 31 – IPSec Settings

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.
Local Security gateway type	Select an interface on which IPSec will be established (outgoing interface). NOTE: The Local Security Gateway Type IP address must match the Remote Security Gateway Type IP address on the IPSec device at the other end of the tunnel.
IP address	The WAN (Internet) IP address of the Geneko Router automatically appears. If the Geneko Router is not yet connected to the GSM/UMTS network this field will be blank.
Local ID Type	Authentication identity for one of the participant. It can be an IP address or a fully-qualified domain name preceded by @. When using certificates, this field must be filled with information from the certificate CN= field (for example FQDN is @vpn.something.com and user FQDN is someone@something.com if that's what's written in the certificate files).
Local Security Group Type	Define if only the computer with a specific IP address or whole subnet will be able to access the tunnel.
IP Address	Select the local LAN user(s) behind the Geneko 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.
Subnet Mask	Enter the subnet mask.
Remote Security Gateway Type	Select the type you want to use: IP Only - Only a specific IP address will be able to establish a tunnel. NOTE: The Remote Security Gateway Type you select should match the Local Security Gateway Type selected on the IPSec device at the other end of the tunnel.
IP Address	IP address of the remote end with which the tunnel will be formed.
Remote ID Type	Authentication identity for one of the participant. Can be an IP address or fully–qualified domain name preceded by @.
Remote Security Group Type	Define if only the computer with a specific IP address or whole subnet will be able to access the tunnel.
IP Address	Select the remote LAN user(s) behind the Geneko 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.
Subnet Mask	Enter the subnet mask.
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 for the encryption code. For key management, the Geneko Router uses only IKE with Preshared Key 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 and the same key.
Key Exchange mode	**IKE with Preshared Key File** One or more files which contain preshared secret must be uploaded in the IPSec key file management menu. IMPORTANT: context of the file should be plain text and without space characters, so if a tool for generating secrets such as OpenSSL, OpenVPN or IPSec PKI commands were used, make sure there are no spaces for example like in term "----BEGIN CERTIFICATE----", where there is a space between words BEGIN and CERTIFICATE. **IKE with X509 certificates and PSK** This option is used when X509 certificates are used for authentication. Certificate files must first be uploaded through pages which are in the main menu under file management. Pre shared key (PSK) is entered manually and must match on both peers. **IKE with X509 certificates and PSK file** This option is used when X509 certificates are used for authentication. Certificate files must first be uploaded through pages which are in the main menu under file management. Pre shared key file (PSK) is chosen from uploaded PSK files in the IPSec key file management and must match on both peers.
Mode	One of following IPSec modes can be choosed: MAIN or AGGRESSIVE.
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 and Group 14 is 2048 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: 3DES, AES-128 (128-bit), AES-192 (192-bit), AES-256 (256-bit), BLOWFISH-128 (128-bit), BLOWFISH-192 (192-bit), BLOWFISH-256 (256-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	If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation

Secrecy	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, Group 5 is 1536 bits and Group 14 is 2048 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, 3DES, AES-128 (128-bit), AES-192 (192-bit), AES-256 (256-bit), BLOWFISH-128 (128-bit), BLOWFISH-192 (192-bit), BLOWFISH-256 (256-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.
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 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.
Key File	Select which key file to use.
CA certificate	Select which CA certificate file to use.
Local Client Certificate	Select which Local Client Certificate file to use.
Local Client Key	Select which Local Client Key file to use.
Enable IKE failover	Enable IKE failover option which will try to periodically re-establish security association.
IKE SA retry	Number of IKE retries, before failover.
Enable tunnel failover	Enables tunnel failover. If there is more than one tunnel defined, this option will failover to other tunnel in case that selected one fails to establish connection.
Ping IP or Hostname	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 pings.
Packet size	Specify size of data field in IP packet for ping message.
Maximum number of failed packets	Set the percentage of failed packets before failover action is performed.
Compress (Support 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 Geneko Router to propose compression when it initiates a connection.
Dead Peer Detection (DPD)	When DPD is enabled, the Geneko 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 gateway in the path and changing to a new port, as defined in RFC 3947. 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.
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 Geneko Router. After that router automatically goes back and begin negotiations of the tunnels by clicking on the ***Start***.

Table 20 – IPSec Parameters

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.

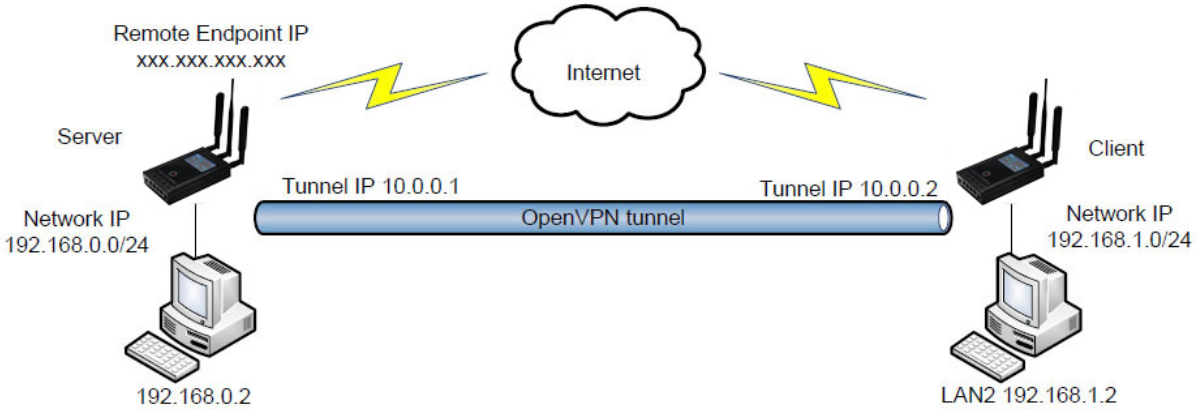


Figure 32 – OpenVPN

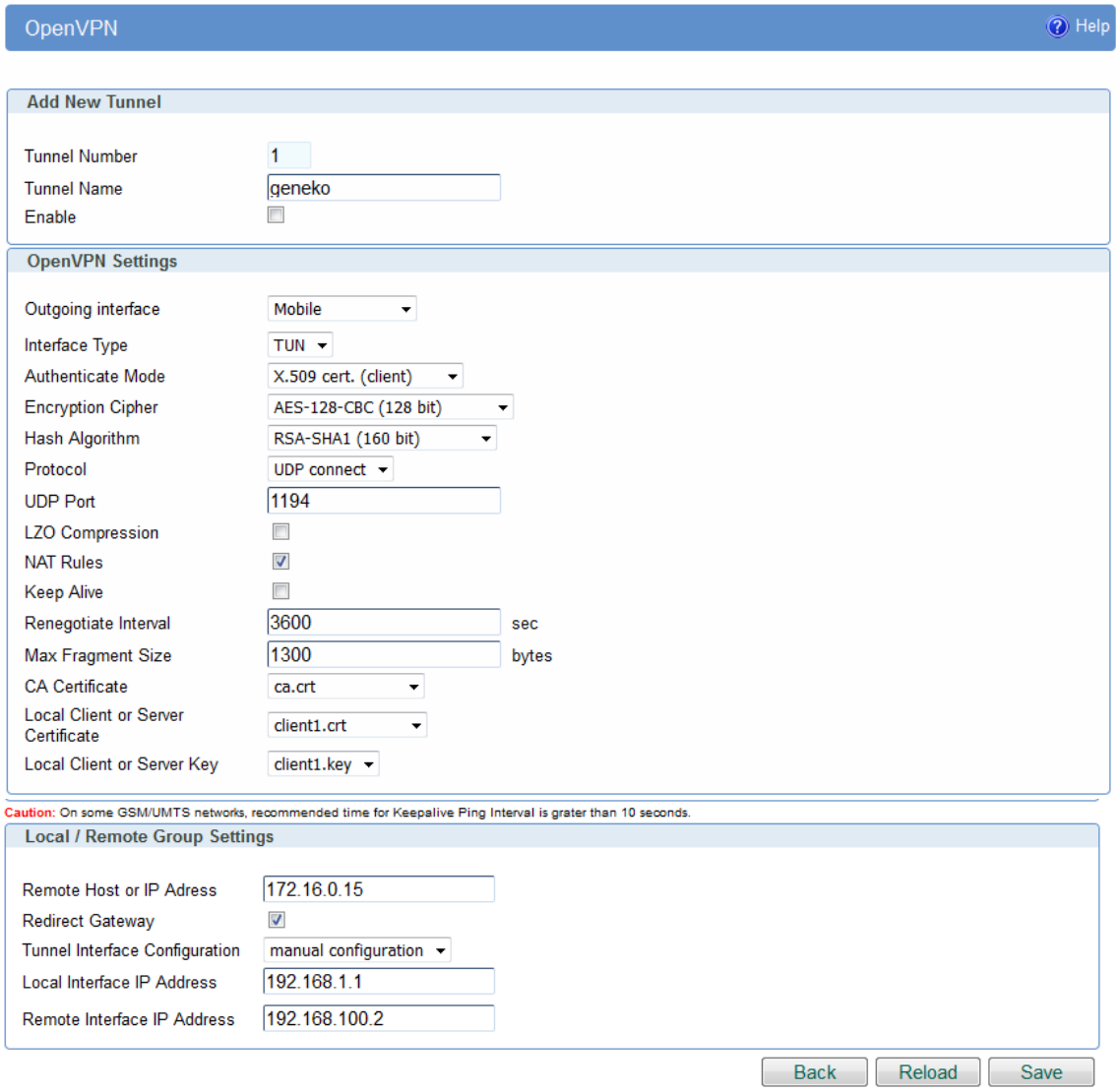


Figure 33 – OpenVPN example 1

Click ***VPN Settings -OpenVPN***, to open the VPN configuration screen. At the *Figure 34* you can see OpenVPN Summary screen. This screen gathers information about settings of all defined OpenVPN tunnels. Up to 3 OpenVPN tunnels can be defined on the GWR router.

OpenVPN Summary and OpenVPN Settings are briefly displayed in following figures and tables.

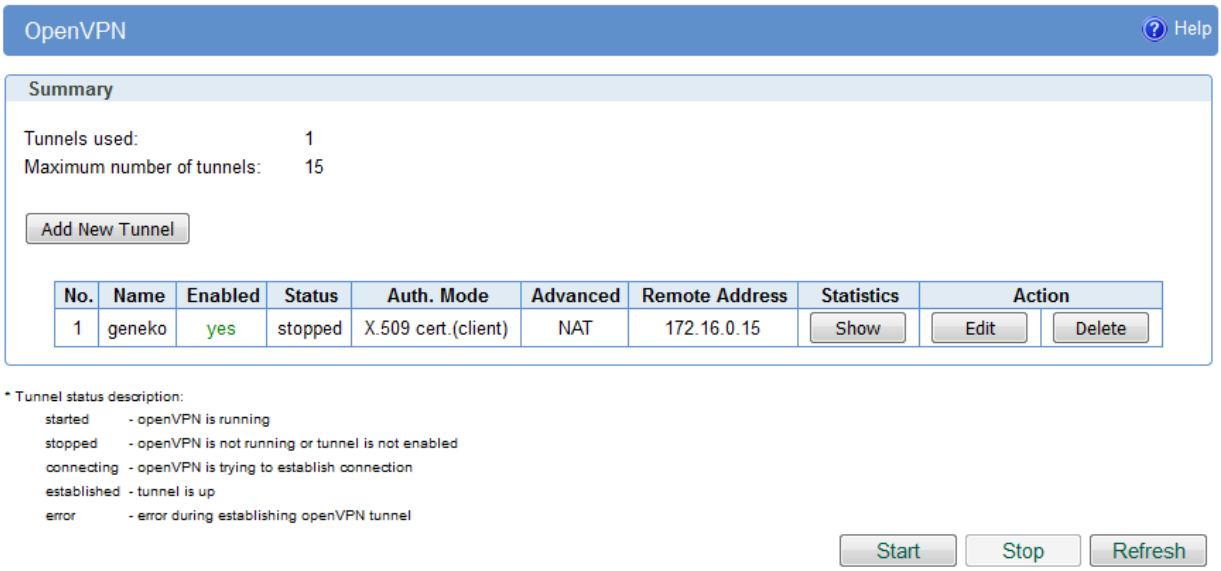


Figure 34 – OpenVPN Summary screen

OpenVPN	
Label	**Description**
IP Filtering	
Tunnel Number	This number will be generated automatically and it represents a number of the tunnel.
Tunnel Name	Enter a name for the OpenVPN 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 this particular OpenVPN tunnel
OpenVPN Settings	
Outgoing Interface	Select Mobile, DSL or Wireless interface.
Interface Type	Select TUN or TAP mode.
Authenticate Mode	Select a method of authentication, options are: NONE, Pre-Shared secret (PSK), Username/Password, X.509 client/server mode. The authentication method determines how the peers are authenticated to each other and to exchange cipher and HMAC keys to protect the data channel. Use NONE if you do not want authentication at all.

	Pre-Shared secret is a simple and easy way to authenticate your hosts. Username/Password can be used only in client mode where your server needs this kind of authentication. X.509 mode is full Transport Layer Security protocol with use of certificate/key pairs. Note that the designation of X.509 client or X.509 server is only for the purpose of negotiating the TLS control channel. Make sure both ends of the OpenVPN tunnel use the same authentication method. Certificate and key files must first be uploaded through web pages listed in the main menu under file management.
Encryption Cipher	Encrypt packets with cipher algorithm. The default is AES-128-CBC, an abbreviation for AES in Cipher Block Chaining mode. On the other hand, Blowfish has the advantages of being fast, very secure, and allowing key sizes of up to 448 bits. Blowfish is designed to be used in situations where keys are changed infrequently. OpenVPN supports the CBC cipher mode.
Hash Algorithm	Authenticate packets with HMAC using message digest algorithm. The default is SHA1. HMAC is a commonly used message authentication algorithm (MAC) that uses a data string, a secure hash algorithm and a key, to produce a digital signature. OpenVPN's usage of HMAC is to first encrypt a packet, then HMAC the resulting ciphertext. In TLS mode, the HMAC key is dynamically generated and shared between peers via the TLS control channel. If OpenVPN receives a packet with a bad HMAC it will drop the packet. HMAC usually adds 16 or 20 bytes per packet. Set none to disable authentication.
Protocol	Select a protocol you want to use for tunnel connection. UDP connect and TCP client will need the "Remote Host or IP Address" field in order to successfully establish a tunnel.
TCP/UDP port	Enter a port number for a tunnel connection.
LZO Compression	Use fast LZO compression. This may add up to 1 byte per packet for incompressible data.
NAT Rules	NAT Rules is enabled by default.
Keep Alive	Use this mechanism to keep tunnel alive.
Ping Interval	Ping interval for sending pings over the TCP/UDP control channels. Number of seconds is specified in this field.
Ping Timeout	Defines a timeout interval in seconds after which a restart of OpenVPN tunnel will be triggered. This value must be twice as "Ping Interval" value.
Max Fragment Size	Enable internal datagram fragmentation so that no UDP datagrams are sent which are larger than max bytes. This option is available only when UDP protocol is being used. There are circumstances where using OpenVPN's internal fragmentation capability may be your only option, such as tunneling a UDP multicast stream which requires fragmentation.
Pre-shared Secret	Use Static Key encryption mode (non-TLS).
Generate PSK	Check this option and use "Generate" button to produce a pre-shared secret.
Paste	Use this option to manually paste a pre-shared secret from remote host's PSK file.
CA Certificate	Certificate authority (CA) file, also referred to as the root certificate.
DH Group	Choose a Diffie-Hellman parameter group. These parameters may be considered public. Available only in X.509 server mode
Username	Enter a username for authentication to the remote host server.

Password	Enter a password for authentication to the remote host server.
Local Certificate	Local peer's signed certificate, must be signed by a certificate authority whose certificate is in "CA Certificate" field.
Local Private Key	Local peer's private key.
	Local/Remote Group Settings
Remote Host or IP Address	Enter a remote peer IP address or host name. This filed is available only in UDP connect and TCP client mode.
Redirect Gateway	Check this option in order to use tunnel interface for default route.
Tunnel Interface Configuration	"Pull from server" mode is used when remote peer is an OpenVPN server and from where configuration will be pulled. In "Manual configuration" mode, you can enter tunnel interface IP addresses.
Local Interface IP Address	This is the IP address of the local VPN endpoint of local tunnel interface.
Remote Interface IP Address	This is the IP address of the remote VPN endpoint of remote tunnel interface.
Network Topology	Configure virtual addressing topology. **net30** - use a point-to-point topology, by allocating one /30 subnet per client. **p2p** - use a point-to-point topology where the remote endpoint of the client's tunnel interface always points to the local endpoint of the server's tunnel interface. This mode allocates a single IP address per connecting client. Only use when none of the connecting clients are Windows systems **subnet** - use a subnet rather than a point-to-point topology by configuring the tunnel interface with a local IP address and subnet mask. This mode allocates a single IP address per connecting client and works on Windows as well.

Table 21 – OpenVPN parameters

Settings – PPTP

The GWR Router can be used as a PTPP (Point-to-Point Tunneling Protocol) client. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

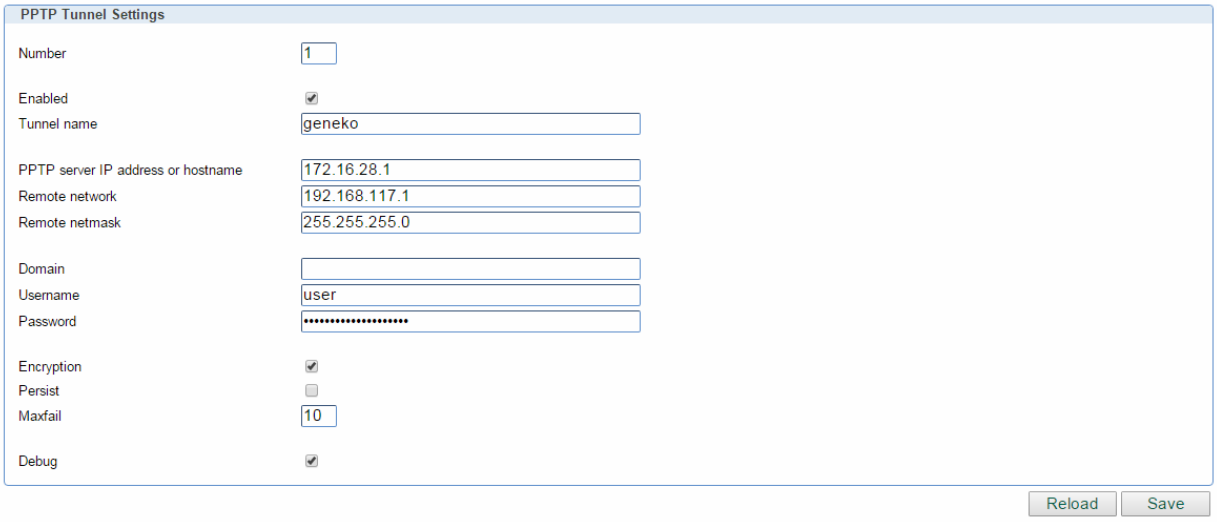


Figure 35 – PPTP configuration page

PPTP	
Label	**Description**
Number	Selected tunnel number. Nubmer of PPTP tunnels is limited to 5.
Enabled	Select this option to enable tunnel.
Tunnel name	Unique tunnel identifier.
PPTP server IP address or hostname	IPv4 address of remote PPTP server.
Remote network	After the tunnel is established, route to this network will be added.
Remote netmask	Netmask of remote subnet to route.
Domain	Some PPTP servers require domain name for authentication.
Username	Username to authenticate ourselves to remote server.
Password	Password to authenticate ourselves to remote server.
Encryption	Leave this option enabled to use default MPPE (Microsoft encryption) and MPPC (Microsoft compression) protocols.
Persist	If this option is enabled, tunnel will try to reconnect.
Maxfail	Max number of retries to reconnect. 0 for infinite retries.
Debug	Enable extra information in system log.
Edit	Click Edit to edit selected tunnel from the table.
Delete	Click Delete to delete selected tunnel from table.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to create new, or save changes to existing tunnel.

Table 22 – PPTP parameters

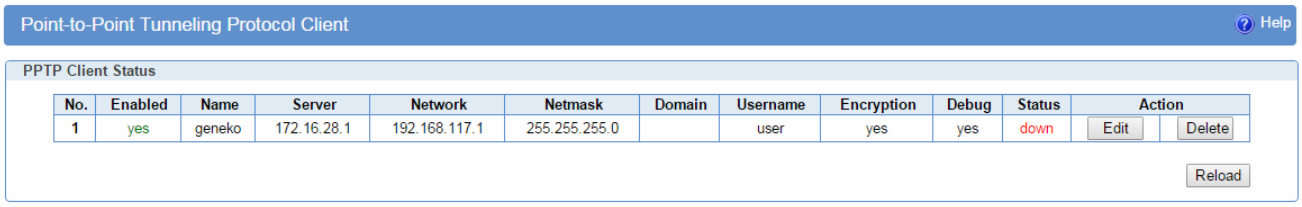


Figure 36 – PPTP Summary screen

Settings – L2TP

L2TP is suitable for Layer-2 tunneling. Static tunnels are useful to establish network links across IP networks when the tunnels are fixed. L2TP tunnels can carry data of more than one session. Each session is identified by a session id and its parent tunnel's tunnel id. A tunnel must be created before a session can be created in the tunnel.

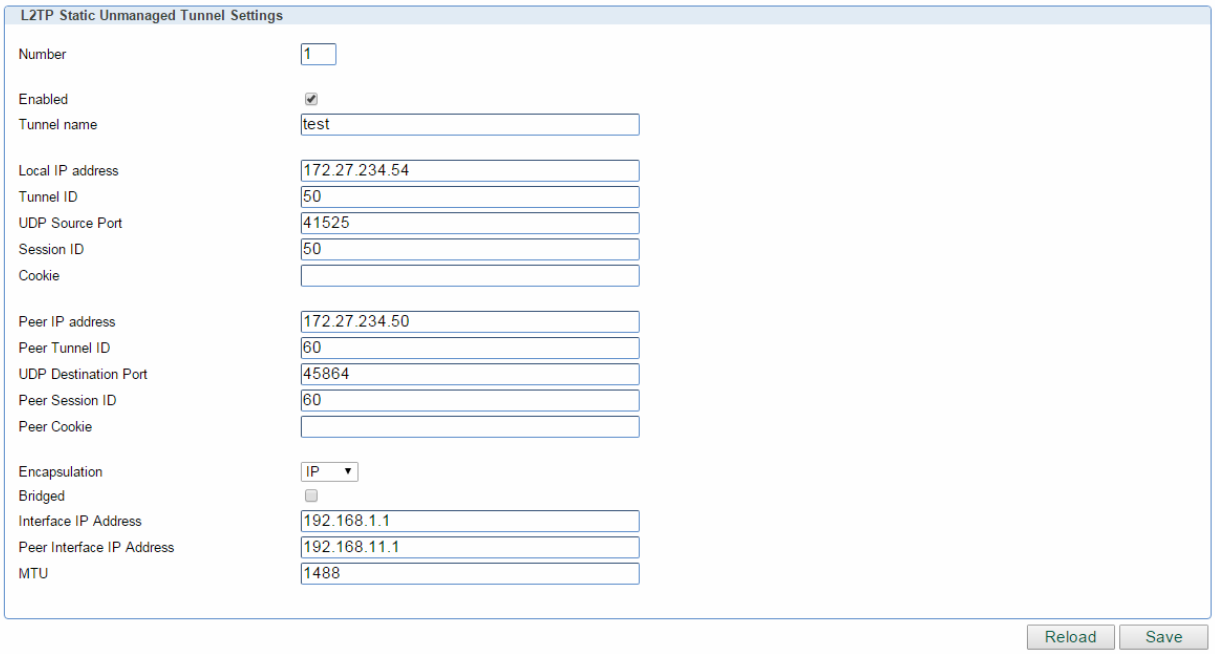
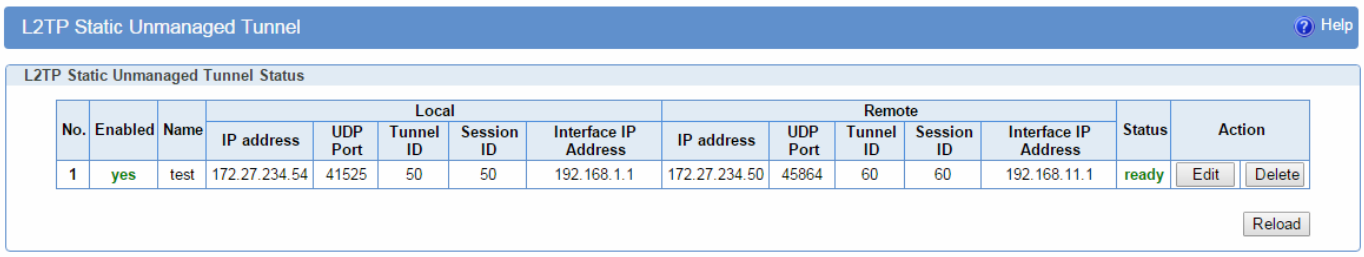


Figure 37 – L2TP configuration page

L2TP	
Label	**Description**
Number	Selected tunnel number. Number of L2TP tunnels is limited to 5.
Enable	Select this option to enable L2TP tunnel.
Tunnel name	Unique tunnel identifier.
Local IP address	Set the IP address of the local interface to be used for the tunnel. This address must be the address of a local interface.
Tunnel ID	Set the tunnel id, which is a 32-bit integer value. Uniquely identifies the tunnel. The value used must match the peer tunnel id value being used at the peer.
UDP Source Port	Set the UDP source port to be used for the tunnel. Must be present when UDP

	encapsulation is selected. Ignored when ip encapsulation is selected.
Session ID	Set the session id, which is a 32-bit integer value. Uniquely identifies the session being created. The value used must match the peer_session id value being used at the peer.
Cookie	Sets an optional cookie value to be assigned to the session. This is a 4 or 8 byte value, specified as 8 or 16 hex digits, e.g. 014d3636deadbeef. The value must match the peer cookie value set at the peer. The cookie value is carried in L2TP data packets and is checked for expected value at the peer. Default is to use no cookie.
Peer IP address	Set the IP address of the remote peer.
Peer Tunnel ID	Set the peer tunnel id, which is a 32-bit integer value assigned to the tunnel by the peer. The value used must match the tunnel id value being used at the peer.
UDP Destination Port	Set the UDP destination port to be used for the tunnel. Must be present when UDP encapsulation is selected. Ignored when IP encapsulation is selected.
Peer Session ID	Set the peer session id, which is a 32-bit integer value assigned to the session by the peer. The value used must match the session id value being used at the peer.
Peer Cookie	Sets an optional peer cookie value to be assigned to the session. This is a 4 or 8 byte value, specified as 8 or 16 hex digits, e.g. 014d3636deadbeef. The value must match the cookie value set at the peer. It tells the local system what cookie value to expect to find in received L2TP packets. Default is to use no cookie.
Encapsulation	Set the encapsulation type of the tunnel. Valid values for encapsulation are: UDP, IP.
Bridged	The two interfaces can be configured with IP addresses if only IP data is to be carried. To carry non-IP data, the L2TP network interface is added to a bridge instead of being assigned its own IP address. Since raw ethernet frames are then carried inside the tunnel, the MTU of the L2TP interfaces must be set to allow space for those headers.
Interface IP Address	Local private P-t-P IP address.
Peer Interface IP Address	Remote private P-t-P IP address.
MTU	MTU of the L2TP interface. Default 1446 for bridged or 1488 for Layer 3 tunnel.
Edit	Click Edit to edit selected tunnel from the table.
Delete	Click Delete to delete selected tunnel from table.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to create new, or save changes to existing tunnel.

Table 23 – L2TP parameters



No.	Enabled	Name	Local					Remote					Status	Action	
			IP address	UDP Port	Tunnel ID	Session ID	Interface IP Address	IP address	UDP Port	Tunnel ID	Session ID	Interface IP Address			
1	yes	test	172.27.234.54	41525	50	50	192.168.1.1	172.27.234.50	45864	60	60	192.168.11.1	ready	Edit	Delete

Figure 38 – L2TP Summary screen

File management

CA Certificate

This page is used to manage CA certificate files so they can be used for peer authentication. Certification authority (CA) certificates are certificates that are issued by a CA to itself or to a second CA for the purpose of creating a defined relationship between the two CAs. A certificate that is issued by a CA to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy. Once the trusted root has been established, it can be used to authorize subordinate CAs to issue certificates on its behalf. Although the relationship between CAs is most commonly hierarchical, CA certificates can also be used to establish trust relationships between CAs in two different public key infrastructure (PKI) hierarchies. In all of these cases, the CA certificate is critical to defining the certificate path and usage restrictions for all end entity certificates issued for use in the PKI. Usually this file is called ca.crt or ca.pem or ca.der and it can be generated with various tools, for example with OpenSSL, OpenVPN e.t.c.
There are options to first browse for the file, then to upload the file. After one or more files are uploaded, a table with uploaded files is shown with the option to delete each of them if they are no longer needed.

CA Certificate Files Management	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.
Details	Details button for displaying details about the certificate (issuer, valid from, valid until)
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button, it is used to start the upload of the file.

