## Content

LIST OF FIGURES	
LIST OF TABLES	
DESCRIPTION OF THE GPRS/EDGE/HSDPA ROUTER	
Examples of Possible Application	
Technical Parameters	
GWR Router features	
Product Overview	
Front panel	
Back panel	
Top Panel Putting Into Operation	
Declaration of conformity	
Device Configuration	
DEVICE CONFIGURATION	14
NOTE.	
Add/Remove/Update manipulation in tables	
Save/Reload changes	
Status Information	
Status mornation	
Status - General Status - Network Information	
Status - WAN Information	
Settings - Network	
Settings - DHCP Server	
Settings - WAN Setting	
Settings – Routing Port translation	
Settings – Dynamic Routing Protocol Routing Information Protocol (RIP)	21
RIP routing engine for the GWR Router	
Settings – VPN Settings	
Generic Routing Encapsulation (GRE)	
GRE Keepalive	. 31
Internet Protocol Security (IPSec)	
OpenVPN	38
Settings - IP Filtering	
IP Filtering configuration example	
Settings – DynDNS	
Settings - Serial Port	
Serial port over TCP/UDP settings	
Modbus Gateway settings	
Maintenance - Device Identity Settings	
Maintenance - Administrator Password	
Maintenance - Date/Time Settings	
Maintenance - Diagnostics	
Maintenance - Update Firmware	
Maintenance - Settings Backup	
Import Configuration File Export Configuration File	
Maintenance - Default Settings	
Maintenance - Deraut Settings Maintenance - System Reboot	
Management – Command Line Interface	
Management – Command Line Interface Management – Remote Management	
Management – Connection Manager	υI



Management - Simple Management Protocol (SNMP)	64
Management - Logs	65
CONFIGURATION EXAMPLES	67
GWR Router as Internet Router	67
GRE Tunnel configuration between two GWR Routers	68
GRE Tunnel configuration between GWR Router and third party router	73
IPSec Tunnel configuration between two GWR Routers	
IPSec Tunnel configuration between GWR Router and Cisco Router	84
A. How to Achieve Maximum Signal Strength with GWR Router?	90
Antenna placement	
Antenna Options	



# List of Figures

Figure 1 - GWR Router	6
Figure 2 - GWR Router front panel	
Figure 3 