Table 24 – CA Certificate

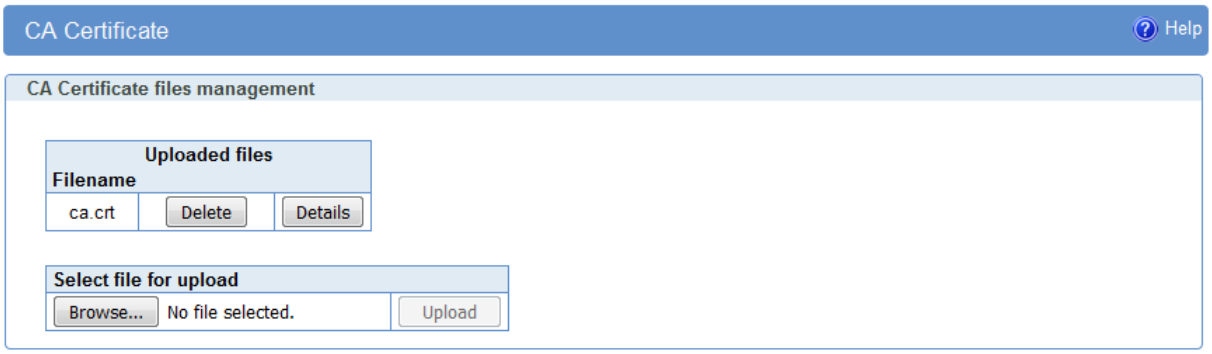


Figure 39 – CA Certificate

Private Certificate

This page is used to manage local client certificate files so they can be used for peer authentication. In cryptography, a client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity. Usually this file is called client1.crt or client1.pem or client1.pem and it can be generated with various tools, for example with OpenSSL, OpenVPN e.t.c. There are options to first browse for the file, then to upload the file. After one or more files are uploaded, a table with uploaded files is shown with the option to delete each of them if they are no longer needed.

Private Key Certificate Files Management	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.
Details	Details button for displaying details about the certificate (issuer, valid from, valid until)
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button, it is used to start the upload of the file.

Table 25 – Private Certificate

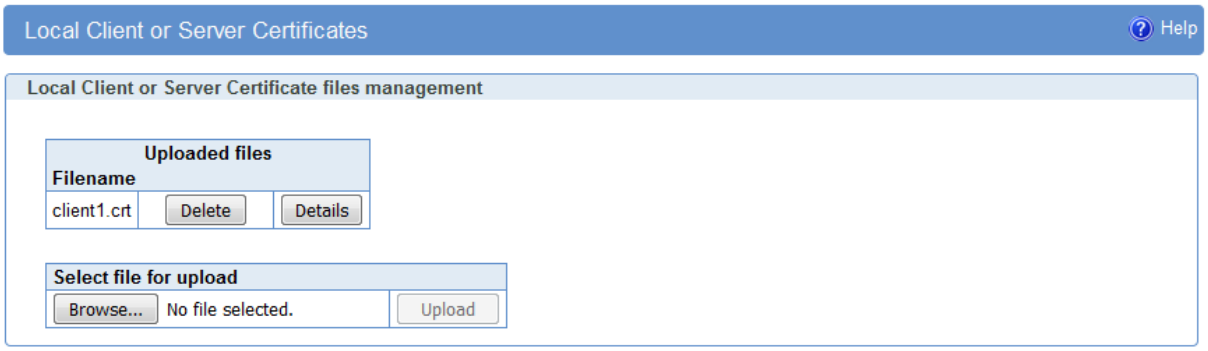


Figure 40 – Private Certificate

Private Key

This page is used to manage local client or server key files so they can be used for peer authentication. In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a distinguished name in the case of an X.509 certificate) which must be signed using the applicant's private key. The CSR also contains the public key chosen by the applicant. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information. The three main parts that a certification request consists of are the certification request information, a signature algorithm identifier, and a digital signature on the certification request information. The first part contains the significant information, including the public key. The signature by the requester prevents an entity from requesting a bogus certificate of someone else's public key. Thus the private key is needed to produce, but it is not part of, the CSR.

Local Client or Server Key files management	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.
Details	Details button for displaying details about the certificate (issuer, valid from, valid until)
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button, it is used to start the upload of the file.

Table 26 – Private Key

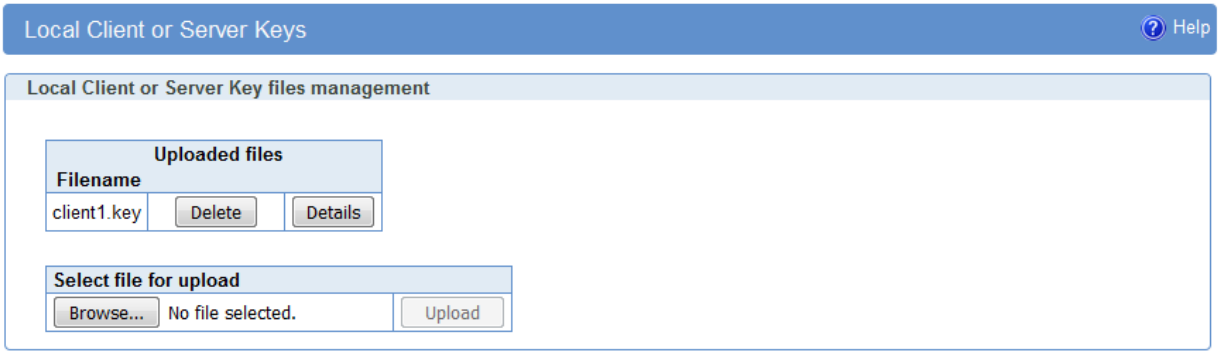


Figure 41 – Private Key

CRL Certificate

This page is used to manage Certificate Revocation List certificate files so they can be used for validating certificates. In the operation of some cryptosystems, usually public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted. There are two different states of revocation defined in RFC 3280: revoked and hold. Usually this file is called crl.crl or crl.pem and it can be generated with various tools, for example with OpenSSL, OpenVPN e.t.c.

Certificate Revocation List Files Management	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.
Details	Details button for displaying details about the certificate (issuer, valid from, valid until)
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button, it is used to start the upload of the file.

Table 27 – CRL Certificate

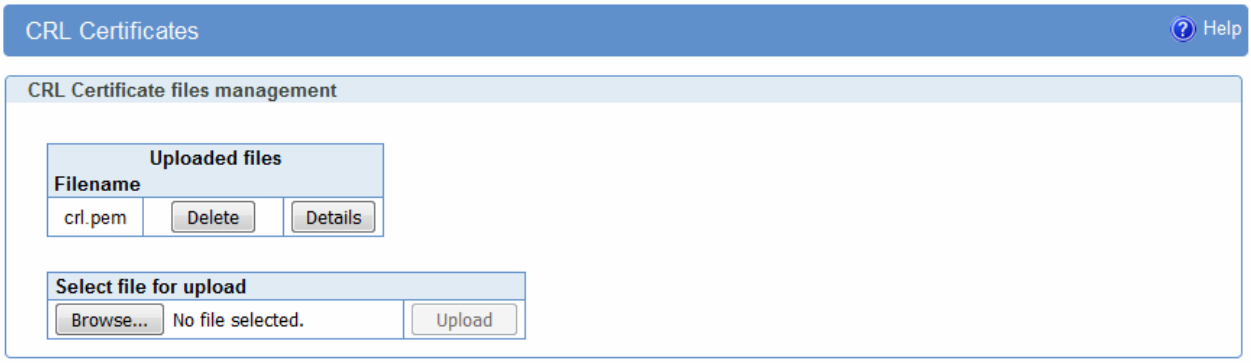


Figure 42 – CRL Certificate

Preshared Key Files

This page is used to manage textual key files with shared secret written into them so the same file can be used on more peers for their authentication.
IMPORTANT: context of the file should be plain text and without space characters, so if a tool for generating secrets such as OpenSSL, OpenVPN or IPSec PKI commands were used, make sure there are no spaces for example like in term "----BEGIN CERTIFICATE----", where there is a space between words BEGIN and CERTIFICATE.
There are options to first browse for the file, then to upload the file. After one or more files are uploaded, a table with uploaded files is shown with the option to delete each of them if they are no longer needed.

Key Files Management	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.
Details	Details button for displaying contents of the file.
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button; it is used to start the upload of the file.

Table 28 – Preshared Key Files

Figure 43 – Preshared Key files management

Settings – Firewall – IP Filtering

TCP/IP traffic flow is controlled over IP address and port number through router's interfaces in both directions. With firewall options it is possible to create rule which exactly matches traffic of interest. Traffic can be blocked or forward depending of action selected. It is important when working with firewall rules to have in mind that traffic for router management should always be allowed to avoid problem with unreachable router. Firewall rules are checked by priority from the first to the last. Rules which are after matching rule are skipped.

Firewall	
Label	**Description**
Firewall Rule Basic	
Enable Firewall	This field specifies if Firewall is enabled at the router.
Firewall Rules	
Priority	This field indicates the order in which the rule will be processed.
Name	Field shows the Rule Name that you gave to the firewall rule.
Enabled	This field shows if rule is enabled or disabled. After clicking on Apply rule button, only enabled rules will be applied.
Chain	Field displays chosen chain of the firewall rule.
Service	This field displays a service which is based on a predefined service protocol and service port. Also it can specifies a custom defined values.
Protocol	The protocol of the rule or of the packet to check. The specified protocol can be one of All, TCP, UDP, UDPLITE, ICMP, ESP, AH, SCTP or it can be a numeric value (from 0 to 255), representing one of these protocols or a different one. The number zero is equivalent to all. Protocol all will match with all protocols and is taken as default when this option is omitted.
Port(s)	This field specifies a service port with predefined or custom defined values.
Input Interface	Select the name of an interface via which a packet was received (only for packets entering the INPUT and FORWARD chains).
Output Interface	Select the name of an interface via which a packet is going to be sent (for packets entering the FORWARD and OUTPUT chains).
Source address	Field shows source IP-address of the packet. It can be single IP address, range of IP addresses or "any".
Destination Address	Destination IP -address for the packet. It can be single IP address, range of IP addresses or "any".

Packet state	This option, when combined with connection tracking, allows access to the connection tracking state for this packet. Possible states are INVALID meaning that the packet could not be identified for some reason which includes running out of memory and ICMP errors which don't correspond to any known connection, ESTABLISHED meaning that the packet is associated with a connection which has seen packets in both directions, NEW meaning that the packet has started a new connection, or otherwise associated with a connection which has not seen packets in both directions, and RELATED meaning that the packet is starting a new connection, but is associated with an existing connection, such as an FTP data transfer, or an ICMP error.
Policy	Field shows selected firewall policy: ACCEPT, REJECT or DROP. If selected policy is REJECT field displays chosen reject type of the firewall rule.
DDos	This field shows if Distributed Denial of Service is disabled or enabled.
Edit	This link opens screen where you can change the rule's settings.
Delete	Click on this link to delete the rule and all settings for that particular rule.
Add New Rule	Click Add New Rule to add a new firewall rule. After you have added the rule, you will see it listed in the Summary table.
Apply rules	Click Apply rules to apply your firewall rules to the Geneko Router.

Table 29 – Firewall parameters

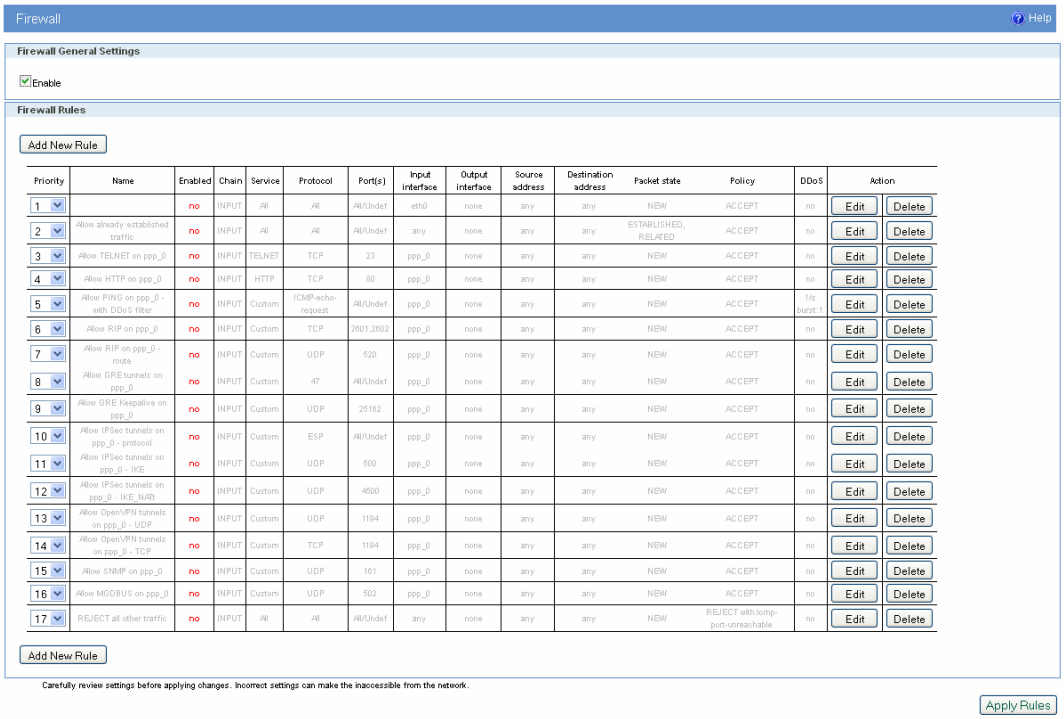


Figure 44 – Firewall configuration page

Settings – Firewall – MAC Filtering

MAC filtering can be used to restrict which Ethernet devices can send packets to the router. If MAC filtering is enabled, only Ethernet packets with a source MAC address that is configured in the MAC Filter table will be allowed. If the source MAC address is not in the MAC Filter table, the packet will dropped.

MAC Filtering Settings	
Label	**Description**
Enable MAC Filtering	This field specifies if MAC Filtering is enabled at the router
Enable	Enable MAC filtering for a specific MAC address
Name	Field shows the Rule Name that is given to the MAC filtering rule
MAC address	The Ethernet MAC source address to allow
Reload	Click **Reload** to discard any changes and reload previous settings
Save	Click **Save** to save changes back to the GWR router

Table 30 – MAC filtering parameters

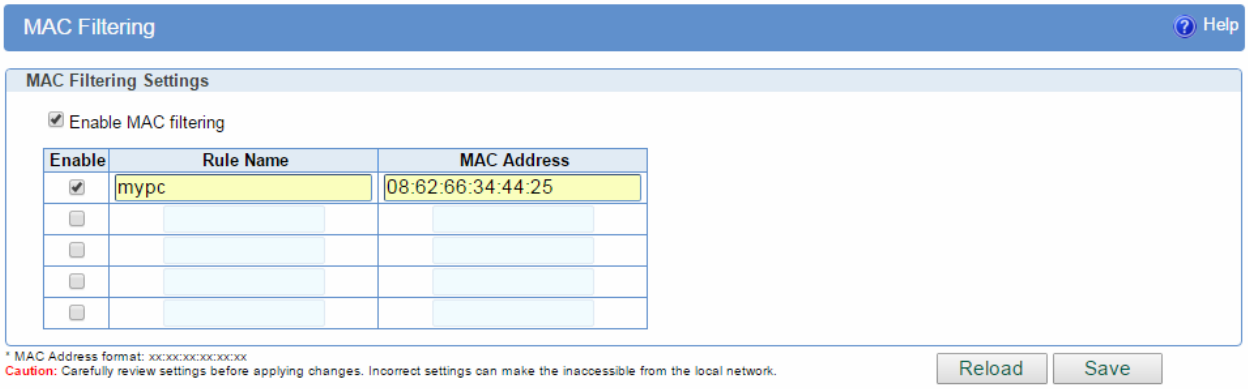


Figure 45 – MAC filtering configuration page

Settings – Dynamic DNS

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 46*.

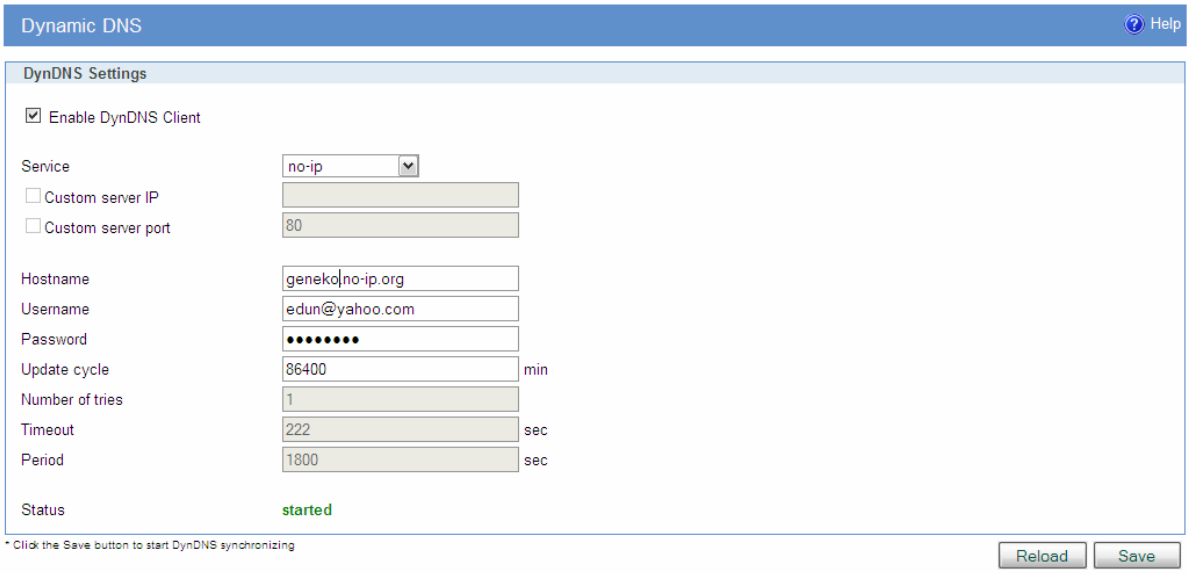


Figure 46 – DynDNS settings

DynDNS	
Label	**Description**
Enable DynDNS Cilent	Enable DynDNS Client.
Interface	Select on which interface DynDNS works (Mobile, Wireless or DSL).
Service	The type of service that you are using, try one of: no–ip, dhs, pgpow, dyndns, dyndns–static, dyndns–custom, ods, easydns, dyns, justlinux and zoneedit.
Custom Server IP or Hostname	The server IP or Hostname 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.
Update cycle	Defines interval between updates of the DynDNS client. Default and minimum value for all DynDNS services, except No–IP service, is 86400 seconds. Update cycle value for No–IP service is represented in minutes and minimum is 1 minute.
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 Router.

Table 31 – 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.

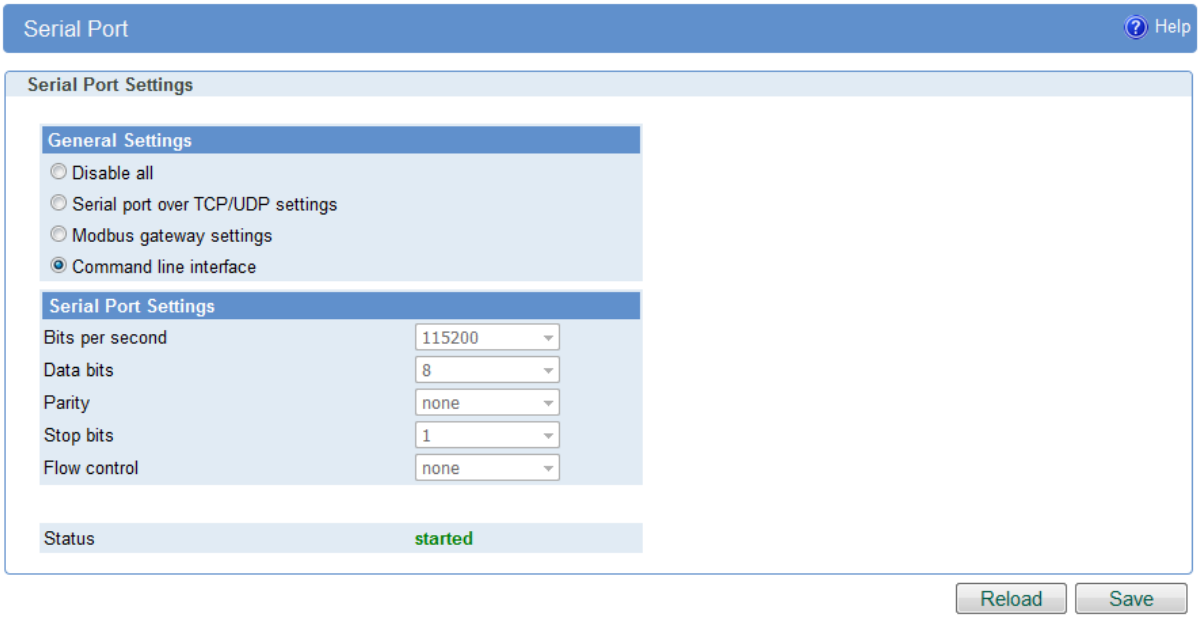


Figure 47 – Serial Port Settings initial menu

General Settings	
Label	**Description**
Disable All	Disable serial to Ethernet converter and Modbus gateway.
Serial port over TCP/UDP settings	Enable serial to Ethernet converter. This provides a way for a user to connect from a network connection to a serial port.
Modbus gateway settings	Enable translation between Modbus/TCP and Modbus/RTU.

Table 32 – Serial port 1 parameters

Serial port over TCP/UDP settings

The GWR 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 Router supports RFC 2217 (remote control of serial port parameters).

Serial Port over TCP/UDP Settings	
Label	**Description**
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.
Type	Select whether to use server IP address or server hostname.
Server IP address	Enter server's IP address.
Server hostname	Enter server's hostname.
Bind to TCP port	Number of the TCP/IP port on which to accept connections from for this device.
Type of socket	Either raw or telnet. Raw enables the port and transfers all data as-is. Telnet enables the port and runs the telnet protocol on the port to set up telnet parameters. This is most useful for using telnet.
Enable local echo	Enables or disables local echo.
Enable inactivity timeout	Close connection after some period of inactivity.
Enable retry timeout	Timeout for retrying connection to unreachable server or port.
Check TCP connection	Enable connection checking.
Kepalive idle time	Set keepalive idle time in seconds.
Kepalive interval	Set time period between checking.

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

Table 33 – Serial Port over TCP/UDP parameters

Click *Serial Port* Tab to open the Serial Port Configuration screen. Use this screen to configure the GWR Router serial port parameters *(Figure 48)*.

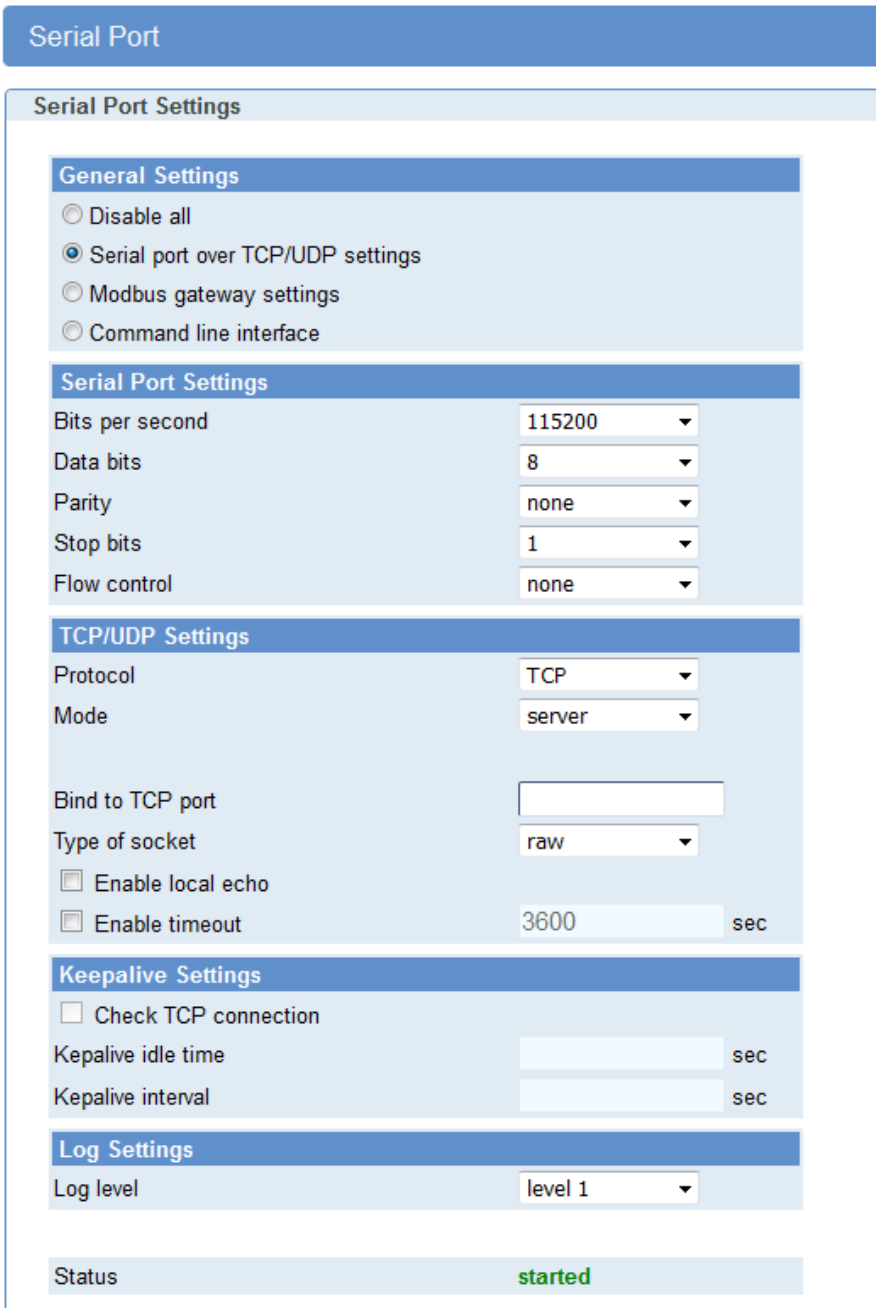


Figure 48 – Serial Port configuration page

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 settings to configure Modbus. At the *Figure 49* – Modbus gateway configuration page you can see screenshot of Modbus Gateway configuration menu.

Modbus Gateway Settings	
Label	**Description**
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.
Pause between request	Set pause between requests in milliseconds. Valid values are between 1 and 10000. Default value is 100).
Maximum number of retries	If no valid response is 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 Router and activate/deactivate serial to Ethernet converter.

Table 34 – Modbus gateway parameters

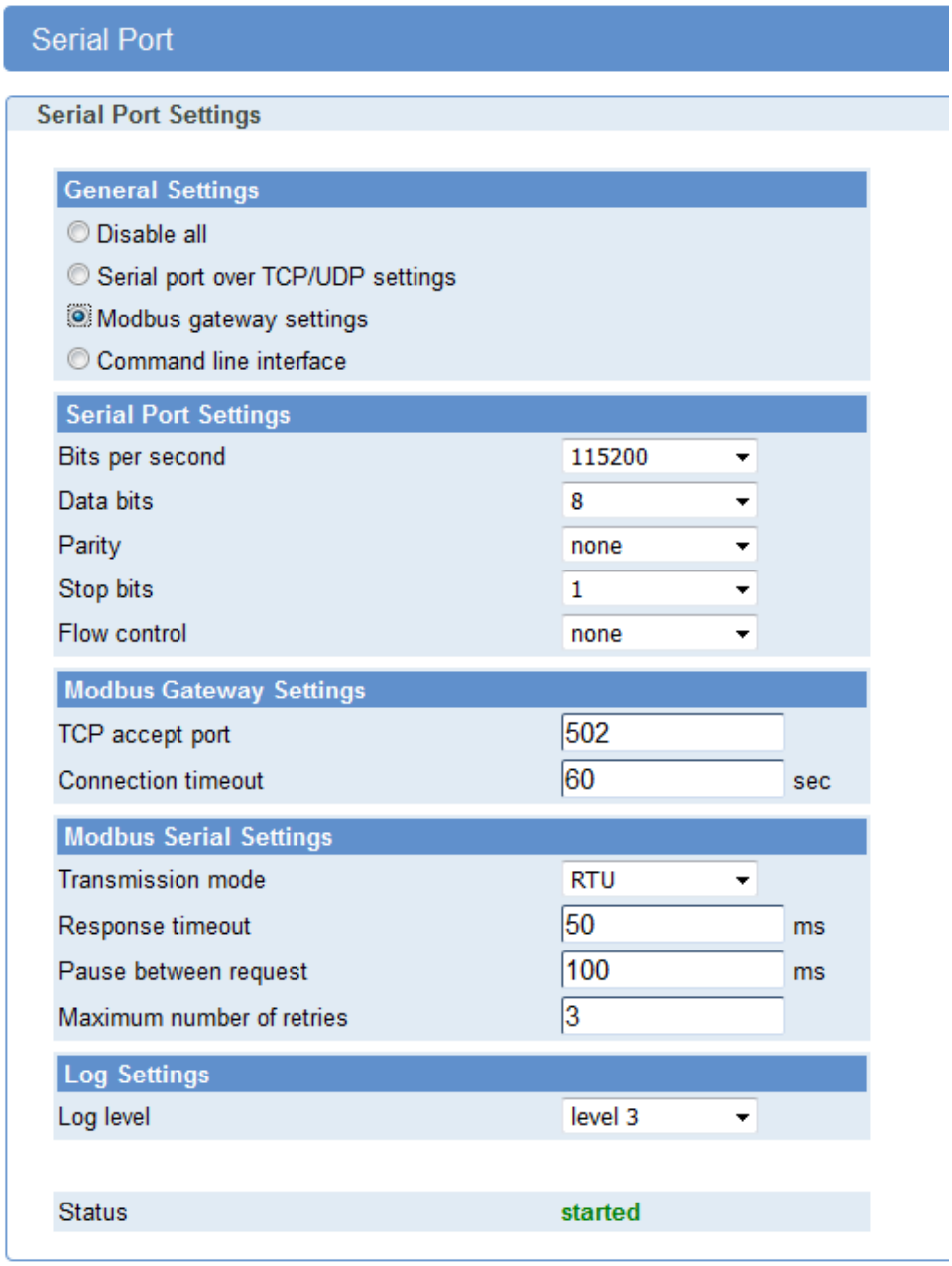


Figure 49 – Modbus gateway configuration page

SMS – SMS Remote Control

SMS remote control feature allows users to execute a short list of predefined commands by sending SMS messages to the router. GWR 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

5. In order to establish PPP connection over the other SIM card, user should send SMS containing following string:
   :SWITCH-SIM
   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.

6. In order to restart whole router user should send SMS containing following string:
   :REBOOT
   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.

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**). SMS service centre number can be obtained automatically (option "Use default SMSC is enabled") or manually by entering number under field "Custom SMSC".

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

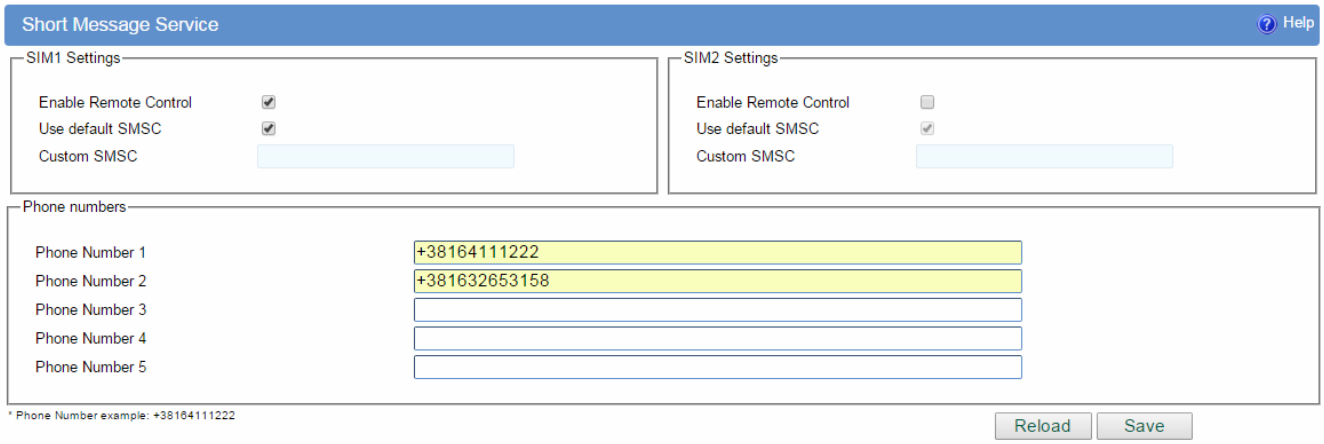


Figure 50 – SMS remote control configuration

SMS – Send SMS

SMS send feature allows users to send SMS message from WEB interface. In following picture is page from where SMS can be sent. There are two required fields on this page: Phone number and Message. Sending SMS messages is possible with this application. The SMS message will be sent after entering Phone number and Message and by pushing button Send

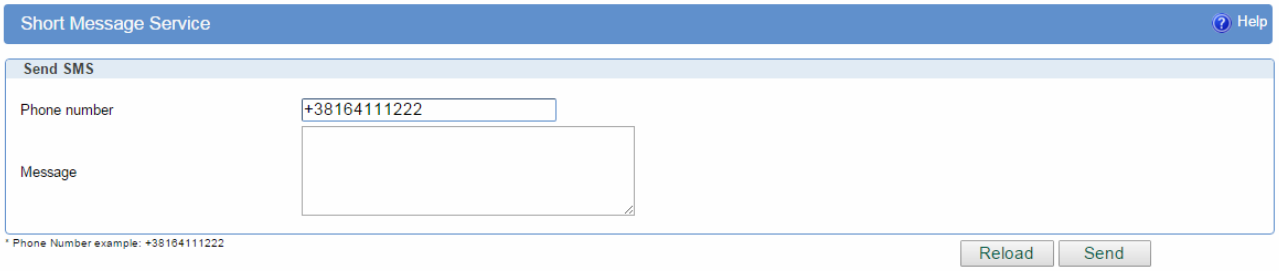


Figure 51– Send SMS

Maintenance

The GWR 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 – System Control

Create a scheduled task to reboot the device at a regular interval.

Figure 52 – System control

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 53*.

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

Table 35 – Device Identity parameters

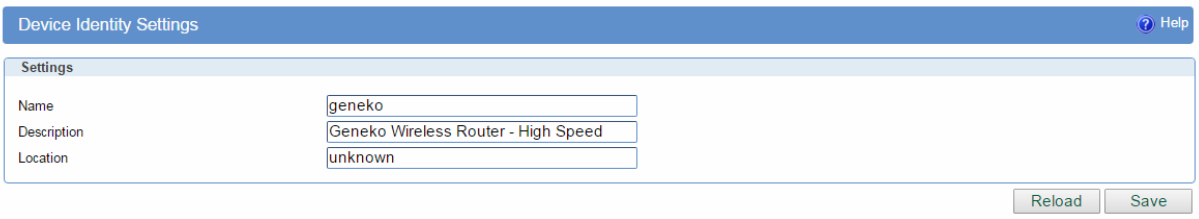


Figure 53 – Device Identity Settings configuration page

Maintenance – Authentication

By ***Administrator Password*** Tab it is possible to activate and deactivate 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 54*.

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.

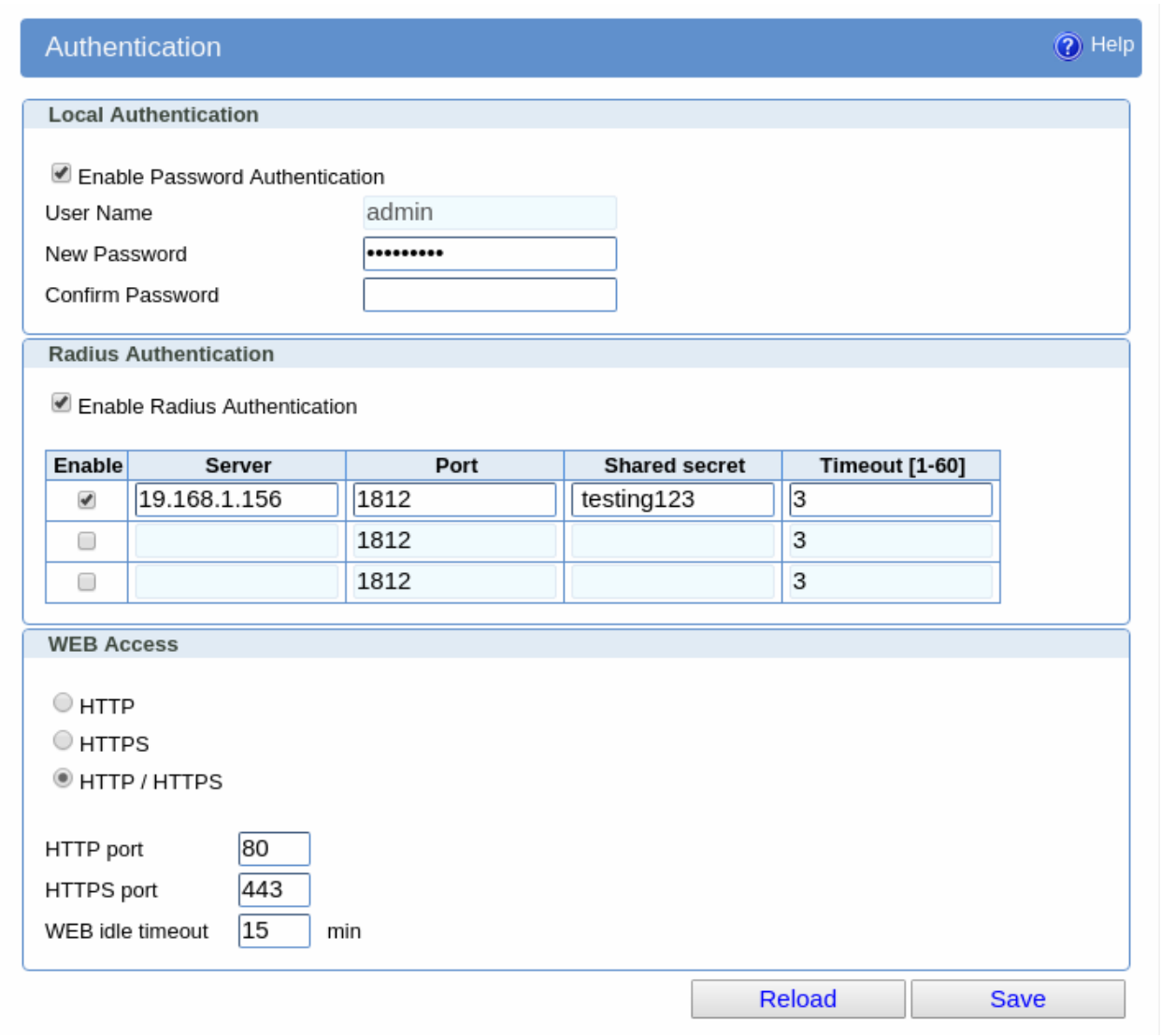


Figure 54 – Router Management configuration page

Administrator Password	
Label	**Description**
Enable Password Authentication	By this check box you can activate or deactivate function for local (passwd) authentication when you access to web/console application.
Username	This field specifies Username for user (administrator) login purpose.
New Password	Enter a new password for GWR Router. Your password must have 20 or fewer characters and cannot contain any space.
Confirm Password	Re–enter the new password to confirm it.
Enable Radius Authentication	By this check box you can activate or deactivate function for authentication via remote radius server.
Enable	Enable or disable usage of this radius server.

Server	Enter remote radius server IP address or hostname.
Port	Enter remote radius server port
Shared secret	Enter remote radius server shared secret.
Timeout	Enter remote radius server timeout in seconds [1-60].
HTTP	Bind HTTP to specified port
HTTPS	Bind HTTPS to specified port
HTTP/HTTPS	Bind HTTP and HTTPS to specified port
WEB GUI idle timeout	WEB session timeout
Save	Click ***Save*** button to save your changes back to the GWR Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 36 – Router Management

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 settings on the GWR Router are done through window Date/Time Settings.

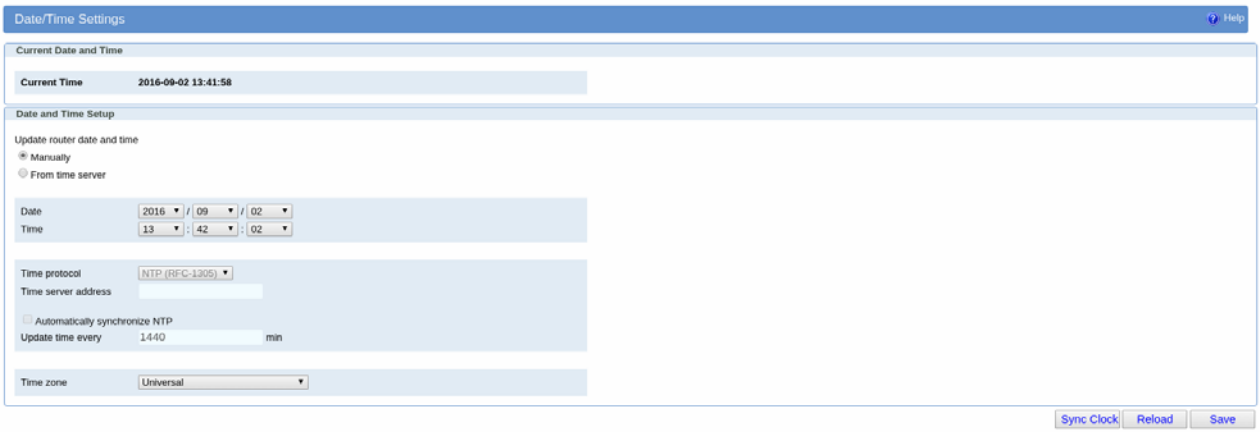


Figure 55 – Date/Time Settings configuration page

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.
Time Protocol	Specify time protocol. Currently only NTP is supported.
Time Server Address	Enter the Hostname or IP address of the NTP server.
Automatically synchronize NTP	Setup automatic synchronization with time server.
Update time every	Time interval for automatic synchronization.

Time Zone	Select your time zone.
Save	Click ***Save*** button to save your changes back to the GWR Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 37 – Date/time parameters

Maintenance – Diagnostics

The GWR 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 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 56 – Diagnostic page

Maintenance – Update Firmware

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

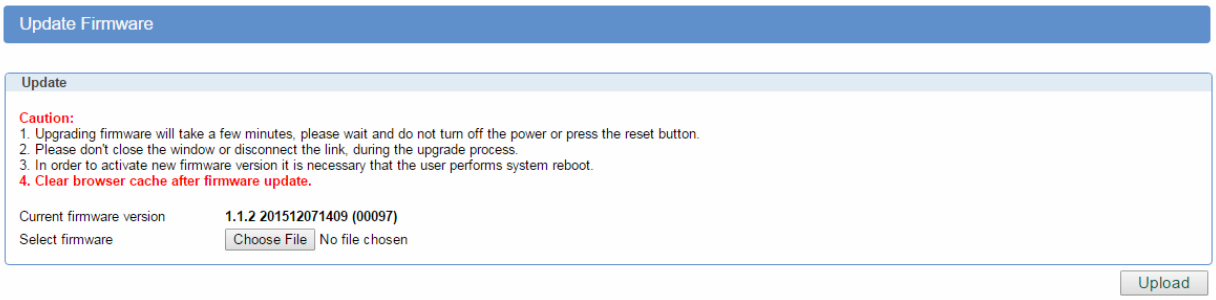


Figure 57 – Update Firmware page

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 not changed and after that the system continues to operate with previous values.

Maintenance – Import/Export Settings

This feature allows you to make a backup file of complete configuration or some part of the configuration on the GWR 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 *Figure 58*. To use the backup file, you need to import the configuration file that you previously exported.

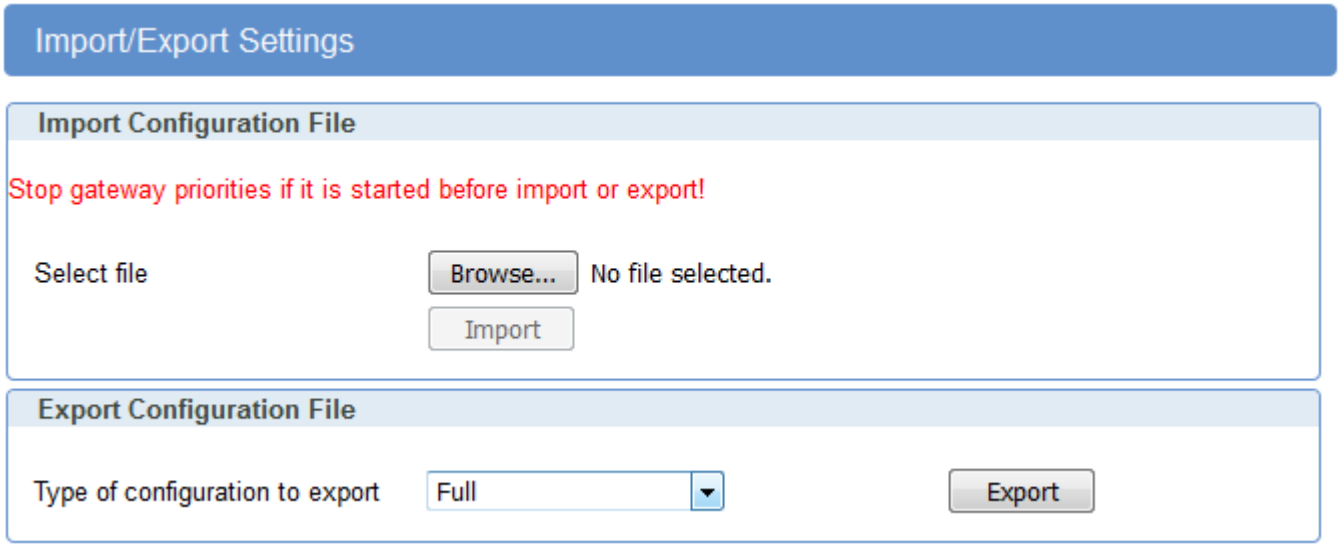


Figure 58 – Export/Import the configuration on the router

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***.

By default, this file will be called ***Configuration.tar.gz.*** This file contains ***confFile.bkg , ripd.conf, cacert and crlcert , keyFile, Iccert, Ickey*** files.

Maintenance – Default Settings

Use this feature to clear all of your configuration information and restore the GWR 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 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.

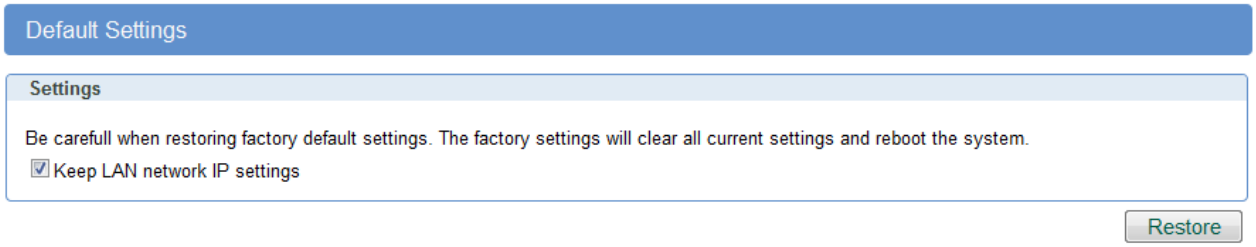


Figure 59 – Default Settings page

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 Router reboot. This does not affect the router's configuration.

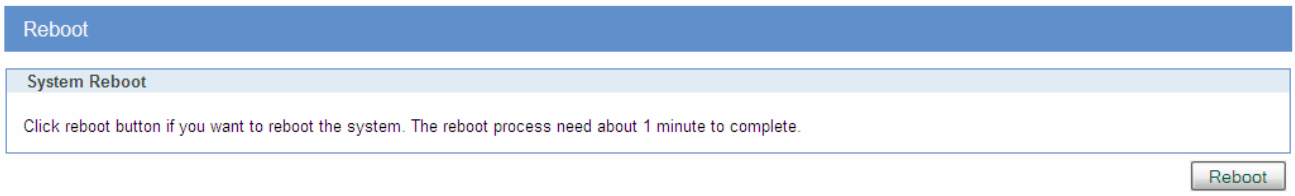


Figure 60 – System Reboot page

Management – Display settings

Display settings on the GWR Router are done through window Display Settings.

Figure 61 – Display Settings

Display Settings	
Label	**Description**
Enable Screen Saver	This field specifies if screen saver is enabled at the Geneko Router.
Timeout	Number between 30-60
IP Address Timeout	Number between 5-10
Save	Click ***Save*** button to save your changes back to the GWR Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 38 – Date/time parameters

Management – Timed Actions

Create a schedule of actions to be performed in a certain time of the day. There is a possibility to add more actions for each day of the week.

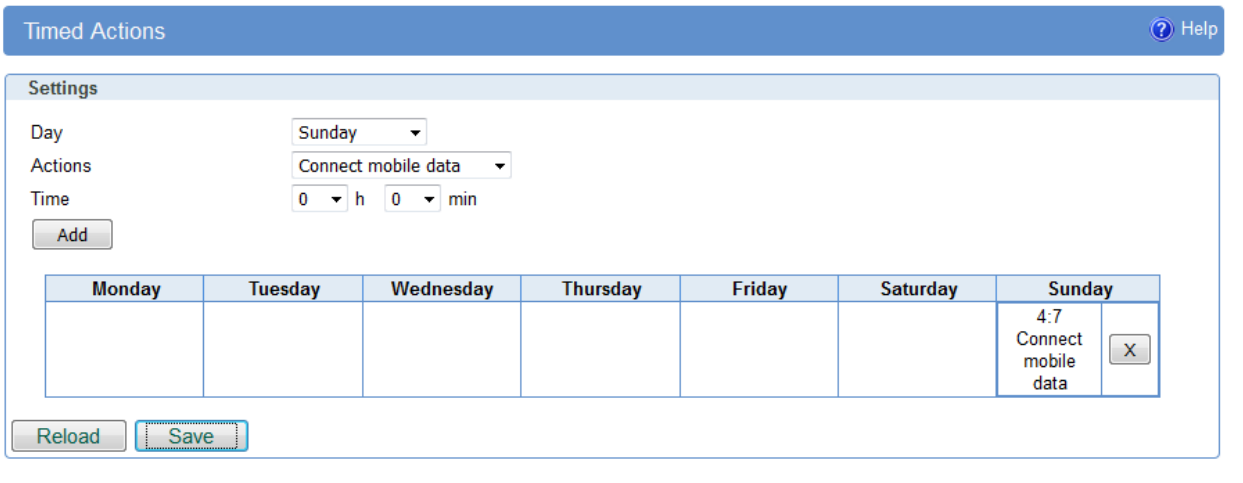


Figure 62 – Timed actions

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 63-Command Line Interface.*

Command Line Interface	
Label	**Description**
CLI Settings	
Enable telnet service	Enable or disable CLI via telnet service. CLI via telnet is disabled by default.
Enable ssh service	Enable or disable CLI via ssh service. CLI via ssh is disabled by default.
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 CLI View mode in minutes. After timeout, session will auto logout.
Admin Mode Timeout	Inactivity timeout for CLI Edit mode in seconds. Note that Username and Password for Edit mode are the same as Web interface login parameters. After timeout, session will auto logout.
Save	Click ***Save*** to save your changes back to the GWR Router.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 39 – Command Line Interface parameters

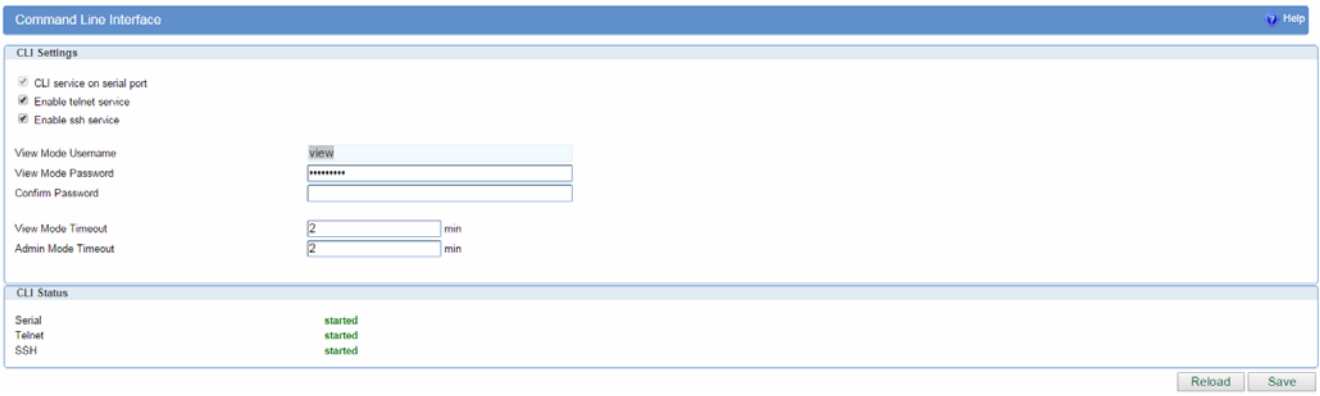


Figure 63 – Command Line Interface

CLI status: Serial started, Telnet stopped, SSH stopped is state by the default, when the router is turned on.

Management – Remote Management

Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of GWR routers. In order to use this utility user has to enable Remote Management on the router.

Figure 64 – Remote Management

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

Table 40 – 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 on *Figure 65*.

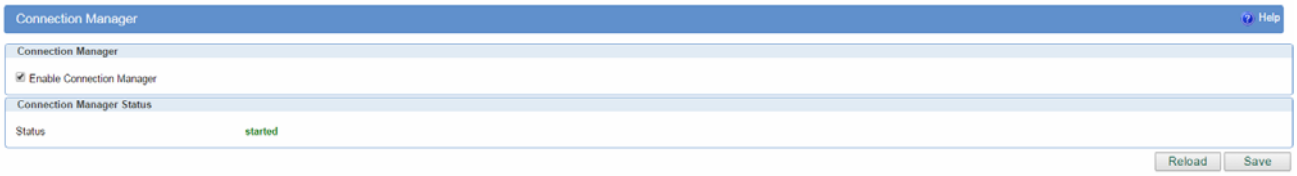


Figure 65 – Connection Manager

Getting started with the Connection Wizard

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

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

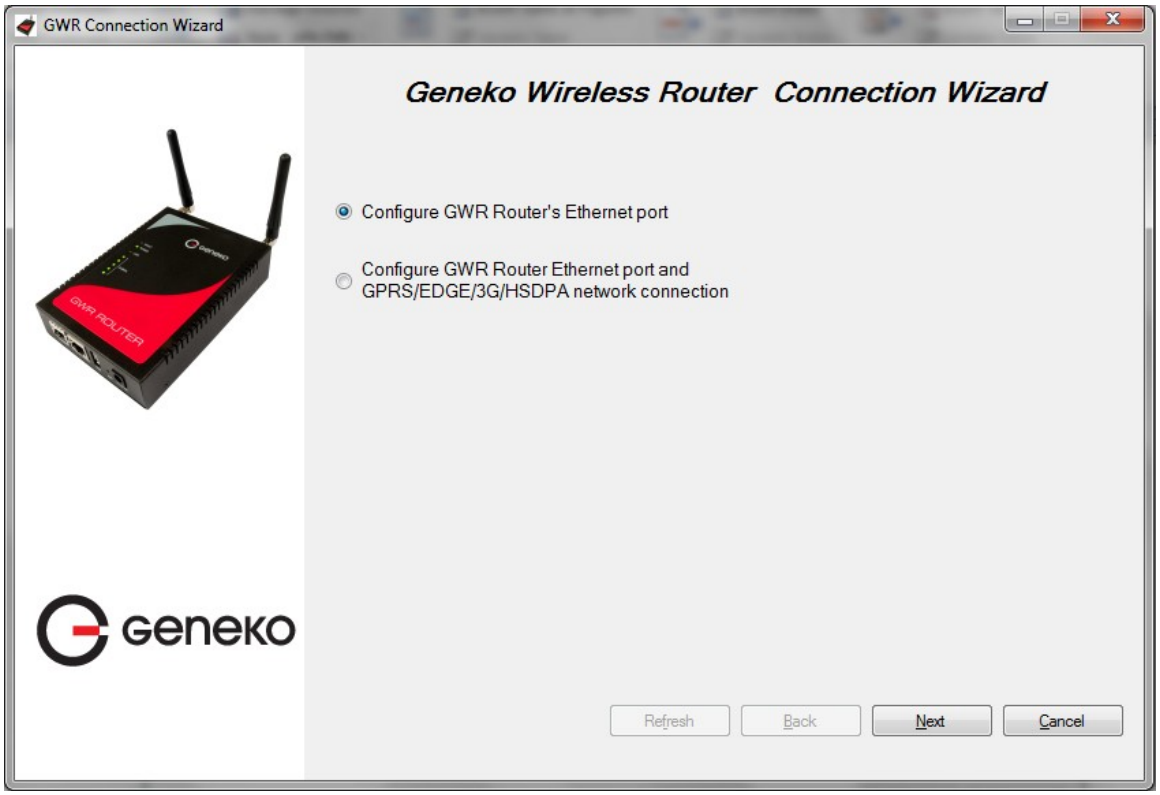


Figure 66 – Connection Wizard – Initial Step

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).

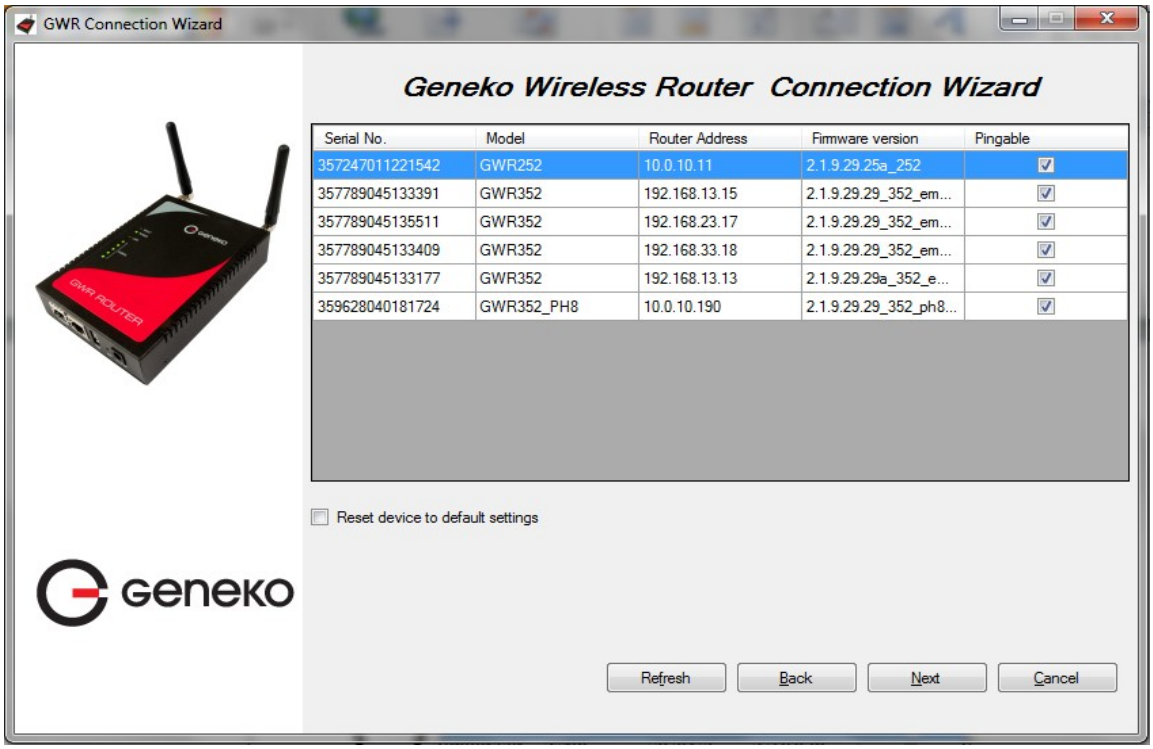


Figure 67 – Connection Wizard – Router Detection

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

Figure 68 – 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 69 – 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 (Simple Network Management Protocol) is a network protocol that provides network administrators with the ability to monitor the status of the Geneko 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.

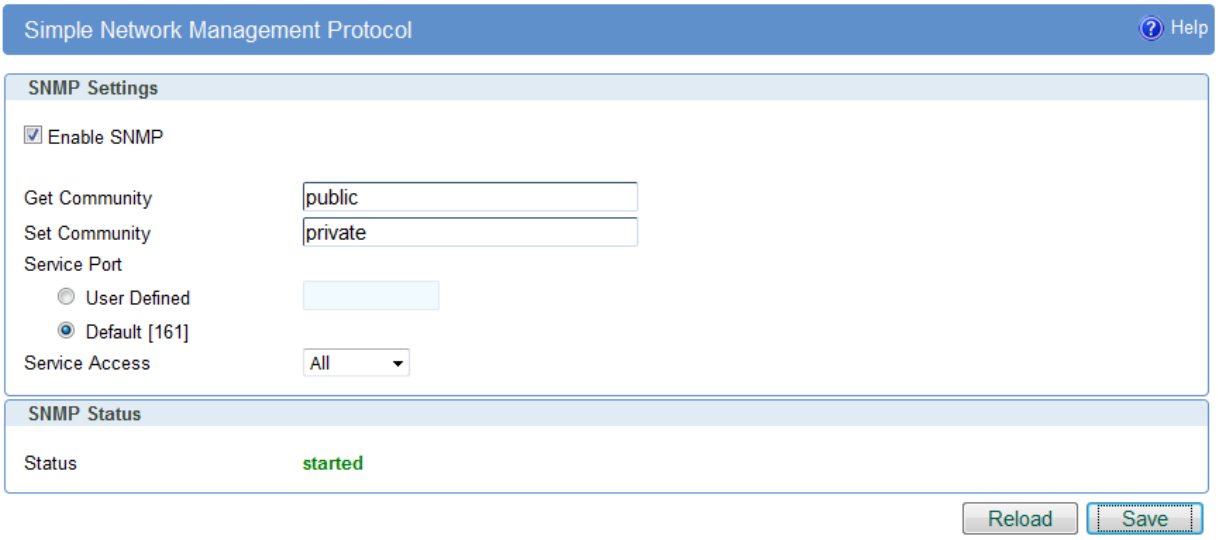


Figure 70 – SNMP configuration page

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.
Set Community	Create the name for a group or community of administrators who can view SNMP data and send SET commands via SNPM. The default is private. It supports up to 64 alphanumeric characters.
Service Port	Sets the port on which SNMP data will be sent/received. 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 all interfaces.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR Router and enable/disable SNMP.

Table 41 – SNMP parameters

Examples of commands:

```
marijana@marijana-VirtualBox:~$ snmpget -v2c -c public  192.168.1.1 .1.3.6.1.4.1
.41581.1.1.1.0
iso.3.6.1.4.1.41581.1.1.1.0 = INTEGER: -79
marijana@marijana-VirtualBox:~$
```

Figure 71 – SNMP get command

```
marijana@marijana-VirtualBox:~$ snmpget -v2c -c public  192.168.1.1 .1.3.6.1.4.1
.41581.1.1.1.0
iso.3.6.1.4.1.41581.1.1.1.0 = INTEGER: -79
marijana@marijana-VirtualBox:~$
```

Figure 72 – SNMP set command

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.

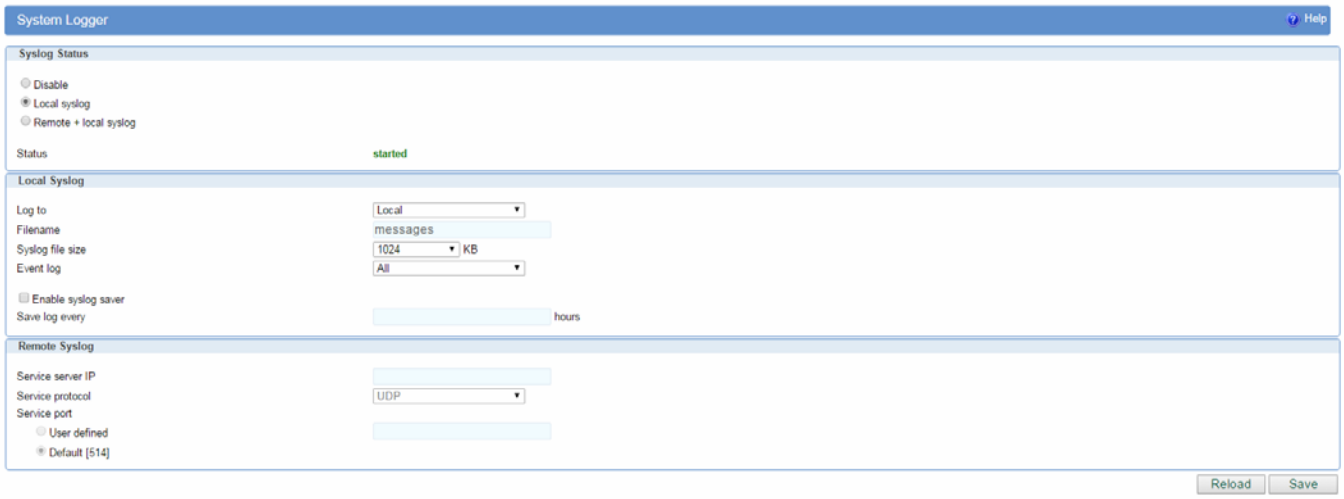


Figure 73 – Syslog configuration page

The GWR 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.
Local syslog	Mark this option in order to enable Local syslog feature.
Remote + local syslog	Mark this option in order to enable remote and local syslog feature
Log to	Set router syslog storage to the router's internal buffer(local) or external to the USB flash. If you choose USB flash, drive must be formatted using the FAT32 file system.

Syslog file size	Set log size on one of the six predefined values. [10 / 20 / 50 / 128 / 256 / 512 / 1024]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 file system.
Save log every	Set time duration between two saves.
Service server IP	The Geneko 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 protocol	Sets the protocol type.
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.
Reload	Click Reload to discard any changes and reload previous settings
Save	Click ***Save*** button to save your changes back to the GWR Router and enable/disable Syslog.

Table 42 – 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 exit the web–based utility, you will need to re–enter your Username and Password to log in and then manage the Router.)

CHROOT

A chroot environment is an operating system call that will change the root location temporarily to a new folder. Chroot runs a command or an interactive shell from another directory, and treats that directory as root. Only a privileged process and root user can use chroot command.

Use Putty, Secure CRT and etc. on Windows, or Putty, GTK on Linux for connection over serial RS-232 port or SSH over LAN port.

For example: Use SSH to enter in global configuration mode.

SSH 192.168.1.1 // SSH to br0 at TCP port 22 //

Login as: **admin**
admin@192.168.1.1's password: **admin**
admin@geneko> gwr_chroot

Press TAB twice quickly to see all commands which are available.
The list of possibilities is:

!	dirs	interfaces-up	ping6	tee
./	disown	ip	popd	telnet
:	dmesg	ipcalc	pppstats	test
JSON.sh	do	ipsec	printf	tftp
[	done	ipsec-mode	ps	tftpd
[[	du	ipsec-routes	pushd	then
]]	ebtables	ipsec-sa-status	pwd	time
alias	echo	ipsec-status	read	times
ar	egrep	iptables-view	readarray	top
arping	elif	jobs	readlink	touch
awk	else	json2lua	readonly	tr
basename	enable	kill	realpath	traceroute
bash	env	killall	reboot	trap
bg	esac	ldd	return	true
bind	eval	less	rip-ripd-conf	tty
break	exec	let	rip-zebra-conf	type
builtin	exit	ln	rm	typeset
bunzip2	export	local	route	udpsvd
busybox	expr	local_dns	run-parts	ulimit
bzcat	factory_default	logger	scp	umask
cal	false	logname	sed	unalias
caller	fc	logout	select	uname
case	fg	ls	send_at_command	uniq
cat	fgrep	lsof	seq	unset
cd	fi	lua	service	until
chattr	find	luac	set	unzip
chmod	flock	mapfile	sh	upfirmware
clear	for	md5sum	shift	uptime
cmp	free	microcosm	shopt	users
command	ftpd	mkdir	show	usleep
compgen	function	mkfifo	sleep	vi
complete	fuser	mobile-activity	sms_send	wait
compopt	getopts	modem_info	snmp-view	wc
configuration_export	grep	modem_state	sort	wget
configuration_import	gunzip	more	source	which
configuration_show	gzip	mv	ssh	while
continue	hash	nc	strace	who
coproc	head	ncftp	strings	whoami
cp	help	netstat	stty	xargs
cpu	hexdump	nohup	su	xtables-multi
cut	history	nslookup	suspend	yes
date	hostname	ntpdate	syslog_export	zcat
dc	hwclock	od	syslog_start	{
dd	id	openvt	syslog_start+view	}
declare	if	passwd	syslog_stop	
df	ifconfig	perl	tail	
diff	in	pidof	tar	
dirname	interfaces-all	ping	tcpsvd	

Configuration Examples

GWR Router as Internet Router

The GWR 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 Router. The GWR Router uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside world. All outgoing traffic uses the GWR Router mobile IP address.

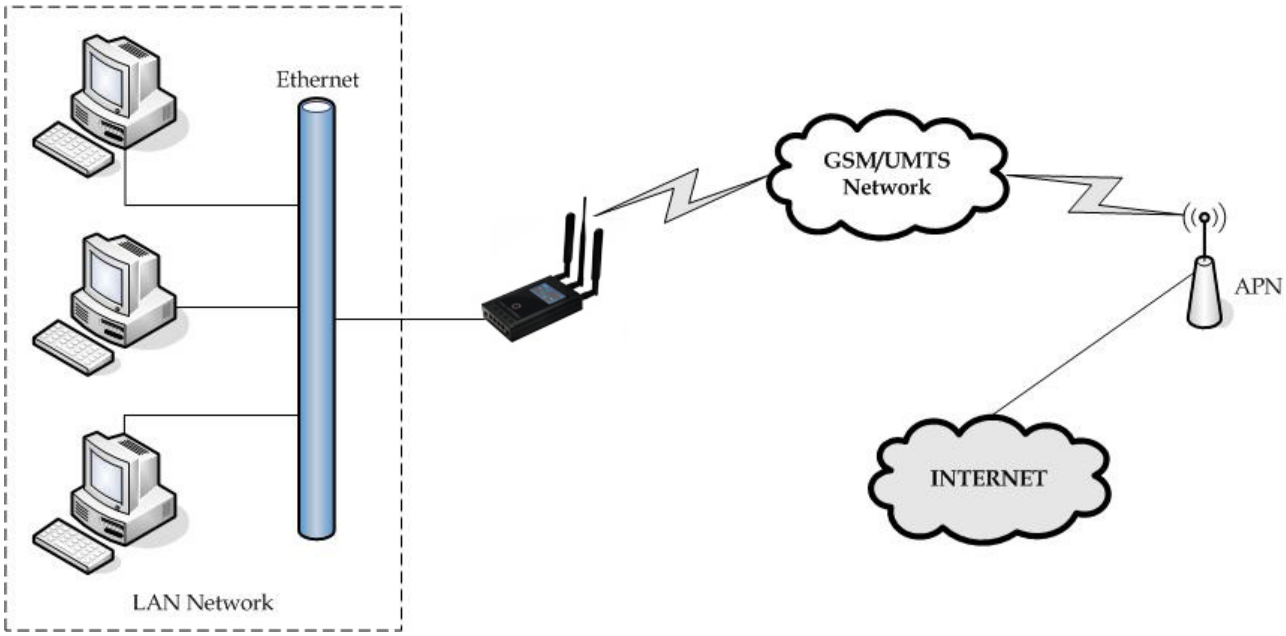


Figure 74 – GWR Router as Internet router

- Click ***LAN Port*** Tab, to open the **LAN Port Settings** 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 ***Mobile 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 (***Mobile 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 add default route via *ppp0* interface.
- Optionally configure IP Filtering to block any unwanted incoming traffic.
- Configure the GWR 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 Routers

GRE tunnel is a type of a VPN tunnel, but it is not a secure tunneling method. Simple network with two GWR Routers is illustrated on the diagram below (Figure 75). Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

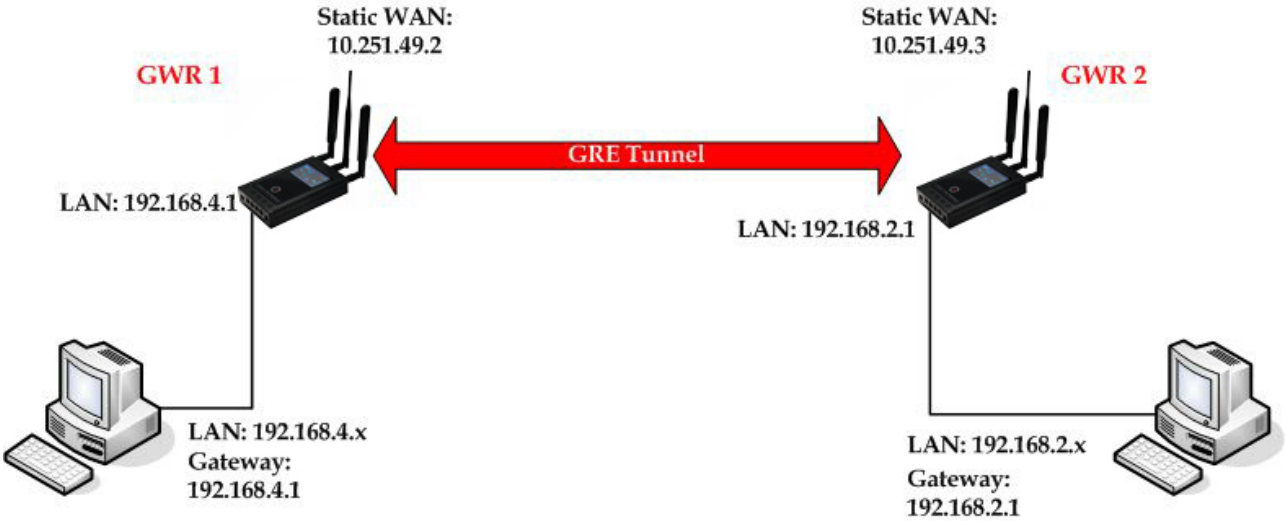


Figure 75 – GRE tunnel between two GWR Routers

The GWR 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 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 Router 1 configuration:

- Click ***LAN Ports***, to open the **LAN Port Settings** 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.

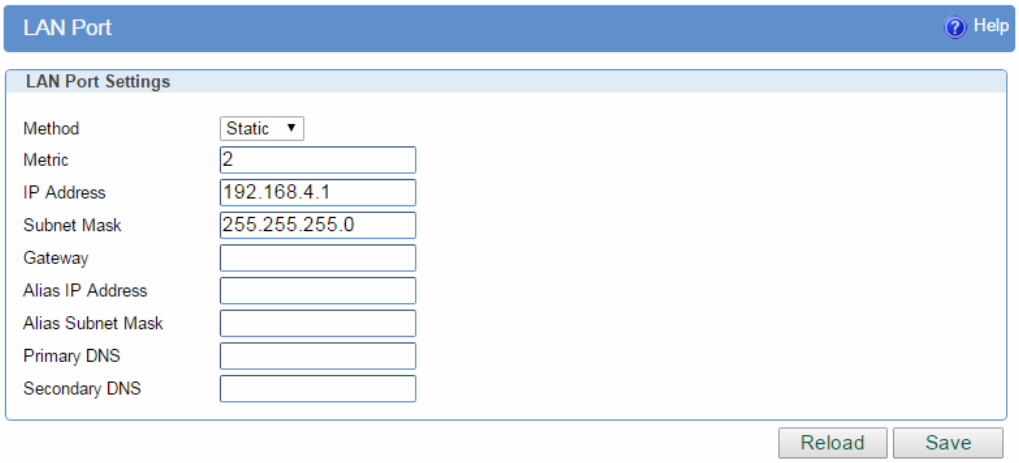


Figure 76 – Network configuration page for GWR Router 1

- 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 ***Mobile 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 (***Mobile 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: 1. 10.251.49.2 (obtained by the network provider)
    2. Select HOST from drop down menu if you want to use host name as peer identifier
  - Tunnel Destination: 1. 10.251.49.3 (obtained by the network provider)
    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.

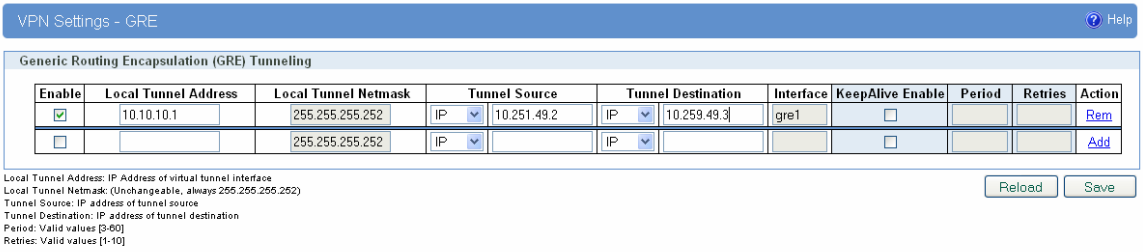


Figure 77 – GRE configuration page for GWR Router 1

- Click **Static Routes** on **Routing** Tab to configure GRE Route. Parameters for this example are:

- Destination Network: 192.168.2.0,
- Netmask: 255.255.255.0,
- Interface: gre_x.

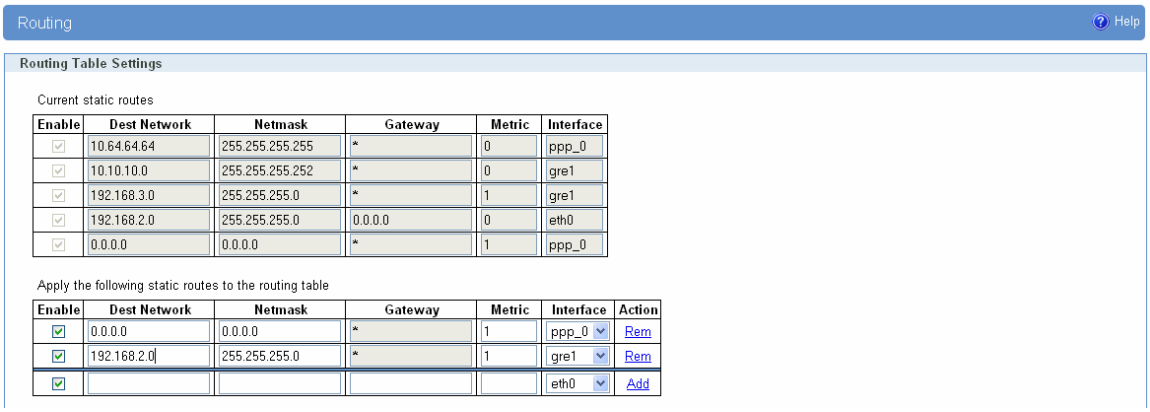


Figure 78 – Routing configuration page for GWR Router 1

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

The GWR Router 2 configuration:

- Click ***LAN Ports*** Tab, to open the **LAN Ports Settings** 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.

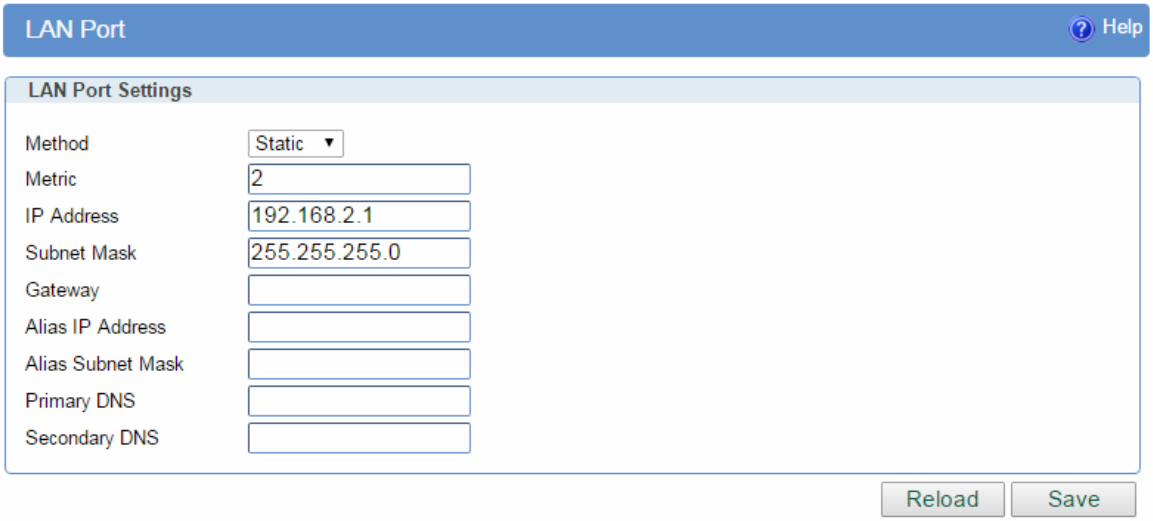


Figure 79 – Network configuration page for GWR Router 2

- 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/LTE provider's network default gateway).
- Click ***Mobile 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 (***Mobile 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: 1. 10.251.49.3 (obtained by the network provider)
    2. Select HOST from drop down menu if you want to use host name as peer identifier
  - Tunnel Destination: 1. 10.251.49.2 (obtained by the network provider)
  - 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.

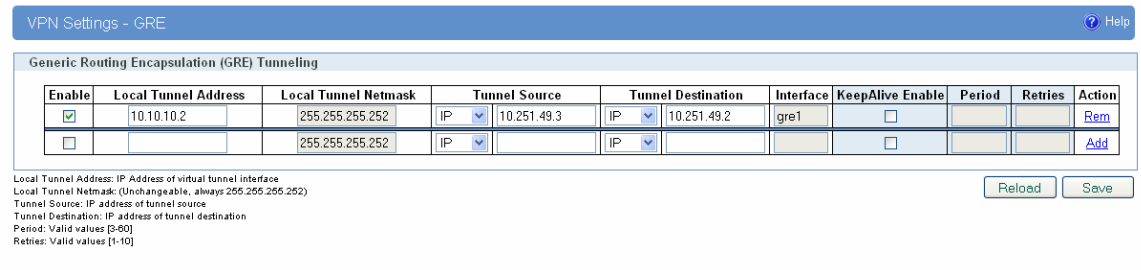


Figure 80 – GRE configuration page for GWR Router 2

- Configure GRE Route. Click ***Static Routes*** on ***Routing*** Tab. Parameters for this example are:
  - Destination Network: 192.168.4.0,
  - Netmask: 255.255.255.0.
  - Interface: gre_x.

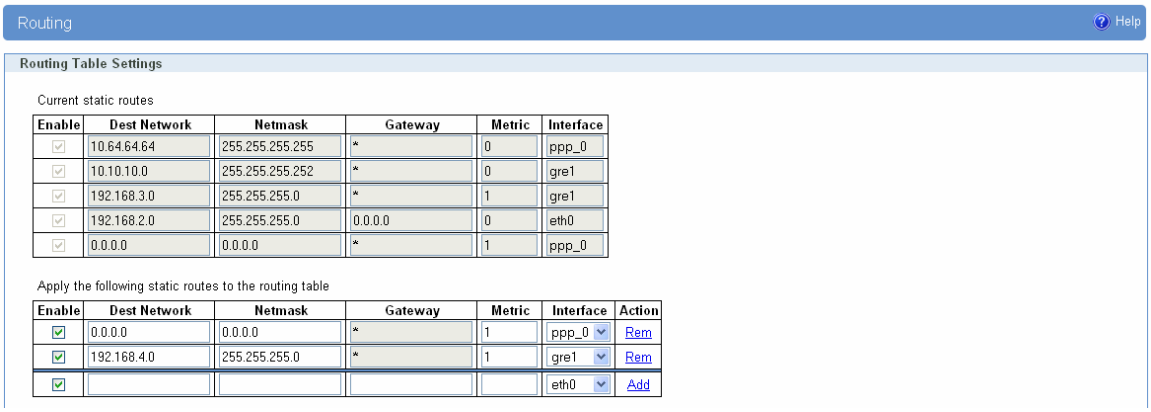


Figure 81 – Routing configuration page for GWR Router 2

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

GRE Tunnel configuration between GWR 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 82*) is illustrated simple network with two sites. Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

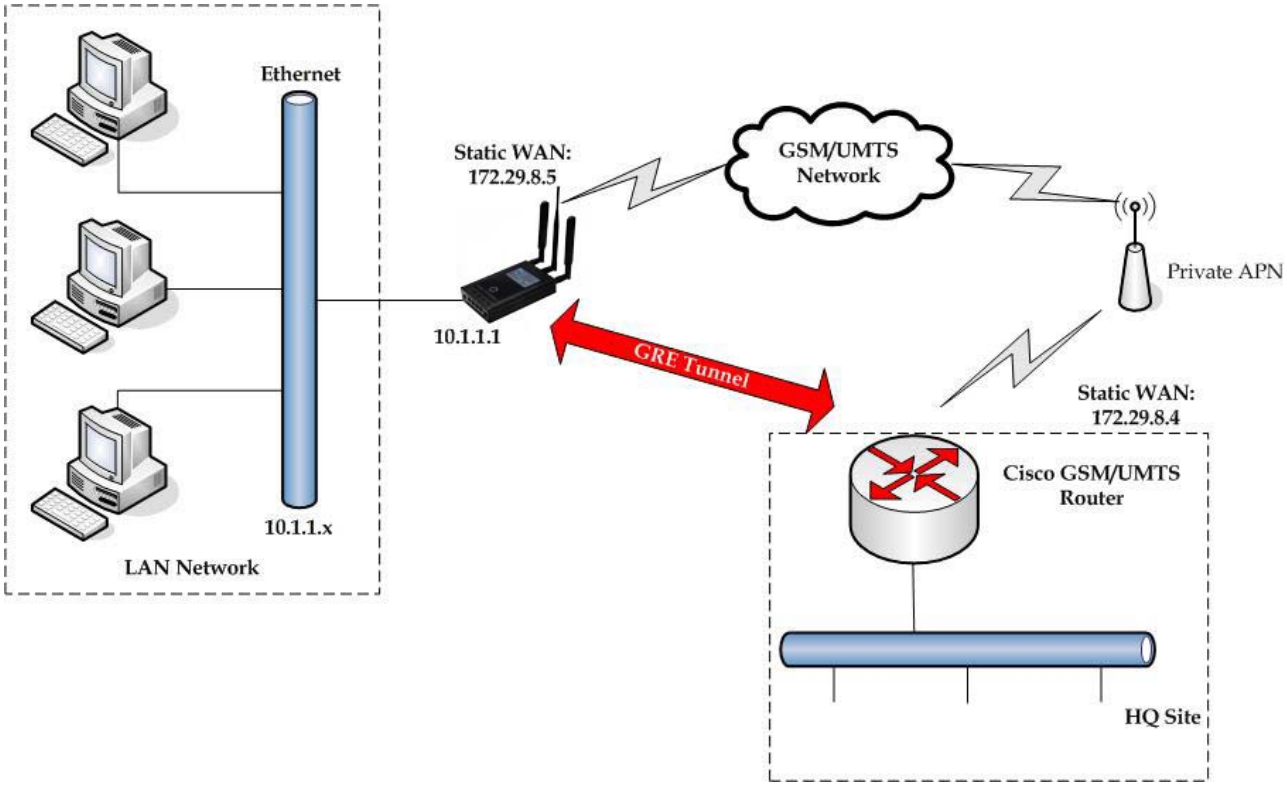


Figure 82 – GRE tunnel between Cisco router and GWR Router

GRE tunnel is created between Cisco router with GRE functionality on the HQ Site and the GWR 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 Router uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside. All outgoing traffic uses the GWR 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 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 has to support GRE protocol,
   - Tunnel peer address will be the GWR Router WAN's mobile IP address. For this reason, a static mobile IP address is preferred on the GWR Router WAN (GPRS) side,
   - Remote Subnet is remote LAN network address and Remote Subnet Mask is subnet of remote LAN.

2. The GWR 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 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 10.10.10.2 255.255.255.252
tunnel source FastEthernet0/0
tunnel destination 172.29.8.5

ip route 10.1.1.0 255.255.255.0 tunnel0

Command for tunnel status: show ip interface brief
```

The GWR Router Sample Configuration:

- Click ***LAN Ports*** Tab, to open the **LAN Port Settings** 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 83 – LAN Port 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 ***Mobile 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 (***Mobile Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings*** > ***GRE Tunneling*** to configure new VPN tunnel parameters:

- Enable: yes,
- Local Tunnel Address: 10.10.10.1,
- 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.

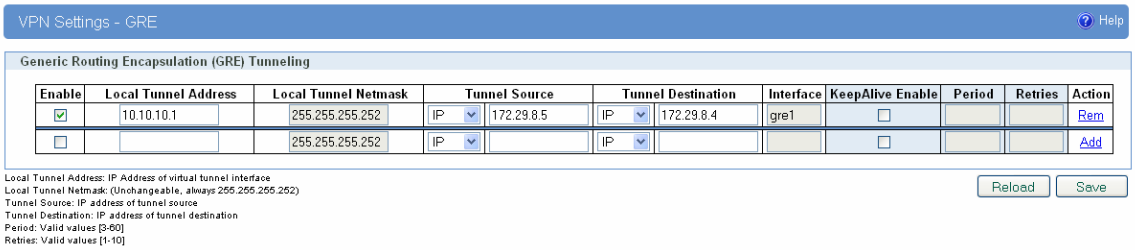


Figure 84 – GRE configuration page

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

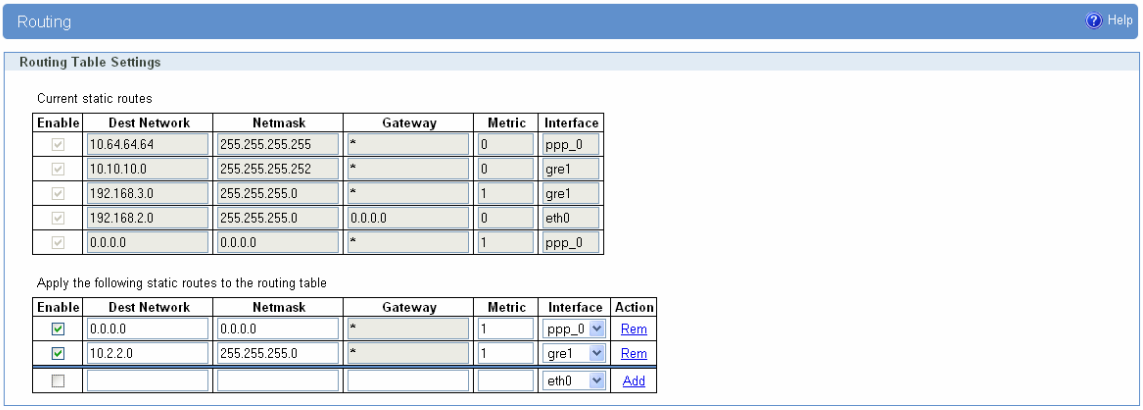


Figure 85 – Routing configuration page

- 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 Routers

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. Simple network with two GWR Routers is illustrated on the diagram below (*Figure 86)*. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

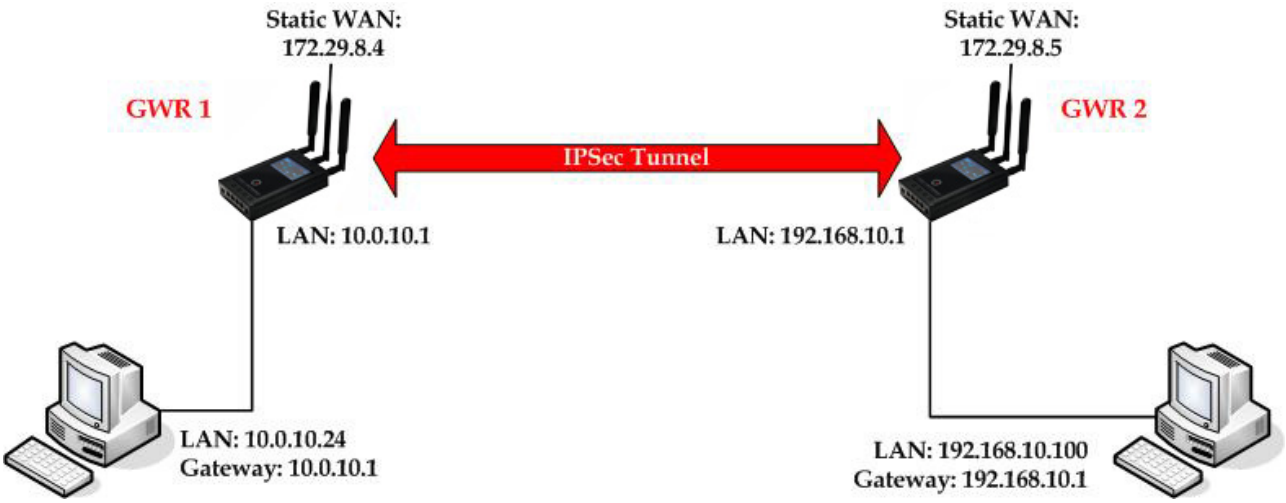


Figure 86 – IPSec tunnel between two GWR Routers

The GWR 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 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* 86 will be used for both scenarios.

#Example

Router 1 and Router 2, have firmware version that provides two modes of negotiation in IPSec tunnel configuration process:

- Aggressive
- Main

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

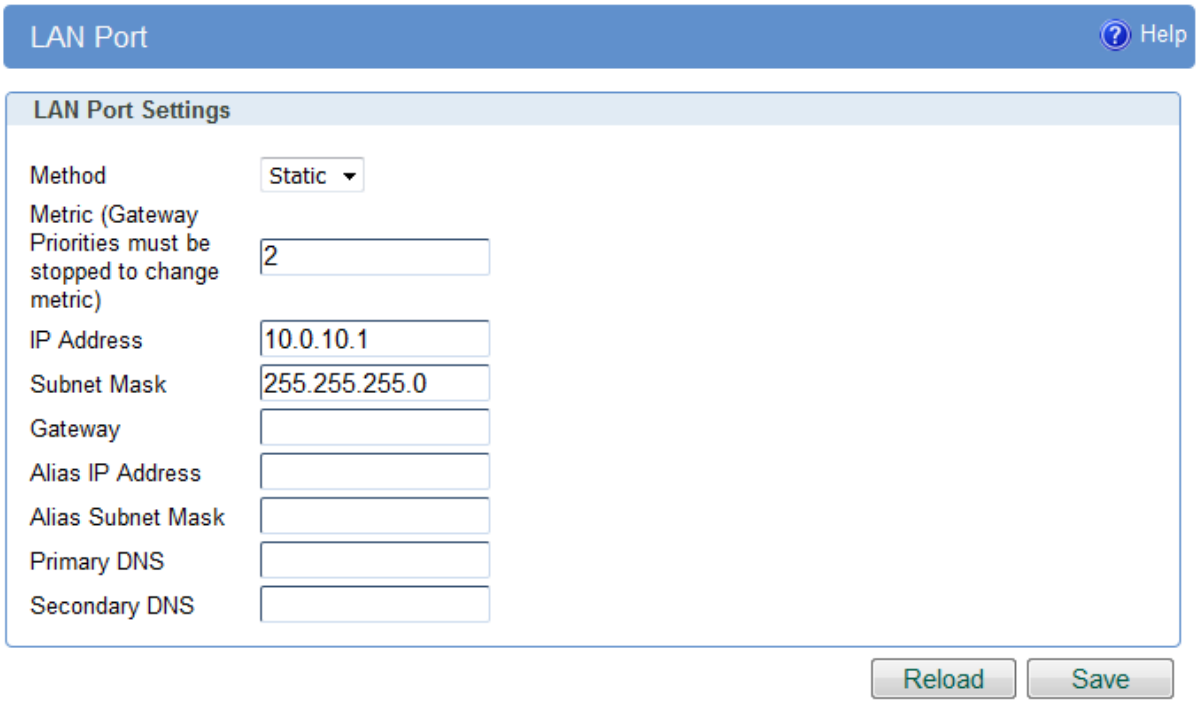


Figure 87 – LAN Port configuration page for GWR Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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: IPsec tunnel,
    - Enable: true,
  - ***Local Group Setup***

    - Local Security Gateway Type:WAN
    - 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: 192.168.10.0
    - Subnet Mask 255.255.255.0

- ***IPSec Setup***
    - Key Exchange Mode: IKE with X509 certificates and PSK,
    - Mode: main,
    - Phase 1 DH group: Group2 (1024),
    - Phase 1 Encryption: 3DES,
    - Phase 1 Authentication: MD5,
    - Phase 1 SA Life Time: 28800,
    - Perfect Forward Secrecy:
    - Phase 2 DH group: Group 2,
    - Phase 2 Encryption: 3DES,
    - Phase 2 Authentication: MD5,
    - Phase 2 SA Life Time: 3600,
    - Preshared Key: genekokey
    - CA certificate: ca.crt
    - Local Client Certificate: client1.crt
    - Local Client Key: client1.key
- ***Failover***
    - 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.

Device 2 Device Tunnel — Help

Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko
Enable	☑

Local Group Setup

Local Security Gateway Type	WAN
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	Subnet
IP Address	192.168.10.0
Subnet Mask	255.255.255.0

Figure 88 – IPSEC configuration page I for GWR Router 1

IPSec Setup

Key Exchange Mode	IKE with X509 certificates and PSK
Mode	main
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	3DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	☐
Phase 2 Encryption	3DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600 sec
Preshared Key	genekokey
CA certificate	ca.crt
Local Client Certificate	client1.crt
Local Client Key	client1.key

Figure 89 – IPSec configuration page II for GWR Router 1

NOTE : Options NAT Traversal and Send Initial Contact are predefined

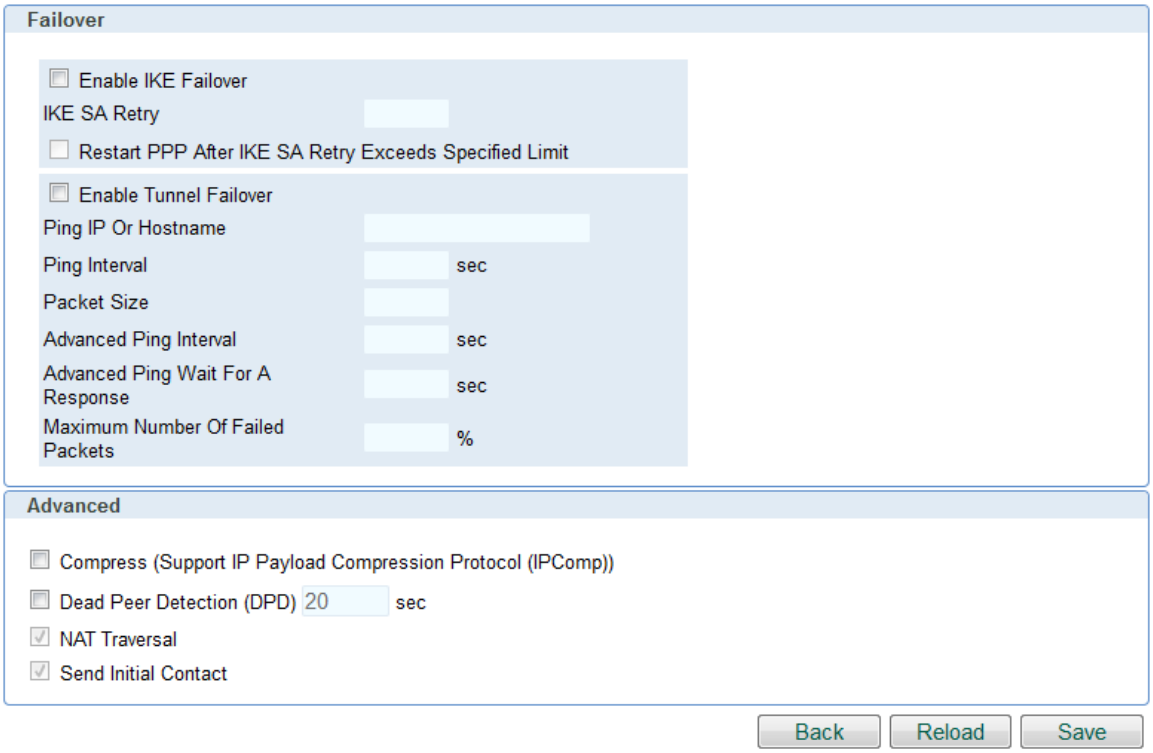


Figure 90 – IPSec configuration page III for GWR Router 1

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

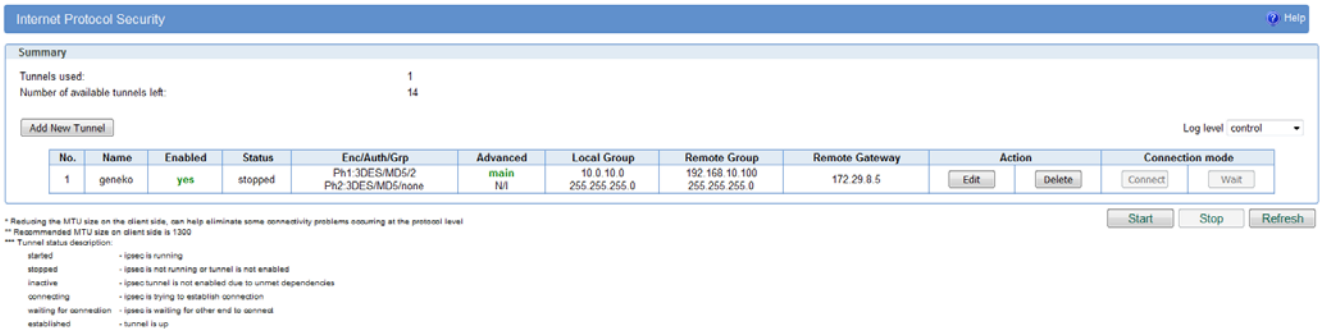


Figure 91 – IPSec start/stop page for GWR Router 1

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

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

The GWR Router 2 configuration:

- Click ***LAN Ports*** Tab, to open the **LAN Ports Settings** 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.

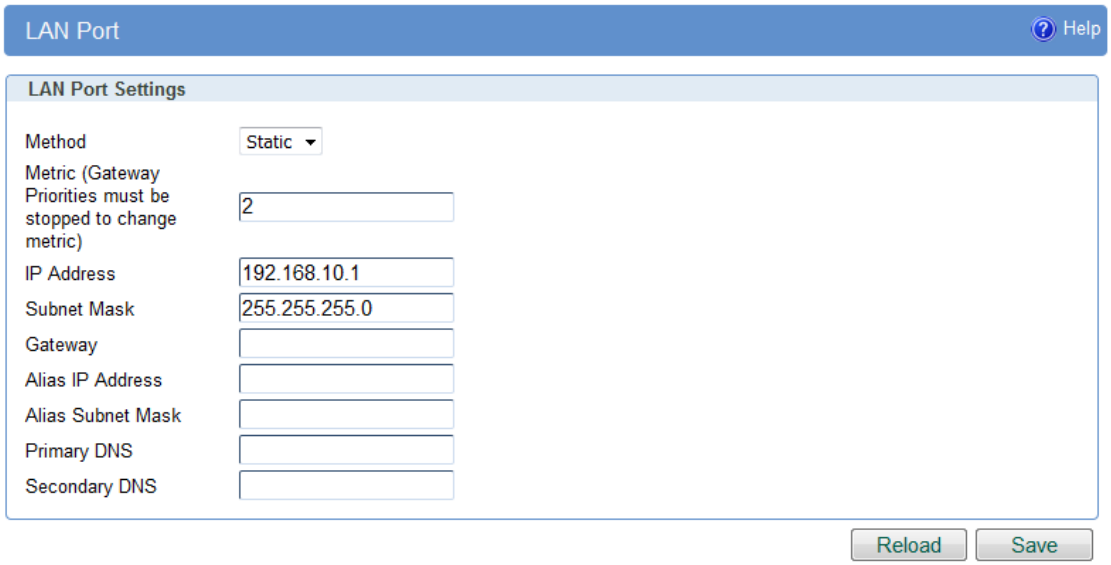


Figure 92 – Network configuration page for GWR Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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: geneko
    - Enable: true.
  - ***Local Group Setup***
    - Local Security Gateway Type: WAN
    - 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: 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
  - ***IPSec Setup***
    - Keying IKE with X509 certificates and PSK
    - Mode: main
    - Phase 1 DH group: Group 2 (1024)

- Phase 1 Encryption: 3DES
- Phase 1 Authentication: MD5
- Phase 1 SA Life Time: 28800
- Perfect Forward Secrecy: false
- Phase 2 Encryption: 3DES
- Phase 2 Authentication: MD5
- Phase 2 SA Life Time: 3600
- Preshared Key: genekokey
- CA certificate: ca.crt
- Local Client Certificate: client1.crt
- Local Client Key: client1.key

- ***Failover***
  - 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.

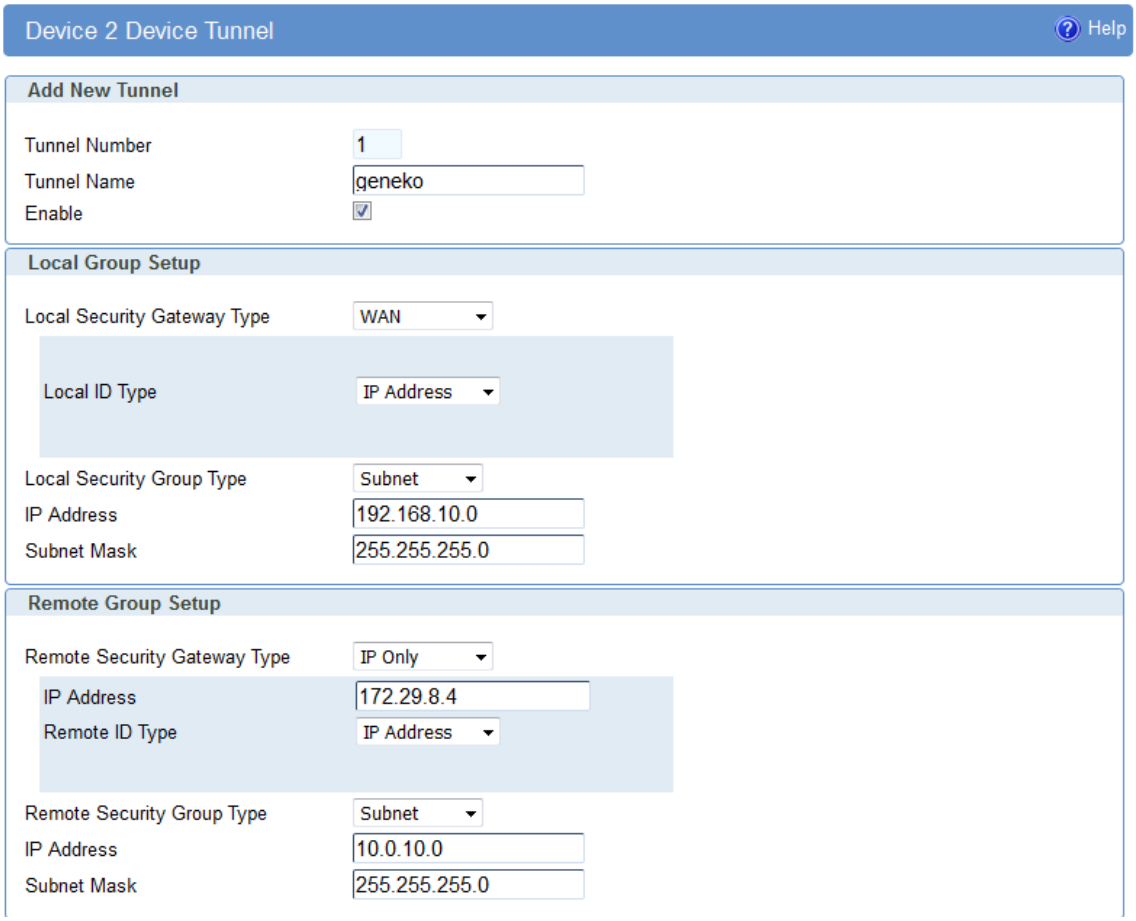


Figure 93 – IPSEC configuration page I for GWR Router 2

IPSec Setup

Key Exchange Mode	IKE with X509 certificates and PSK
Mode	main
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	3DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	
Phase 2 Encryption	3DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600 sec
Preshared Key	genekokey
CA certificate	ca.crt
Local Client Certificate	client1.crt
Local Client Key	client1.key

Figure 94 – IPSec configuration page II for GWR Router 2

NOTE : Options NAT Traversal and Send Initial Contact are predefined.

Failover

Enable IKE Failover	
IKE SA Retry	
Restart PPP After IKE SA Retry Exceeds Specified Limit	
Enable Tunnel Failover	
Ping IP Or Hostname	
Ping Interval	sec
Packet Size	
Advanced Ping Interval	sec
Advanced Ping Wait For A Response	sec
Maximum Number Of Failed Packets	%

Advanced

- Compress (Support IP Payload Compression Protocol (IPComp))
- Dead Peer Detection (DPD) 20 sec
- NAT Traversal
- Send Initial Contact

Back Reload Save

Figure 95 – IPSec configuration page III for GWR Router 2

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

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.

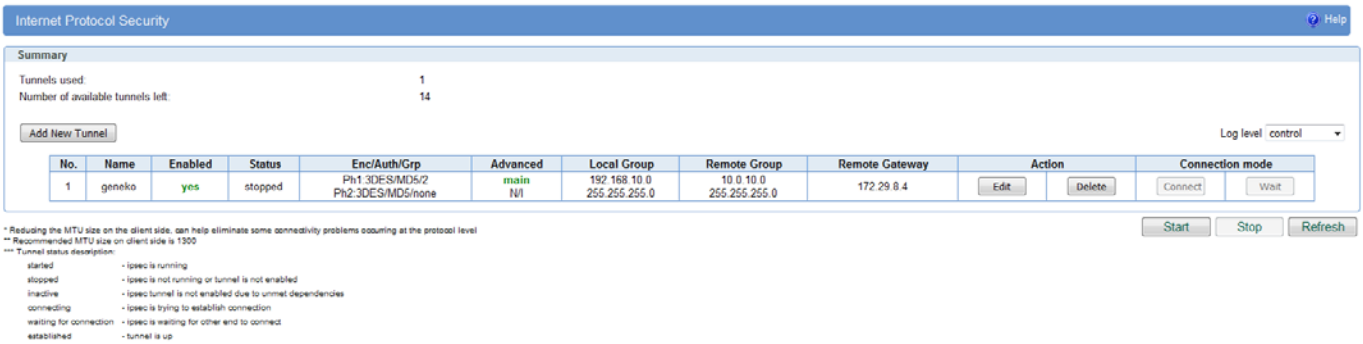


Figure 96 – IPSec start/stop page for GWR Router 2

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

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

IPSec Tunnel configuration between GWR Router and Cisco Router

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

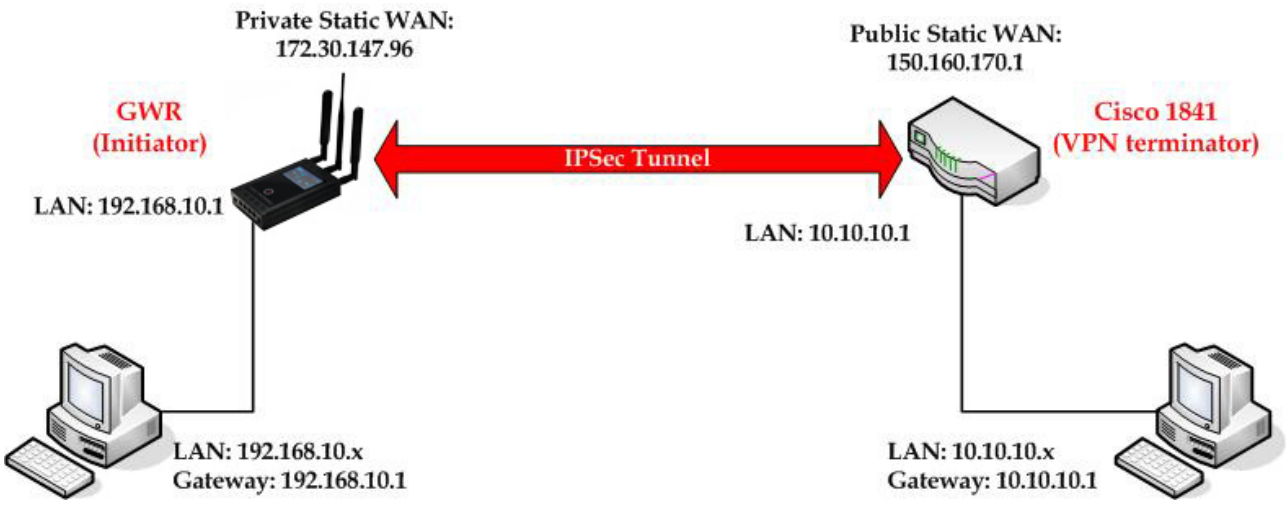


Figure 97 – IPSec tunnel between GWR Router and Cisco Router

The GWR 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 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 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 98 – LAN Port configuration page for GWR Router

- Click ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (***Mobile 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: IPsec tunnel,
        - Enable: true.
    - ***Local Group Setup***
        - Local Security Gateway Type: SIM card,
        - Local ID Type: IP Address,
        - IP Address From: SIM 1 (WAN connection is established over SIM 1),
        - 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.
    - ***IPSec Setup***
        - Keying Mode: IKE with Preshared key,
        - Mode: aggressive,
        - Phase 1 DH group: Group 2,
        - Phase 1 Encryption: 3DES,
        - Phase 1 Authentication: SHA1,
        - Phase 1 SA Life Time: 28800,
        - Phase 2 Encryption: 3DES,
        - Phase 2 Authentication: SHA1,
        - Phase 2 SA Life Time: 3600,
        - Preshared Key: 1234567890.
    - ***Failover***
        - Enable Tunnel Failover: false.
    - ***Advanced***
        - 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.

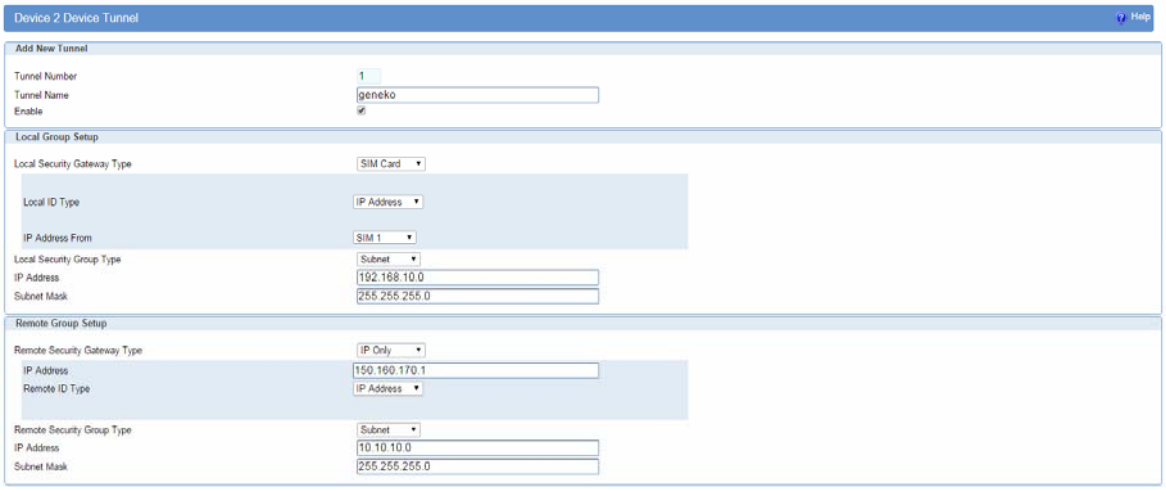


Figure 99 – IPSEC configuration page I for GWR Router

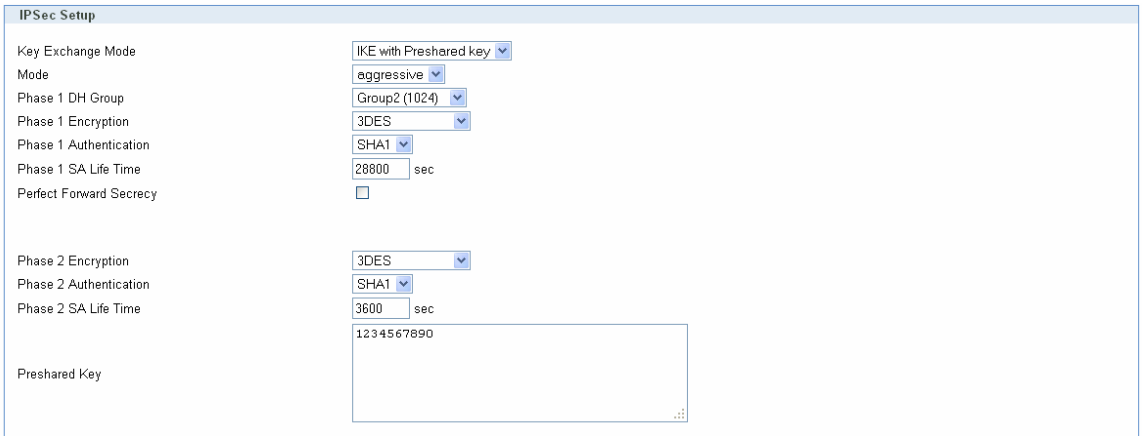


Figure 100 – IPSec configuration page II for GWR Router

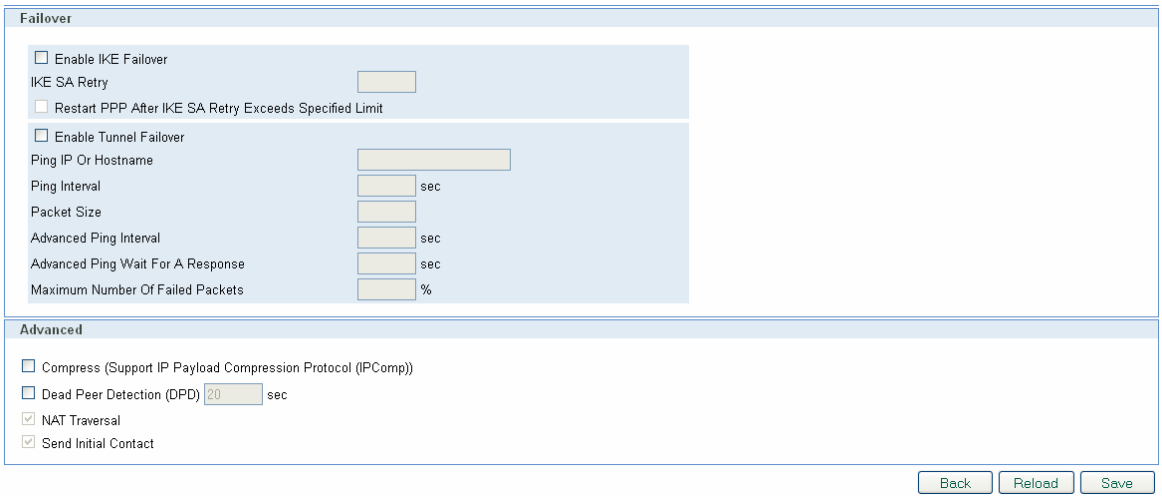


Figure 101 – IPSec configuration page III for GWR Router

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

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

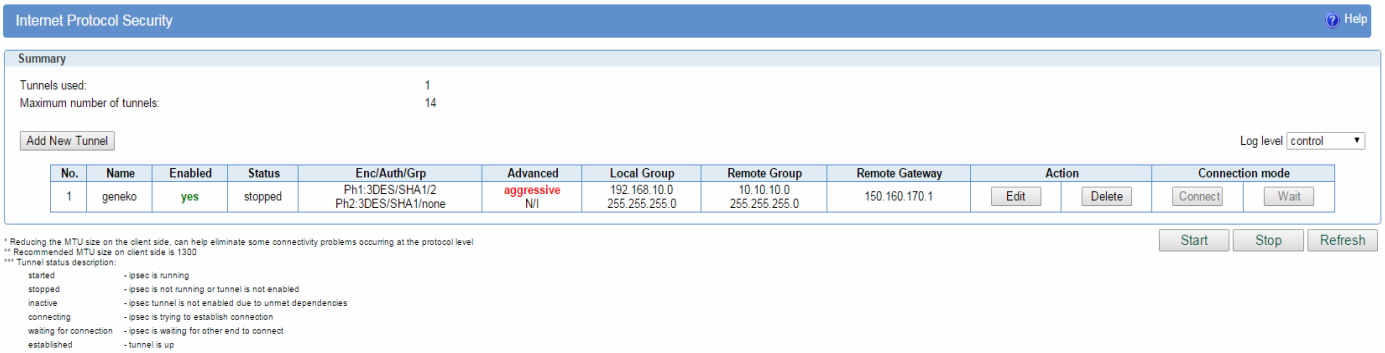


Figure 102 – IPSec start/stop page for GWR Router

- On the device connected on GWR 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
 match address 121
```

```
!
!--- 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 121 permit ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
!
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 Router and Juniper SSG firewall

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. On the diagram below (*Figure 103)* is illustrated simple network with GWR Router and Cisco Router. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

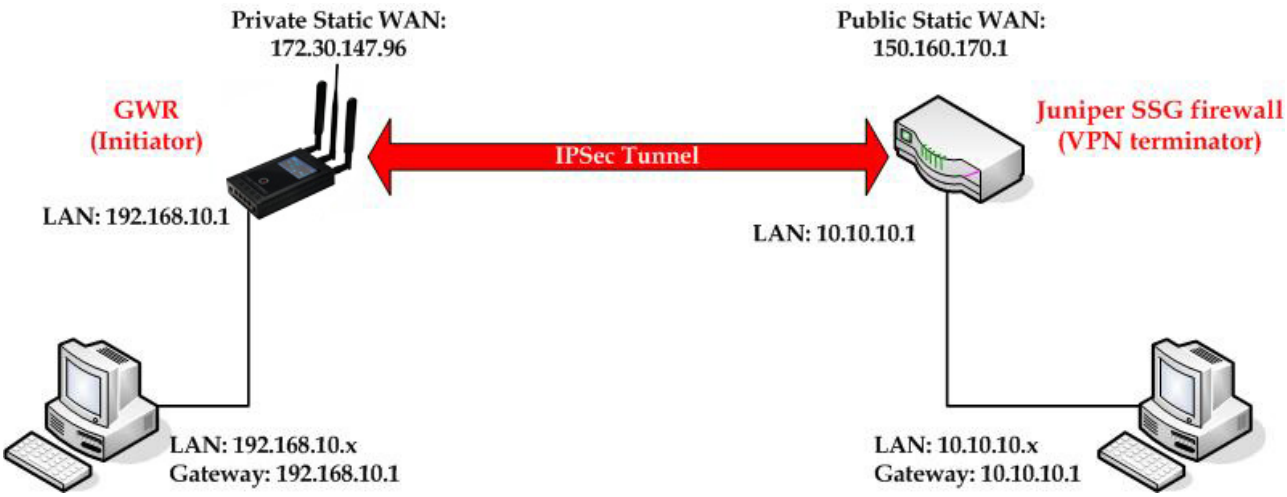


Figure 103 – IPSec tunnel between GWR Router and Juniper SSG firewall

The GWR 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 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 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.

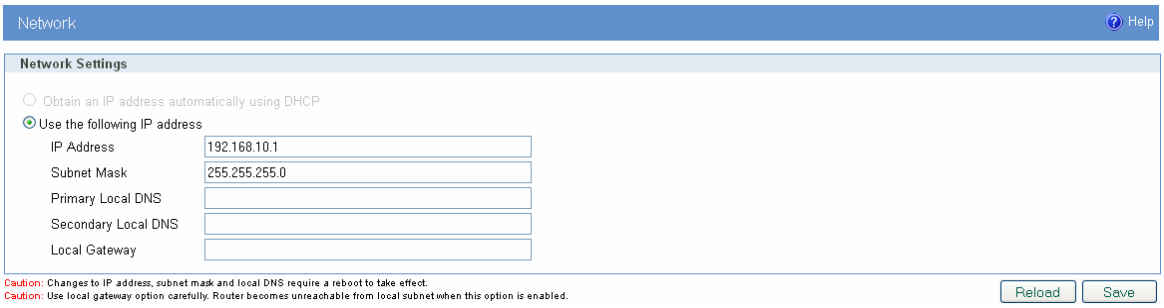


Figure 104 – Network configuration page for GWR Router

- 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: IPsec tunnel,
        - Enable: true.
    - ***IPSec Setup***
        - Keying Mode: IKE with Preshared key,
        - Mode: aggressive,
        - 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.
    - ***Local Group Setup***
        - Local Security Gateway Type: IP Only,
        - Local ID Type: Custom,
        - Custom Peer ID: 172.30.147.96,
        - IP Address: SIM 1,
        - 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.
    - ***Advanced***
        - Compress(Support IP Payload Compression Protocol(IPComp)): false,
        - Dead Peer Detection(DPD): false,
        - NAT Traversal: true,
        - Press ***Save*** to accept the changes.

Device 2 Device Tunnel — Help

Add New Tunnel

Tunnel Number	1
Tunnel Name	IPsec tunnel
Enable	☑

Local Group Setup

Local Security Gateway Type	SIM Card
Local ID Type	Custom
Custom Peer ID	172.30.147.96
IP Address From	SIM 1
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

Figure 105 – IPSec configuration page I for GWR Router

IPSec Setup

Key Exchange Mode	IKE with Preshared key
Mode	aggressive
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	3DES
Phase 1 Authentication	SHA1
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	☑
Phase 2 DH Group	Group2 (1024)
Phase 2 Encryption	3DES
Phase 2 Authentication	SHA1
Phase 2 SA Life Time	3600 sec
Preshared Key	1234567890

Figure 106 – IPSec configuration page II for GWR Router

Failover

☐ Enable IKE Failover	
IKE SA Retry	
☐ Restart PPP After IKE SA Retry Exceeds Specified Limit	
☐ Enable Tunnel Failover	
Ping IP Or Hostname	
Ping Interval	sec
Packet Size	
Advanced Ping Interval	sec
Advanced Ping Wait For A Response	sec
Maximum Number Of Failed Packets	%

Advanced

- ☐ Compress (Support IP Payload Compression Protocol (IPComp))
- ☐ Dead Peer Detection (DPD) 20 sec
- ☑ NAT Traversal
- ☑ Send Initial Contact

Back | Reload | Save

Figure 107 – IPSec configuration page III for GWR Router

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

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

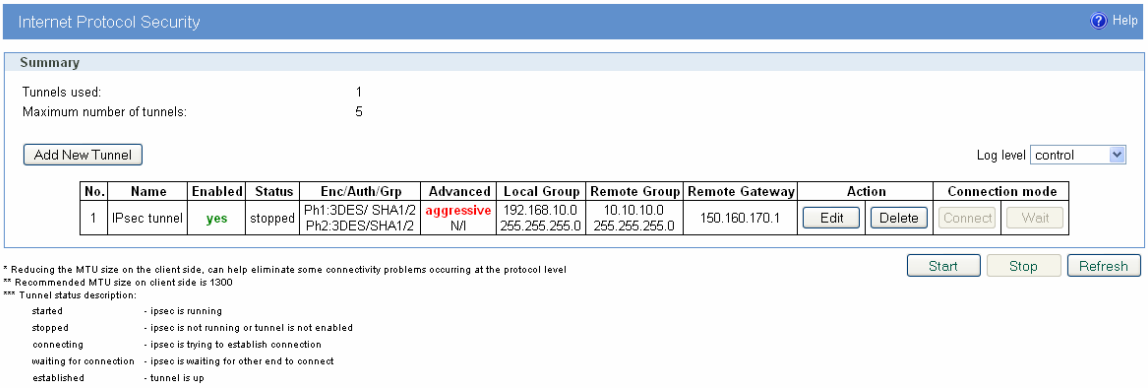


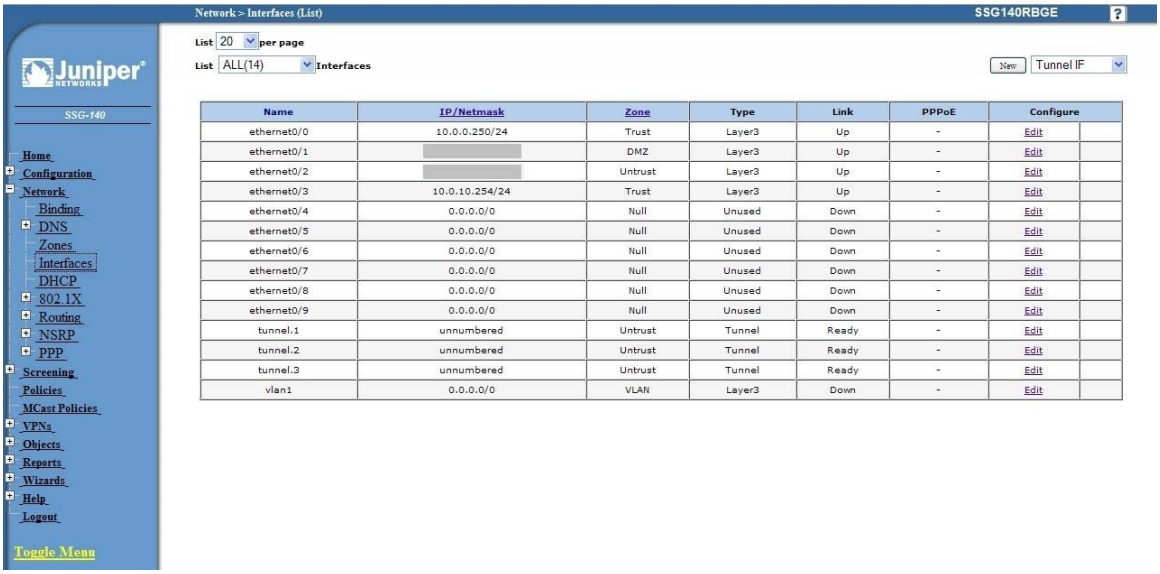
Figure 108 – IPSec start/stop page for GWR Router

- On the device connected on GWR 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		DMZ	Layer3	Up	-	Edit
ethernet0/2		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 109 – Network Interfaces (list)

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

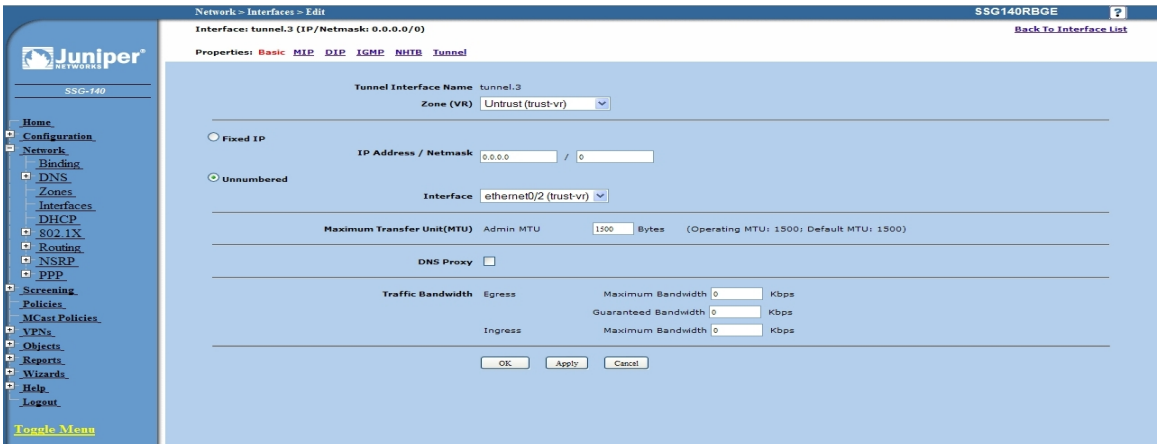


Figure 110 – Network Interfaces (edit)

Step 2 – Create New VPN IPSEC tunnel

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

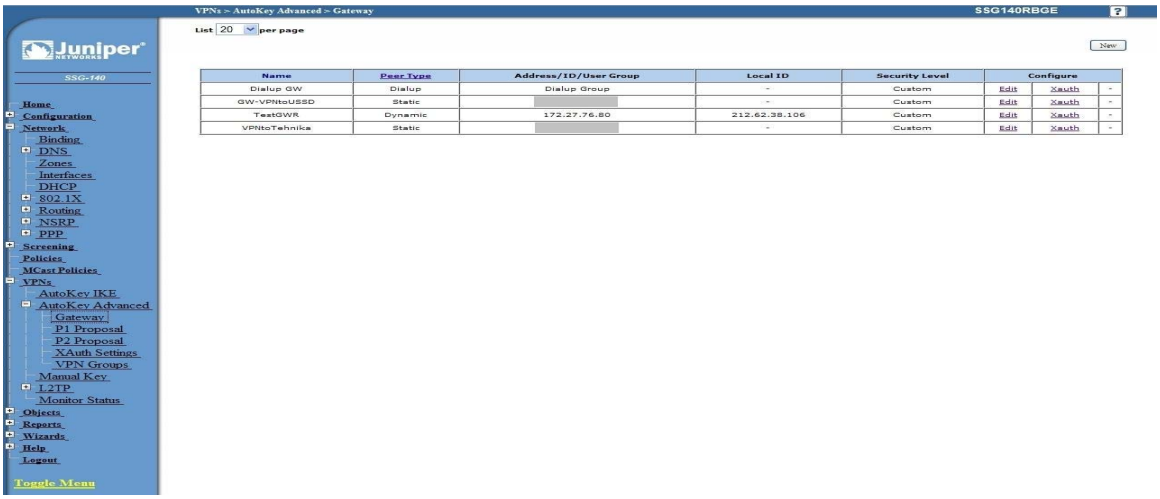


Figure 111 – AutoKey Advanced Gateway

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

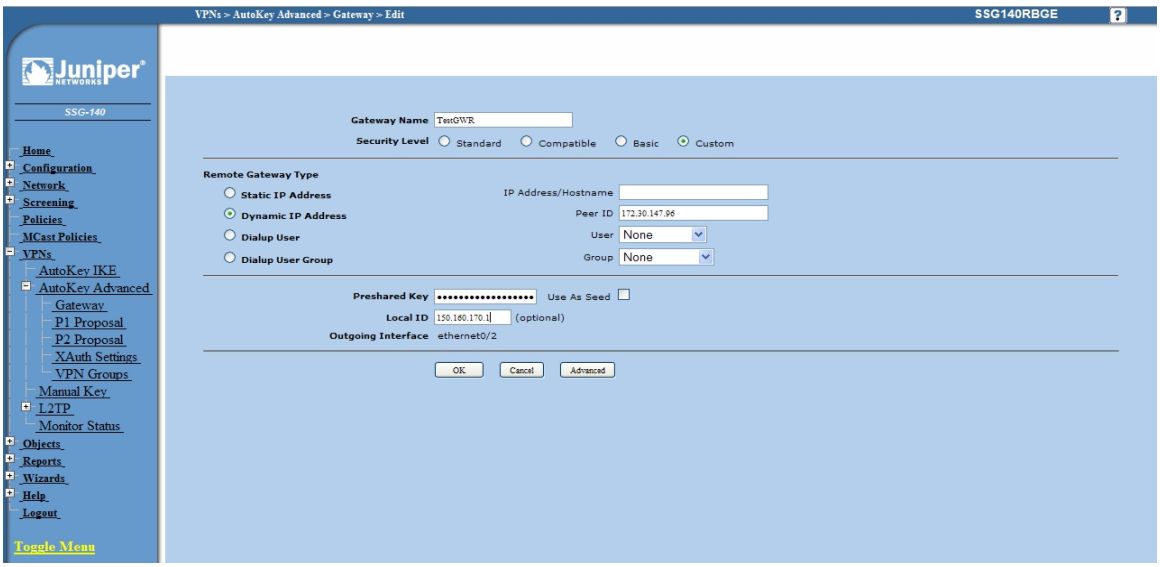


Figure 112 – Gateway parameters

- Click ***Advanced*** button.

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

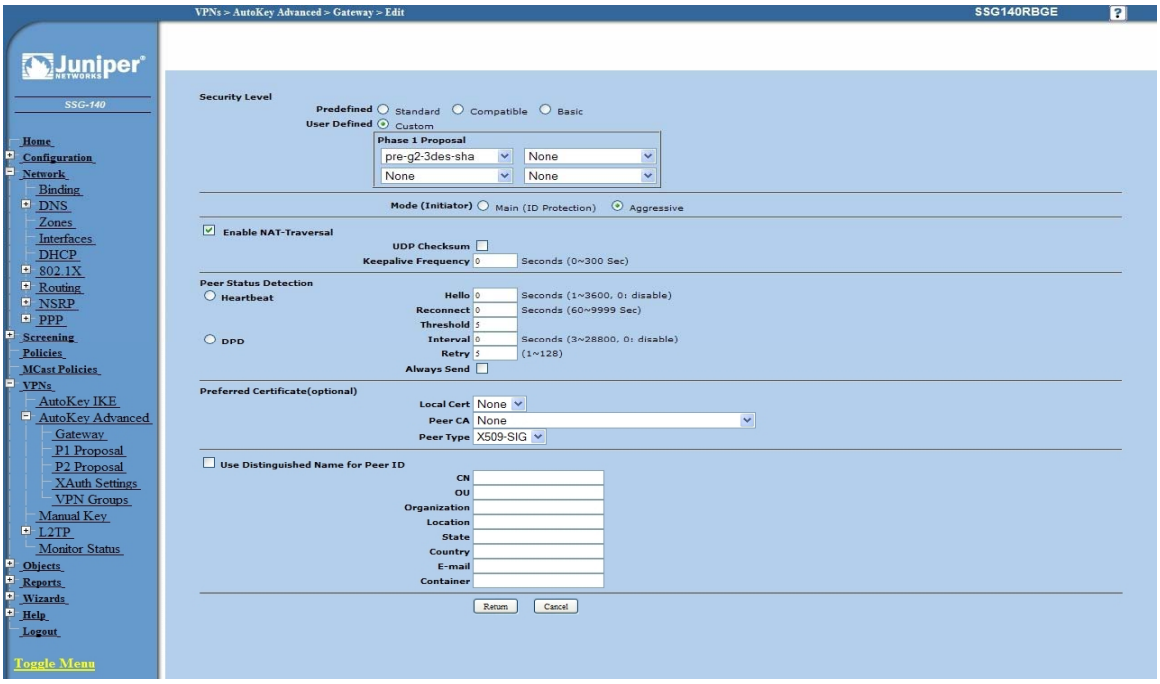


Figure 113 – Gateway advanced parameters

Step 3 – Create AutoKey IKE

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

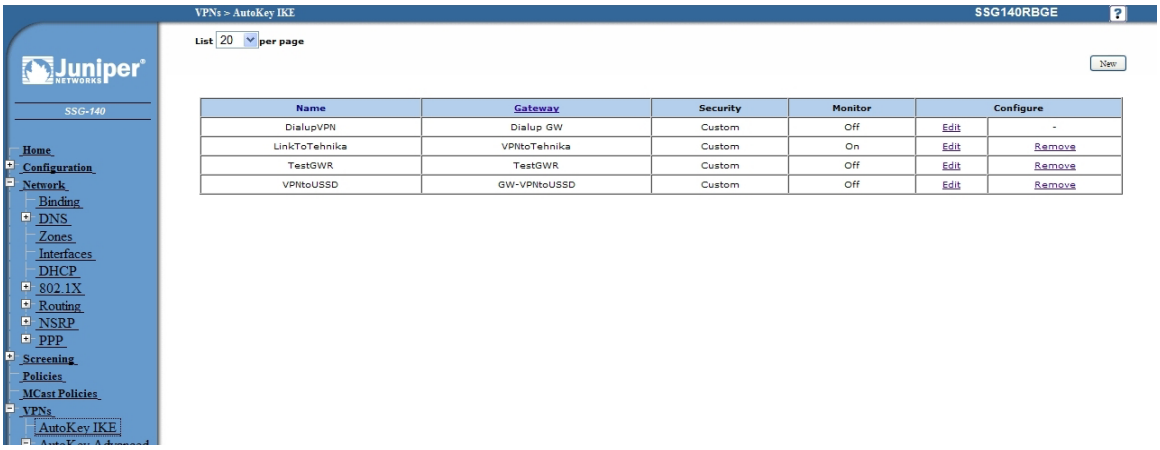


Figure 114 – AutoKey IKE

AutoKey IKE parameters are:

- **VPNname:** TestGWR,

- **Security level:** Custom,
- **Remote Gateway:** Predefined,
- Choose VPN Gateway from step 2.

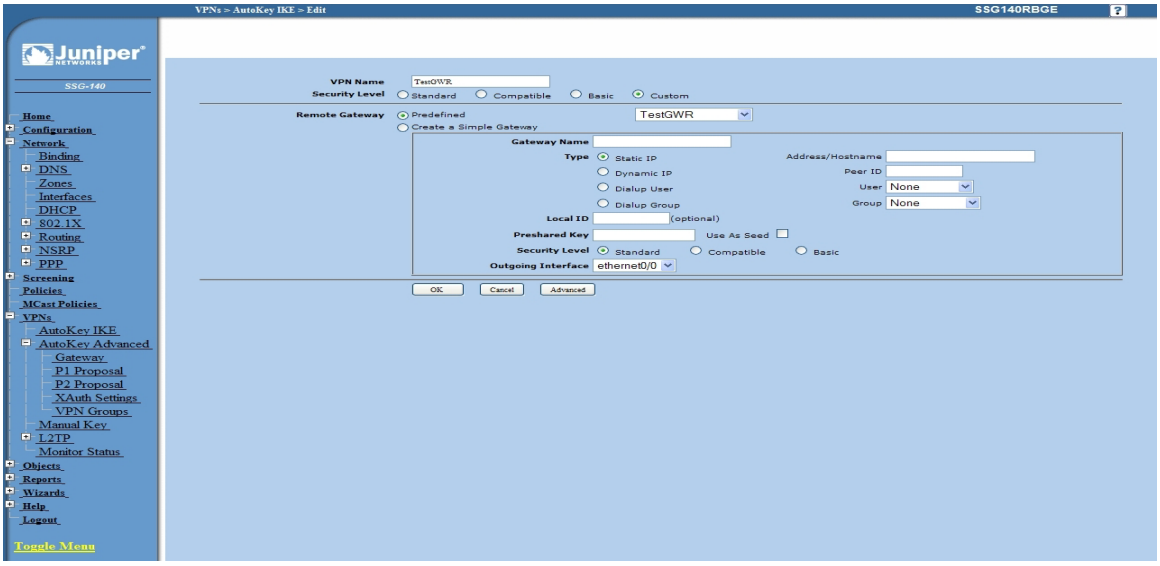


Figure 115 – AutoKey IKE parameters

- 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***.

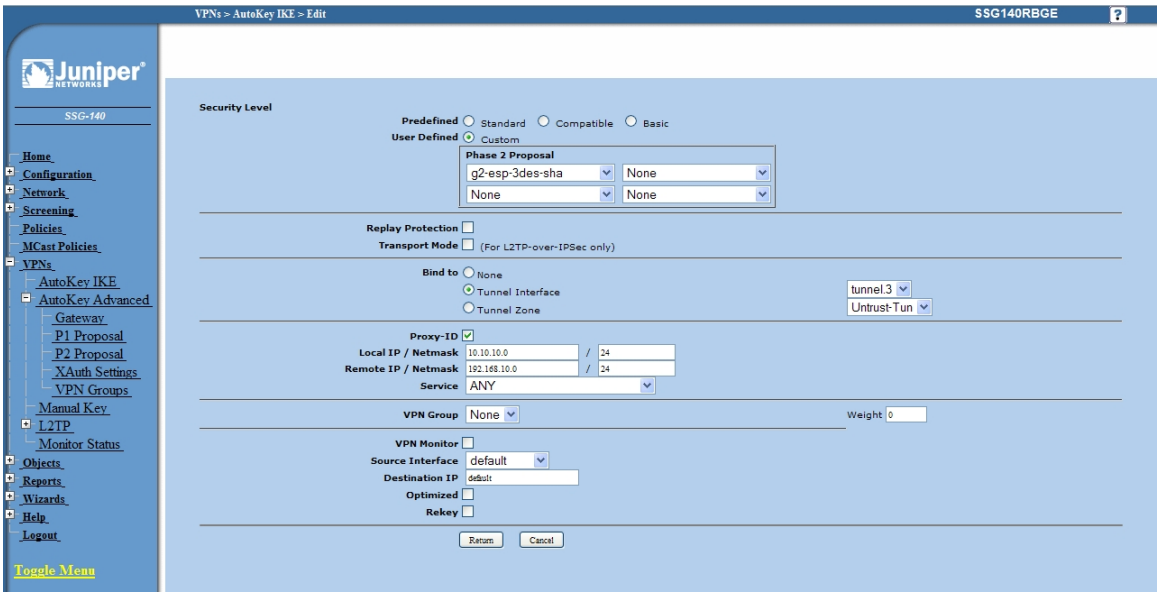


Figure 116 – AutoKey IKE advanced parameters

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.***

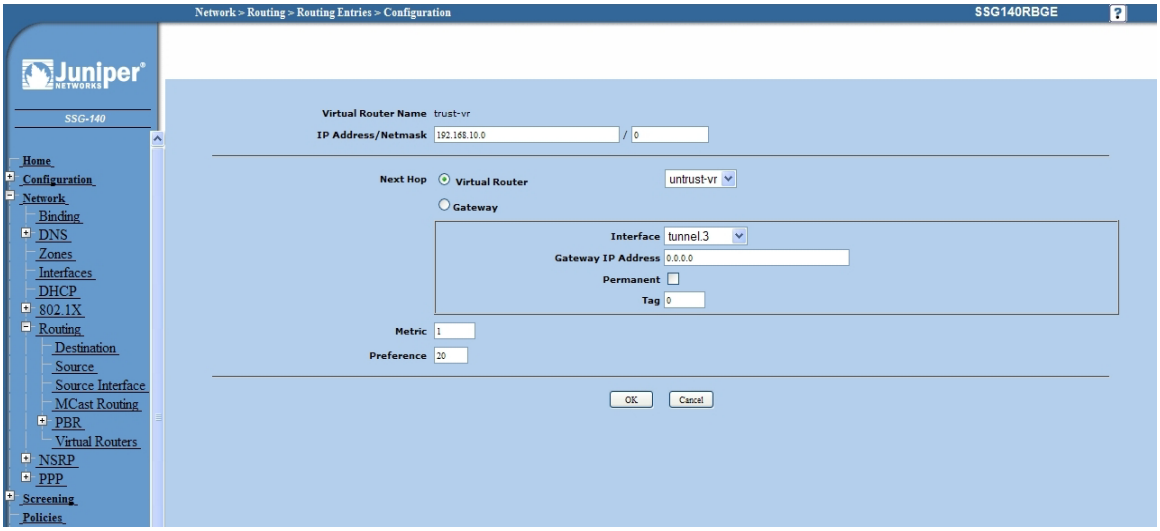


Figure 117 – Routing parameters

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.***

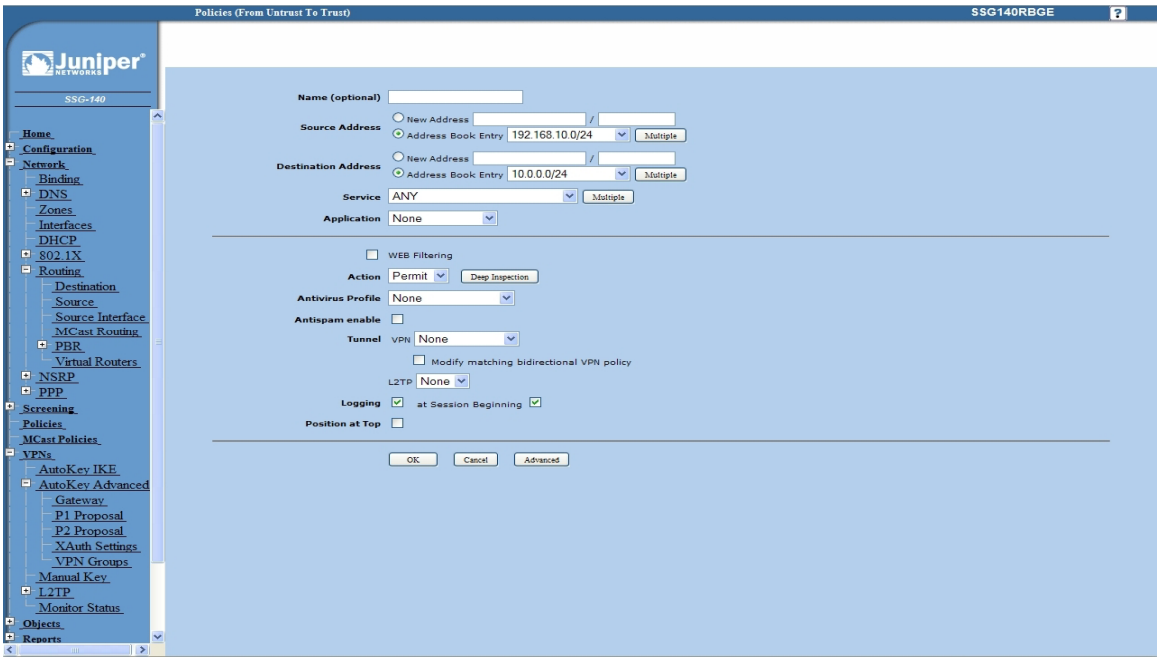


Figure 118 – Policies from untrust to trust zone

- 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.***

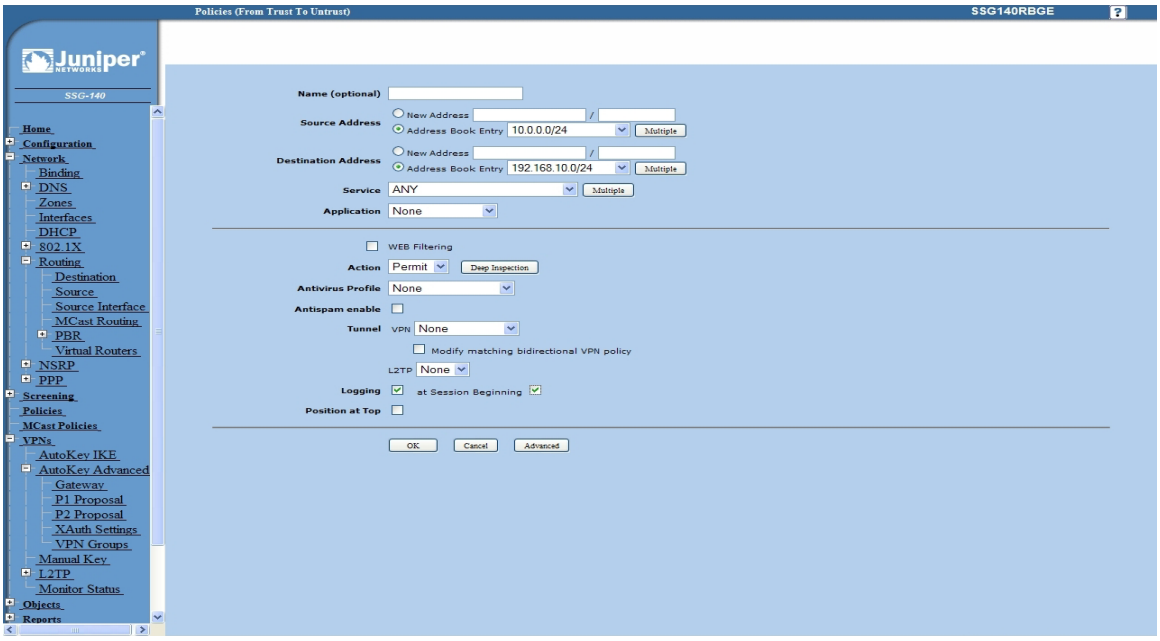


Figure 119 – Policies from trust to untrust zone

OpenVPN tunnel between GWR router and OpenVNP server

Overview

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.

OpenVPN configuration example

Open VPN is established between one central locations and three remote locations with Geneko router configured in TCP client mode. Authentication used is pre-shared secret.

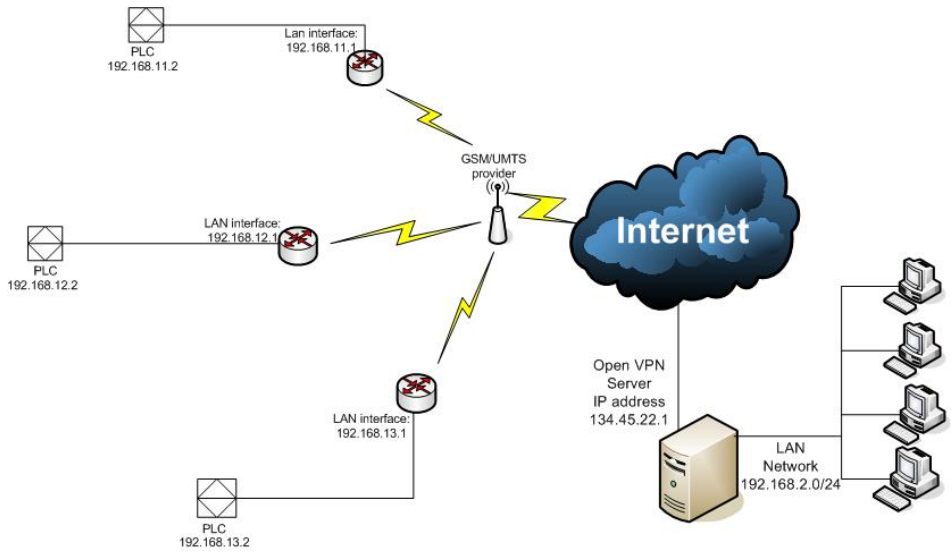


Figure 120 – Multipoint OpenVPN topology

Configuration

1. Open VPN server is in TCP listening mode and it is reachable from the internet over static public IP address 134.45.22.1 and TCP port 1194 (default Open VPN port)
2 Configuration file in Open VPN server is applied in following way:
   a) Open any Text Editor application and make configuration txt file.
   In this example configuration file looks like this

proto tcp-server	TCP server protocol mode
dev tun	dev tun mod of Open VPN server
ifconfig 2.2.2.1 2.2.2.2	Local and remote IP address of the Open VPN tunnel (both addresses must be within 255.255.255.252 subnet)

dev-node adap1	Selection of virtual network adapter named adap1
secret key.txt	Implementing file with pre-shared secret named key.txt
ping 10	Keepalive
comp-lzo	LZO compression enabled
disable-occ	disable option consistency

b) Save configuration file in C:\Program Files\OpenVPN\config as *name*.ovpn file.
It is OpenVPN configuration file directory and you can reach it directly through Start menu>OpenVPN where you get options:

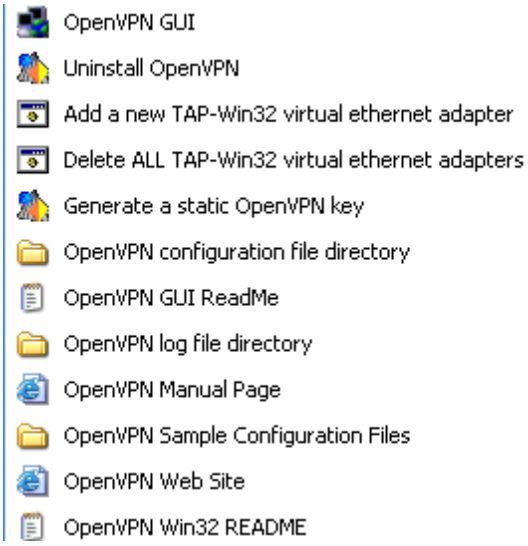


Figure 121 – OpenVPN application settings

c) Generate a static OpenVPN key from the menu above. File will be automatically Saved in Open VPN configuration file directory. Configuration file and pre-shared key must be in same directory.

d) If you have more remote locations every location has to have its own configuration file with different remote interface IP address and virtual network adapter. Second virtual network adapter you can create by selecting "Add a new TAP-Win32 virtual ethernet adapter". The same way you can create the third virtual adapter. Name virtual adapters as adap1, adap2 and adap3.

For example configuration file for second remote location can be:

proto tcp-server
dev tun
ifconfig 2.2.2.5 2.2.2.6
dev-node adap2
secret key.txt
ping 10
comp-lzo
disable-occ

Only difference to previous configuration is 2.2.2.5, 2.2.2.6
(IP address of local and remote interface) and dev-node adap2.
Configuration file for third remote location is:

proto tcp-server
dev tun
ifconfig 2.2.2.9 2.2.2.10
dev-node adap3
secret key.txt
ping 10
comp-lzo
disable-occ

All three configuration files (e.g. Server1.ovpn, Server2.ovpn, Server3.ovpn) have to be saved in same directory C:\Program Files\OpenVPN\config. Name of configuration file is name of your OpenVPN tunnel.

e) Workstation where OpenVPN server is installed should have ip route to subnet which is on the other end of the OpenVPN tunnel. This subnet is reachable over remote OpenVPN interface which is in this case 2.2.2.2. Enter following command in the command prompt:

route –p add 192.168.11.0 mask 255.255.255.0 2.2.2.2
first remote location

route –p add 192.168.12.0 mask 255.255.255.0 2.2.2.6
second remote location

route –p add 192.168.13.0 mask 255.255.255.0 2.2.2.10
third remote location

3. GWR router is configured with SIM card which has internet access. Configuration of OpenVPN is following:

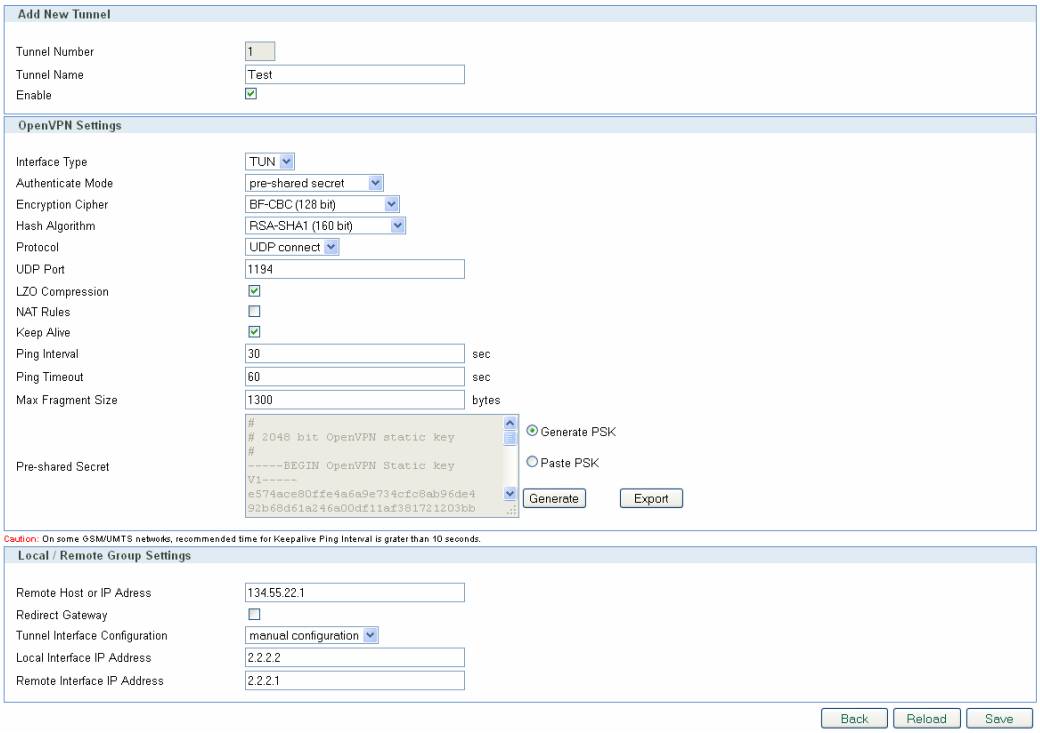


Figure 122 – OpenVPN GWR settings

Where pre-shared secret you paste from the *key.txt* file which you generate on OpenVPN server.

In routing table static IP route to local OpenVPN server network (in this case it is 192.168.2.0/24) should be entered.

Enable	Dest Network	Netmask	Gateway	Metric	Interface	Action
☑	0.0.0.0	0.0.0.0	*	1	ppp_0	Rem
☑	192.168.2.0	255.255.255.0	*	1	tun1	Rem

Figure 123 – Static routes on GWR

TUN1 interface isn't available before you start the OpenVPN tunnel so you must start it first

That accomplishes configuration of the GWR regarding establishing the OpenVPN and routing through it.

Implementation

You start Open VPN tunnel on server side by right click on the icon in notification bar. You choose Open VPN tunnel (Server1) and click Connect. The same procedure repeat for Server2 and Server3.

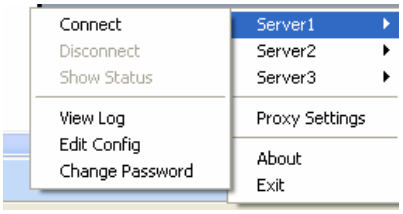


Figure 124 – Starting OpenVPN application

When OpenVPN tunnel is up on the Open VPN server you should get following notification:

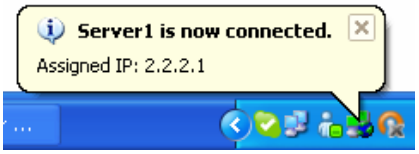


Figure 125 – OpenVPN status on PC

On the GWR side status of the OpenVPN tunnel should be established.

No.	Name	Enabled	Status	Auth. Mode	Advanced	F
1	Test	yes	established	pre-shared secret	LZO/NAT/KeA	

Figure 126 – OpenVPN status on GWR

Port forwarding example

Port forwarding feature enables access to workstations behind the router and redirecting traffic in both traffic flow directions – inbound and outbound. **Direction is selected by interface – PPP0 for inbound (WAN -> ETH0) and ETH0 for outbound traffic (ETH0 ->WAN).**

In the following example there are three types of access to LAN network enabled, every workstation with different service allowed from the outside. LAN is accessed through the WAN IP of the router. Second

and forth rule have additional limitation per source IP address of the incoming packets. The forth defined access flow is redirecting all WEB traffic from the local workstation to one outside IP address, web authentication server for example.

Implemented rules are following:

1. Traffic destined to WAN IP by port 5022 is forwarded to workstation 192.168.1.2 and port 22. Result – SSH is accessible from the outside to the first workstation
2. Traffic destined to WAN IP by port 8080 is forwarded to workstation 192.168.1.3 and port 80. Result – WEB is accessible from the outside to the second workstation. This rule is limited only to traffic coming from the 172.16.234.0/24 subnet
3. Traffic destined to WAN IP from port range 300:400 is forwarded to workstation 192.168.1.4 to port 12345
4. WEB traffic from the workstation 192.168.1.5 is forwarded to one outside IP address (212.62.49.109 for example)

If Source IP and Source Netmask fields are empty stated entry is applied to all incoming packets. When PPP0 interface is selected Destination IP and Netmask are predefined to WAN IP and subnet 32 and cannot be changed.

On the following picture are marked traffic flows stated above.

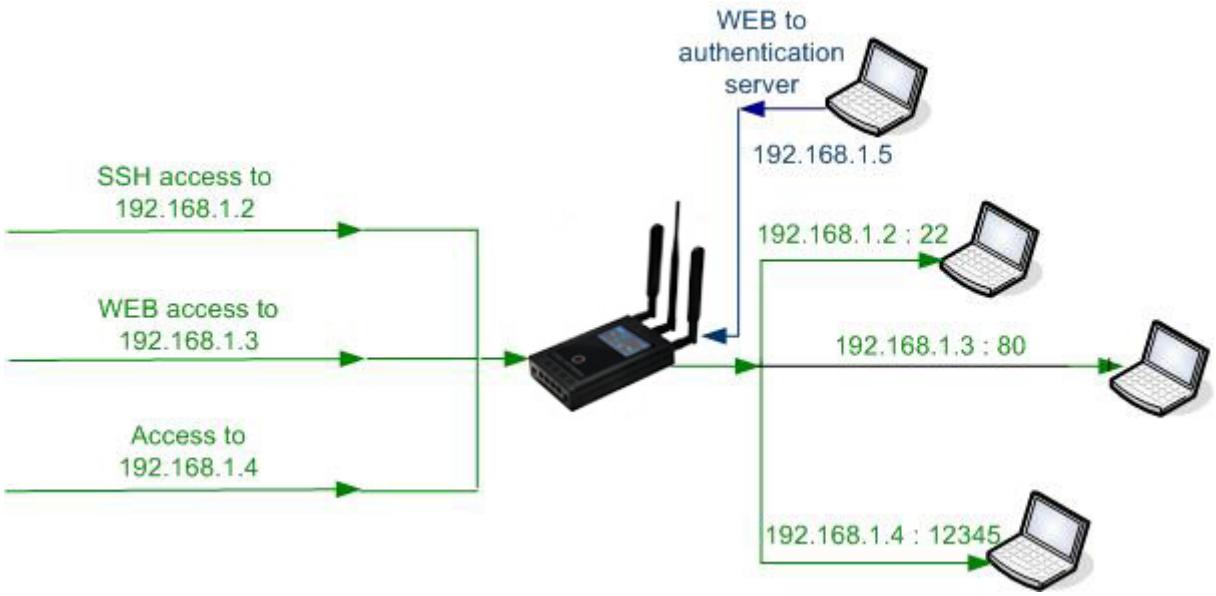
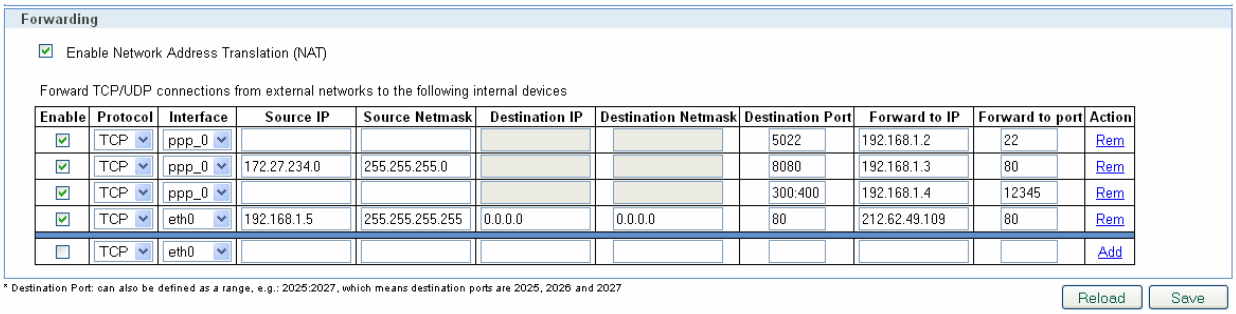


Figure 127 – Portforwarding example

Port forwarding is configured on the ROUTING page selected from the main menu. Configuration of the examples described above is presented in the following picture:



Forwarding

☑ Enable Network Address Translation (NAT)

Forward TCP/UDP connections from external networks to the following internal devices

Enable	Protocol	Interface	Source IP	Source Netmask	Destination IP	Destination Netmask	Destination Port	Forward to IP	Forward to port	Action
☑	TCP	ppp_0					5022	192.168.1.2	22	Rem
☑	TCP	ppp_0	172.27.234.0	255.255.255.0			8080	192.168.1.3	80	Rem
☑	TCP	ppp_0					300:400	192.168.1.4	12345	Rem
☑	TCP	eth0	192.168.1.5	255.255.255.255	0.0.0.0	0.0.0.0	80	212.62.49.109	80	Rem
☐	TCP	eth0								Add

* Destination Port: can also be defined as a range, e.g.: 2025:2027, which means destination ports are 2025, 2026 and 2027

Reload Save

Figure 128 – GWR port forwarding configuration

Serial port – example

For connecting serial devices from remote locations to central location serial transparent conversion can be used. Serial communication is encapsulated in TCP/IP header and on the central location is recognized by the Virtual COM port application. This way serial communication is enabled between two distant locations.

In the picture below serial communication is achieved over GWR router in client mode on remote location and Virtual COM port application on central side. As application is in server mode, IP address of the workstation has to be accessible from the router. In this example that is IP address GWR routers supports both server and client mode, so you can use one GWR router on both side of communication link (one in server and one in client mode).

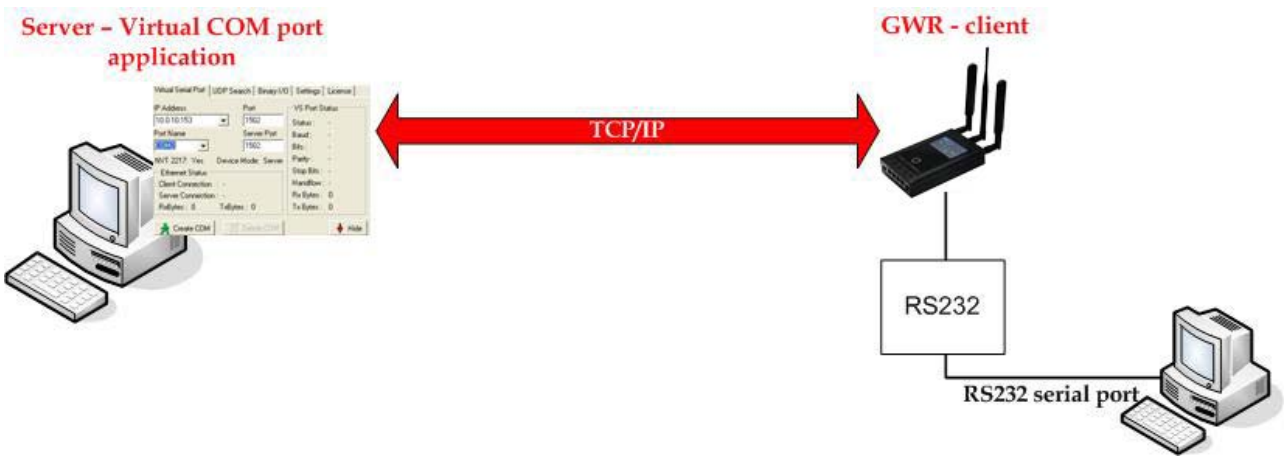


Figure 129 – Transparent serial connection

1. Settings on GWR router

From the main menu on the left side of web interface option SERIAL PORT should be selected and following page is displayed.

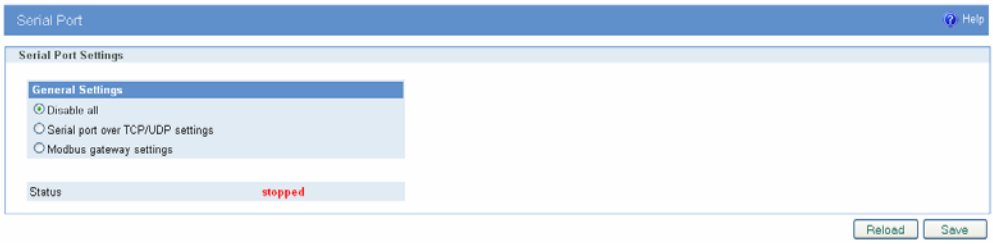


Figure 130 – GWR Serial port settings

Option SERIAL PORT OVER TCP/UDP SETTINGS is used for configuration of transparent serial communication. Configuration parameters are presented in picture below

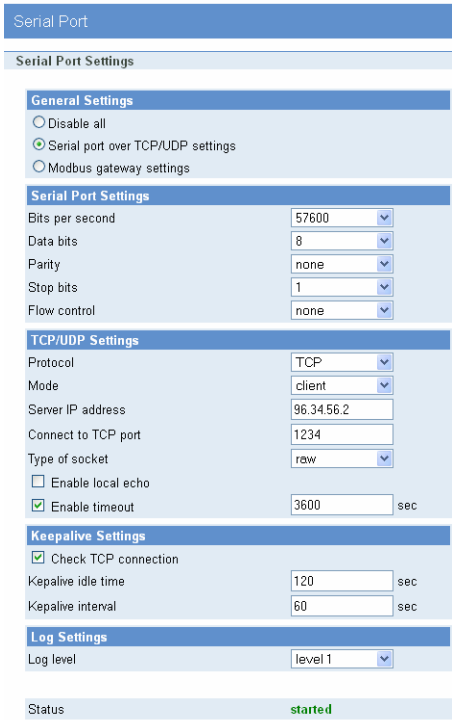


Figure 131 – GWR settings for Serial-to-IP conversion

General Settings

- Serial port over TCP/UDP settings

Serial port settings

- Bits per second: 57600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

TCP/UDP Settings

- Protocol: TCP
- Mode: client
- Server IP address: 96.34.56.2 (IP address of server)
- Connect to TCP port: 1234
- Type of socket: raw
- Enable local echo: Disabled
- Enable timeout: 3600 sec

Keepalive Settings

- Check TCP connection: Enable
- Keepalive idle time: 120 sec
- Keepalive interval: 60 sec

Log Settings

- Log level: level 1

When serial port is configured button SAVE should be selected and STATUS of the service should change to started like on the picture above.

2. Application settings

In this example is used application HW Virtual Serial Port which is installed on workstation on central location. When application is started on Settings tab option "HW VSP works as the TCP Server only" should be enabled.

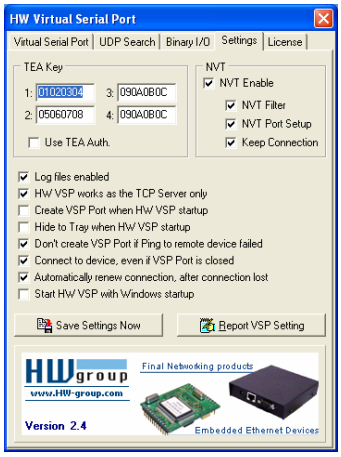


Figure 132 – Virtual COM port application

In Virtual Serial Port tab settings should be following:

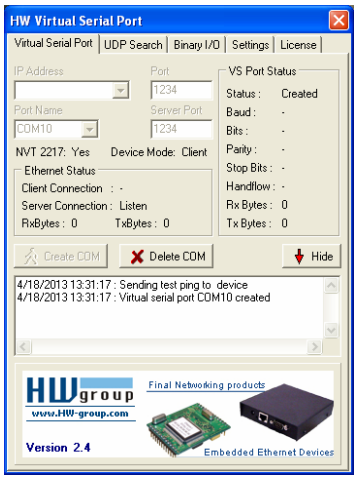


Figure 133 – Settings for virtual COM port

- IP address: - (not used in server mode)
- Port: 1234
- Server Port: 1234
- Port Name: COM10 (random selected)

After "Create COM" is activated if everything is alright in log will be shown message that port COM10 is created, like in picture above. In communication with remote serial device COM10 should be selected on workstation.

Firewall – example

Firewall implemented in GWR routers has numerous options for matching interesting traffic. Traffic flow is controlled through the router with three actions triggered by firewall:

1. ACCEPT – traffic is passed through the router without any changes implemented
2. REJECT – traffic is blocked with ICMP error messages
3. DROP – traffic is blocked without any error messages, connection is retried until the threshold for retransmission is exceeded

By default all traffic is PERMITTED. To block all the traffic not defined under stated rules last entry in firewall table should be DROP ALL.

Rule priority defines order by which router matches inspected packets. After first match between rule and packet, no other rule is compared against matched traffic.

Firewall has 17 predefined rules for the most common usage. These 17 rules are following:

1. Allow ALL from local LAN

All traffic originating from local subnet is allowed to access router Ethernet interface. It is important to keep this rule enabled to prevent losing local management interface.

2. Allow already established traffic

For inbound TCP only. Allows TCP traffic to pass if the packet is a response to an outbound-initiated session.

3. Allow TELNET on ppp_0

Accepts telnet connection from the outside to router's WAN interface, for management over CLI interface

4. Allow HTTP on ppp_0

Accepts WEB traffic from the outside to router's WAN interface, for management over WEB interface

5. Allow PING on ppp_0-with DDoS filter

ICMP traffic to WAN interface of the router is allowed with prevention of Distributed Denial-of-service attack

Allow RIP protocol

6. Allow RIP on ppp_0
7. Allo RIP on ppp_0 – route

Allow GRE protocol

8. Allow GRE tunnels on ppp_0
9. Allow GRE Keepalive on ppp_0

Allow IPSec protocol

10. Allow IPSec tunnels on ppp_0 – protocol
11. Allow IPSec tunnels on ppp_0 – IKE
12. Allow IPSec tunnel on ppp_0 – IKE_NATt

Allow OpenVPN protocol

13. Allow OpenVPN tunnels on ppp_0 – UDP
14. Allow OpenVPN tunnels on ppp_0 – TCP

15. Allow SNMP on ppp_0

SNMP requests are allowed to be sent to the router over WAN interface

16. Allow MODBUS on ppp_0
MODBUS conversion over default port UDP 502 is permitted

17. REJECT all other traffic
All packets which are not stated as ACCEPT in previous rules are denied. If this rule is not enabled all packets which are not stated as DROP/REJECT are permitted.

In following example 8 traffic flows are defined under firewall rules. In the picture presented with green are marked permitted packets and with red blocked.

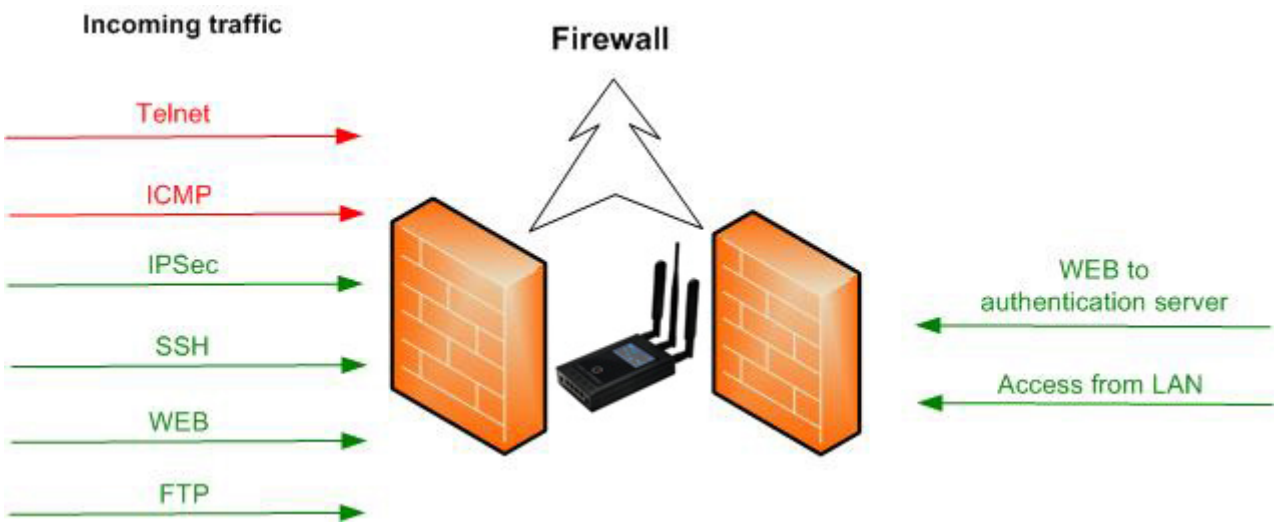


Figure 134 – Firewall example

Firewall is enabled in SETTINGS>FIREWALL page. Page for firewall configuration is presented in the following picture:

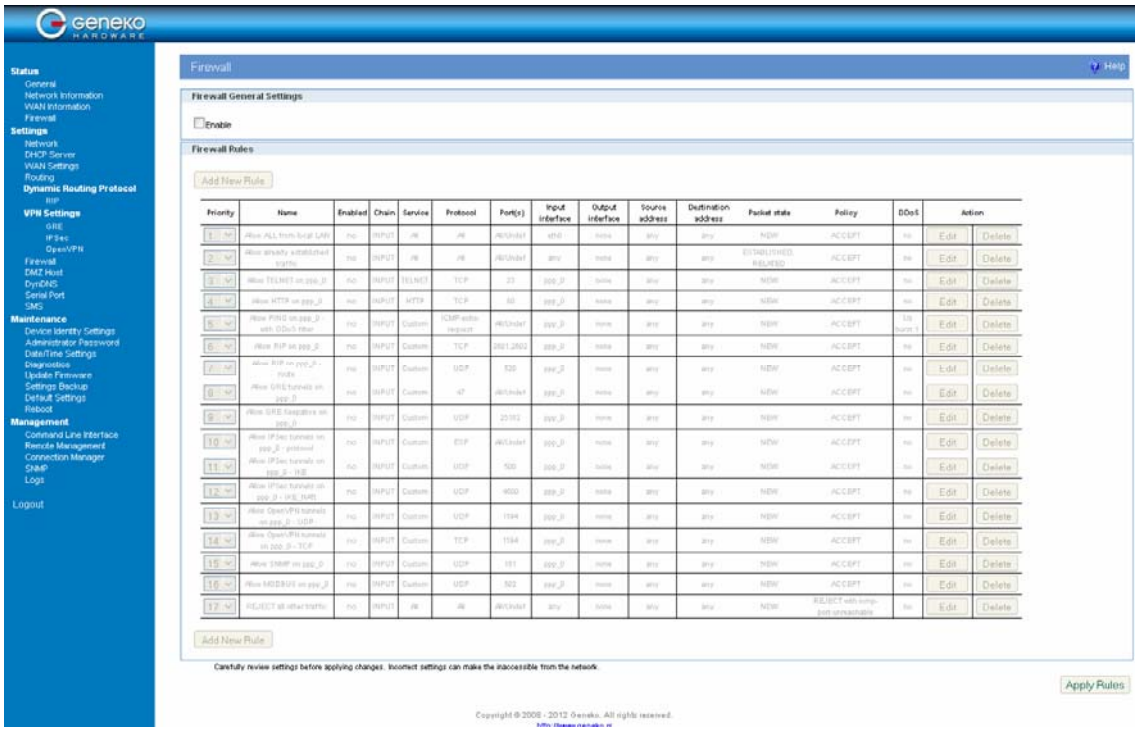


Figure 135 – Initial firewall configuration on GWR

Firstly firewall should be enabled, that is done by selecting:

Firewall General Settings>Enable

Firewall can be configured by enabling or editing existing, predefined rules or by adding new one. Firewall is configured in following way:

1. **Telnet traffic is denied**

Select predefined rule number 3. Configuration page like on picture below is shown.

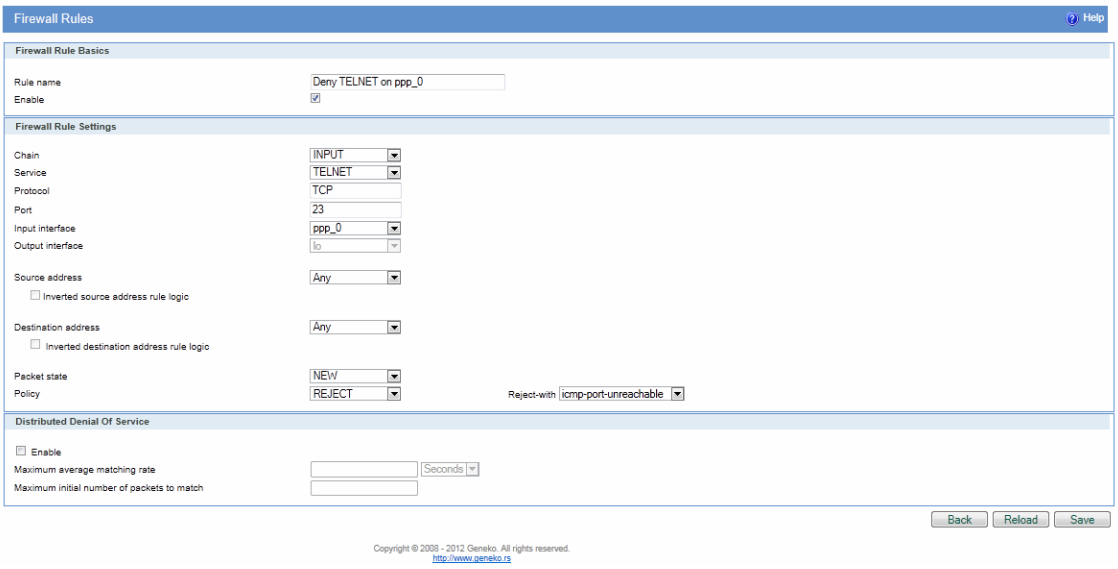


Figure 136 – Filtering of Telnet traffic

ENABLE option should be selected to have this rule active. To deny Telnet traffic POLICY should be changed from ACCEPT to REJECT (ICMP error message type can be selected when policy reject is selected). After that SAVE button should be pressed and user is returned to main configuration page.

2. ICMP traffic is denied from all IP addresses except 212.62.38.196

New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Deny PING to ppp_0 interface
- Enable: selected
- Chain: INPUT
- Service: Custom
- Protocol: ICMP
- ICMP-Type: echo-request
- Input interface: ppp_0
- Source address: Single IP ; 212.62.38.196
- Inverted source address rule logic: selected
- Destination address: Any
- Packet state: NEW
- Policy: REJECT
- Reject-with: icmp-port-unreachable

Configuration should be like on the picture below.

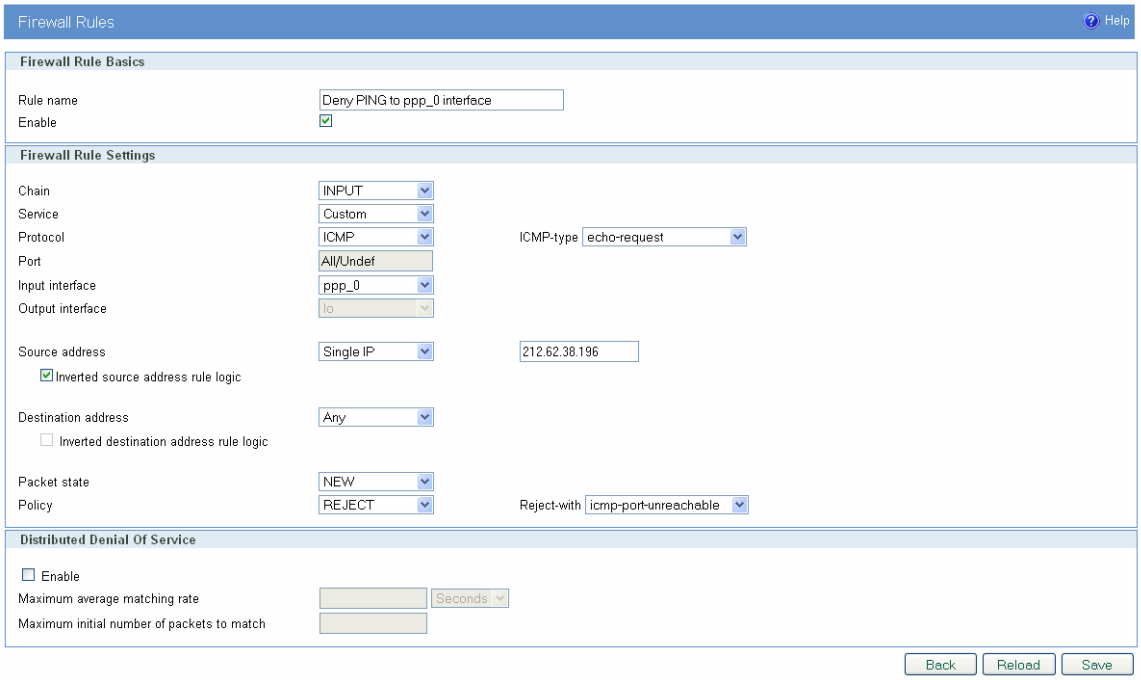


Figure 137 – Filtering of ICMP traffic

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 4 is selected.

3. ICMP traffic is allowed from single IP addresses

With firewall rule configuration shown above, IP address stated in Source address field is excluded from REJECT policy but in order to allow ping from that IP address it has to be matched with another rule. Configuration of appropriate rule for allowing ping traffic originating from precise IP address is shown below

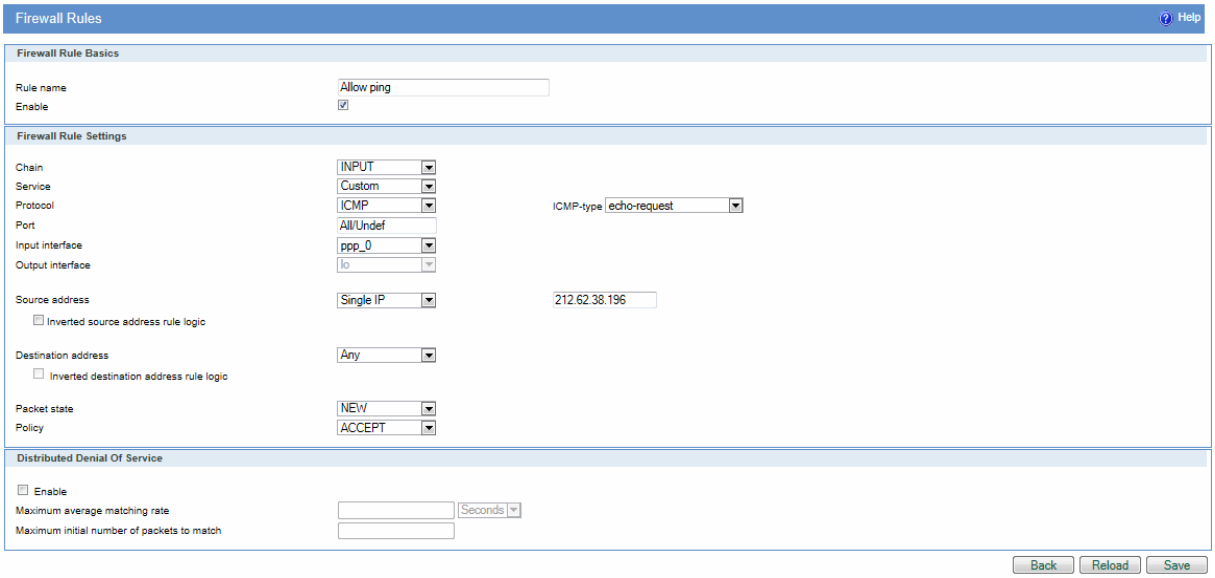


Figure 138 – Allowing ICMP traffic

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 5 is selected.

4. Establishing of IPSec tunnel is allowed

Firewall has to allow IKE and ESP protocol for IPSec tunnel establishment. If NAT traversal is used one additional port has to be allowed. All these rules are predefined and they have priorities 10, 11 and 12 in default firewall configuration (they are named as *Allow IPSec tunnels on ppp_0 –protocol, IKE and NATt*). As these rules are already configured it is enough just to enable them to have IPSec passed through firewall.

10	Allow IPSec tunnels on ppp_0 - protocol	yes	INPUT	Custom	ESP	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
11	Allow IPSec tunnels on ppp_0 - IKE	yes	INPUT	Custom	UDP	500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
12	Allow IPSec tunnels on ppp_0 - IKE_NATt	yes	INPUT	Custom	UDP	4500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete

Figure 139 – IPSec firewall rules

These three rules are enabled in following way:

- Select EDIT of the rule
- Enable: selected
- SAVE and exit

5. SSH access is allowed from IP range 212.62.38.210-220

New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Allow SSH
- Enable: selected
- Chain: INPUT
- Service: Custom
- Protocol: TCP
- Port: Custom; 22
- Input interface: ppp_0
- Source address: Range ; 212.62.38.210 : 212.62.38.220
- Destination address: Any
- Packet state: NEW
- Policy: ACCEPT

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 6 is selected.

6. WEB access is allowed from 212.62.38.210 IP address

In default firewall configuration rule for allowing WEB traffic is predefined (rule with priority 4, named *Allow HTTP on ppp_0*) This rule can be used in example with additional restriction in source IP address to 212.62.38.210. Policy should be configured in following way:

- Enable: selected
- Source address: Single IP; 212.62.38.210
- All other settings should remain the same like in the picture below

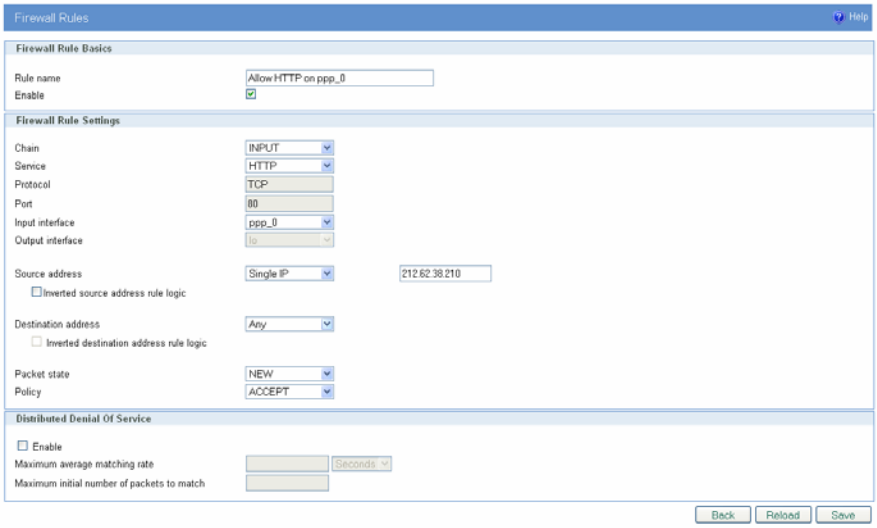


Figure 140 – Allowing WEB access

After configuration is finished SAVE button should be selected and user is returned to main configuration page.

7. FTP traffic is allowed

New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Allow FTP
- Enable: selected
- Chain: INPUT
- Service: FTP
- Protocol: TCP
- Port: 21
- Input interface: ppp_0
- Source address: Any
- Destination address: Any
- Packet state: NEW
- Policy: ACCEPT

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 8 is selected.

8. Access from LAN to router is allowed

This is first rule in predefined firewall settings (*Allow ALL from local LAN*). It is recommended to have this rule enabled to allow access to management interfaces of the router. As this rule is already configured it is enough just to enable it to have access to router from LAN:

- Select EDIT of the rule
- Enable: selected
- SAVE and exit

9. WEB traffic is permitted only to 212.62.38.210 from LAN

This rule is example of traffic filtering in direction from inside to outside. New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Allow HTTP from LAN
- Enable: selected
- Chain: FORWARD
- Service: HTTP
- Protocol: TCP
- Port: 80
- Input interface: eth0
- Output interface: ppp_0
- Source address: Any
- Destination address: Any
- Packet state: NEW
- Policy: ACCEPT

Configuration is shown in following picture:

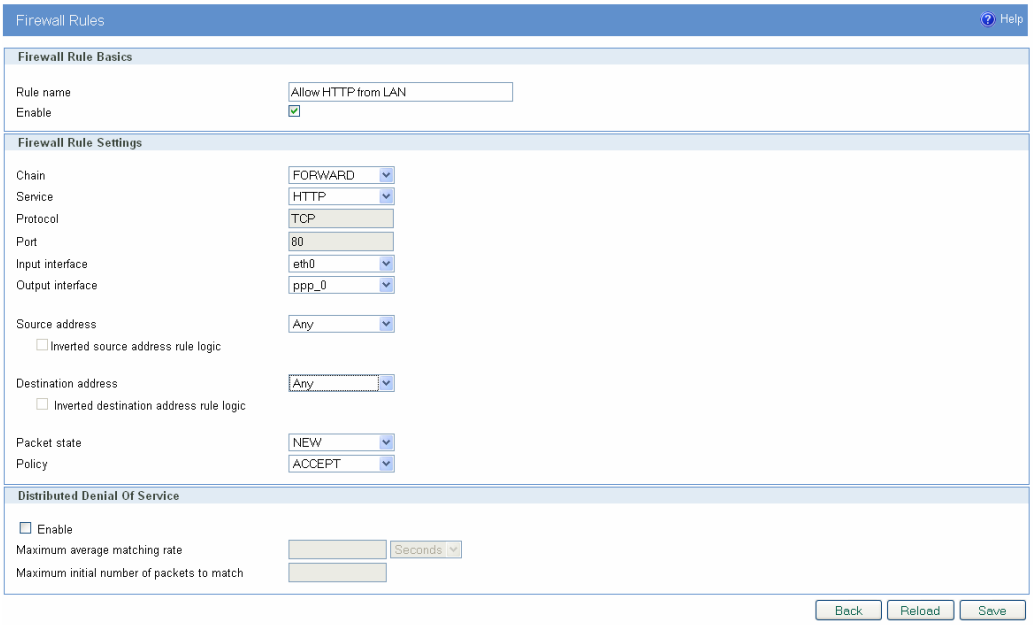


Figure 141 – Outbound rule for WEB access

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 9 is selected.

Additionally to these 11 rules two more rules are enabled:

- Allow already established traffic (priority number 2)
- Reject all other traffic (priority number 22)

After all rules are configured and saved button APPLY RULES in bottom right corner should be selected to activate traffic filtering.

When all 13 rules from this example is configured firewall should look like this:

Firewall

Firewall General Settings

Enable

Firewall Rules

Add New Rule

Priority	Name	Enabled	Chain	Service	Protocol	Port(s)	Input interface	Output interface	Source address	Destination address	Packet state	Policy	DDoS	Action	
1	Allow ALL from local LAN	yes	INPUT	All	All	All/Undef	eth0	none	any	any	NEW	ACCEPT	no	Edit	Delete
2	Allow already established traffic	yes	INPUT	All	All	All/Undef	any	none	any	any	ESTABLISHED, RELATED	ACCEPT	no	Edit	Delete
3	Deny TELNET on ppp_0	yes	INPUT	TELNET	TCP	23	ppp_0	none	any	any	NEW	REJECT with:icmp-port-unreachable	no	Edit	Delete
4	Deny PING to ppp_0 interface	yes	INPUT	Custom	ICMP-echo-request	All/Undef	ppp_0	none	!172.27.234.21	any	NEW	REJECT with:icmp-port-unreachable	no	Edit	Delete
5	Allow ping	yes	INPUT	Custom	ICMP-echo-request	All/Undef	ppp_0	none	212.62.38.196	any	NEW	ACCEPT	no	Edit	Delete
6	Allow SSH	yes	INPUT	Custom	TCP	22	ppp_0	none	212.62.38.210:212.62.38.220	any	NEW	ACCEPT	no	Edit	Delete
7	Allow HTTP on ppp_0	yes	INPUT	HTTP	TCP	80	ppp_0	none	212.62.38.210	any	NEW	ACCEPT	no	Edit	Delete
8	Allow FTP	yes	INPUT	FTP	TCP	21	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
9	Allow HTTP from LAN	yes	FORWARD	HTTP	TCP	80	eth0	ppp_0	any	any	NEW	ACCEPT	no	Edit	Delete
10	Allow IPSec tunnels on ppp_0 - protocol	yes	INPUT	Custom	ESP	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
11	Allow IPSec tunnels on ppp_0 - IKE	yes	INPUT	Custom	UDP	500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
12	Allow IPSec tunnels on ppp_0 - IKE_NATI	yes	INPUT	Custom	UDP	4500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
13	Allow PING on ppp_0 - with DDoS filter	no	INPUT	Custom	ICMP-echo-request	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	15/m burst:10	Edit	Delete
14	Allow RIP on ppp_0	no	INPUT	Custom	TCP	2601,2602	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
15	Allow RIP on ppp_0 - route	no	INPUT	Custom	UDP	520	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
16	Allow GRE tunnels on ppp_0	no	INPUT	Custom	47	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
17	Allow GRE Keepalive on ppp_0	no	INPUT	Custom	UDP	25162	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
18	Allow OpenVPN tunnels on ppp_0 - UDP	no	INPUT	Custom	UDP	1194	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
19	Allow OpenVPN tunnels on ppp_0 - TCP	no	INPUT	Custom	TCP	1194	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
20	Allow SNMP on ppp_0	no	INPUT	Custom	UDP	161	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
21	Allow MODBUS on ppp_0	no	INPUT	Custom	UDP	502	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
22	REJECT all other traffic	yes	INPUT	All	All	All/Undef	any	none	any	any	NEW	REJECT with:icmp-port-unreachable	no	Edit	Delete

Add New Rule

Figure 142 – Complete firewall configuration

SMS management – example

GWR routers can be managed over the SMS messages. Commands from the SMS are executed on the router with status report sent back to the sender.

On the picture below are settings for SMS management where three mobile phone numbers are allowed to send commands to the router over first SIM card. In this example management over SIM2 is not enabled. Please have in mind that router can receive messages only on SIM card which is currently selected. This information is displayed in WAN settings page, Mobile Status, Current SIM card. SMS service center number is automatically obtained.

Short Message Service

SIM1 Settings

Enable Remote Control

Use default SMSC

Custom SMSC

Phone Number 1: +381635938558

Phone Number 2: +381649098473

Phone Number 3: +381609459439

Phone Number 4

Phone Number 5

SIM2 Settings

Enable Remote Control

Use default SMSC

Custom SMSC

Phone Number 1

Phone Number 2

Phone Number 3

Phone Number 4

Phone Number 5

* Phone Number example: +38164111222

Reload Save

Figure 143 – Configuration page for SMS management

Settings are following:

- Enable Remote Control: Enabled
- Use default SMSC: Enabled

- Phone Number 1,2…5: Allowed phone number

From the mobile phone user can send 6 different commands for router management. Commands are following:

1. *:PPP-CONNECT*
2. *:PPP-DISCONNECT*
3. *:PPP-RECONNECT*
4. *:PPP-STATUS*

Reply to this command is one of four possible states:

- CONNECTING
- CONNECTED, WAN_IP:{WAN IP address}
- DISCONNECTING
- DISCONNECTED

5. *:SWITCH-SIM*, for changing SIM slot
6 *:REBOOT*, for router reboot

After every SMS sent to the router, reply is sent back with status information about SMS received by the router.

Defining keepalive functionality

Keep-alive mechanism works through two simple steps.

First step is STANDARD ping proofing. This ping periodically checks if link is alive. Standard ping has 4 packets which are sent over the link and if all 4 are returned keep-alive remains in standard ping proofing mode. If two or more of 4 packets are dropped keep-alive activates ADVANCED ping proofing.

ADVANCED ping proofing is second step in link quality detection. Advanced ping proofing sends 5 ping packets in short period of time and gives statistic how much packets are dropped (for example if 4 packets are dropped, ping lost is 80%). If this value is defined as 100% for example, that means only if all packets are dropped action will be performed (switch SIM or PPP restart). Value which is entered here depends on that how many packets can be tolerated to lose on the link. For example if value 60% is entered 2 packets of 5 (40%) are lost, keep-alive is returned to step one (standard ping proofing) with no action performed. If PPP should be restarted only when all packets are dropped defined value should be 100%.

In following example keepalive is enabled on both SIM cards. Action defined is SWITCH SIM so router will change SIM card when link failure is detected.
Settings are following:

SIM1

Ping target: 8.8.8.8
Ping interval: 120
Advanced ping interval: 10
Advanced ping wait for response: 5
Maximum number of failed packets: 80
Keepalive action: switch SIM

SIM2
Ping target: 212.62.32.1
Ping interval: 120
Advanced ping interval: 10
Advanced ping wait for response: 5

Maximum number of failed packets: 40 (more restrictive condition compared to SIM1)
Keepalive action: switch SIM

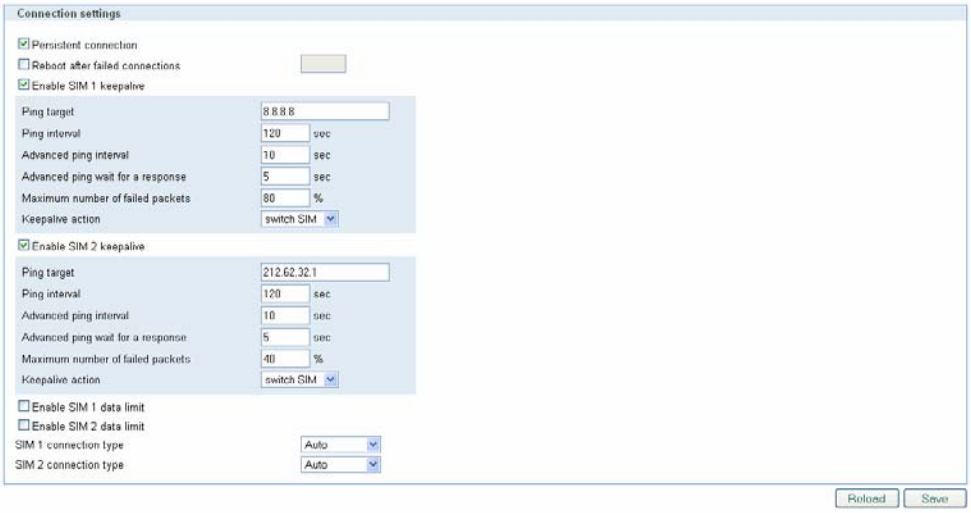


Figure 144 – Configuration page for GSM keepalive

Display

In the left corner is rectangle with number 1 and/or 2 describing which SIM card is present, name of mobile network operator (MTS) and telecommunication standard (WCDMA- Code-Division Multiple Access) .
In the right corner is signal strength (graphic display and dBm value).

Graphic display represents:

Line	FW 1.2.1 and (a newer)
Green 2	-51, -73
Green 1	-75, -83
Yellow	-85, -93
Red 2	-95, -103
Red 1	-105, -111
empty	-113 or less

Figure 145 – Graphic display

Value	RSSI dBm	Condition
0	-113 or less	Marginal or none
1	-111	Marginal
2	-109	Marginal
3	-107	Marginal
4	-105	Marginal
5	-103	Marginal
6	-101	Marginal
7	-99	Marginal
8	-97	Marginal
9	-95	Marginal
10	-93	OK
11	-91	OK
12	-89	OK
13	-87	OK
14	-85	OK
15	-83	Good
16	-81	Good
17	-79	Good
18	-77	Good
19	-75	Good
20	-73	Excellent
21	-71	Excellent
22	-69	Excellent
23	-67	Excellent

24	-65	Excellent
25	-63	Excellent
26	-61	Excellent
27	-59	Excellent
28	-57	Excellent
29	-55	Excellent
30	-53	Excellent
31	-51 or greater	Excellent
99		not known or not detectable

If the router is connected on mobile network the display shows a green semicircular lines from antenna to rectangle labeled CELL.
If the wireless is turned on the display shows a green semicircular lines from antenna to rectangle labeled WiFi.
On the display we can see uptime and current firmware version or IP address for each interface which has an IP address assigned. To change what is displayed, push the button on the back panel of GWR XS router.

Figure 146 – Display

Appendix

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 lighting protection).

- Simply install the GWR 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.

KNOWN ISSUES

Items listed here represent minor problems known at release time. These issues are going to be resolved in a next version.

- GenAir PLS8-E v3 (Revision 01.090) can not work using PPP mode.
- Always use Direct IP mode, which is anyway always recommended to get full LTE speed.
- This is a mobile module issue and it can not be fixed using software upgrade.
- GenAir PLS8-E v3 (Revision 01.090) can not receive SMS messages.
- This is a mobile module issue and it can not be fixed using software upgrade.

GENEKO
Bul. Despota Stefana 59a
11000 Belgrade ▪ Serbia
Phone: +381 11 3340-591, 3340-178
Fax: +381 11 3224-437
e-mail: gwrsupport@geneko.rs
www.geneko.rs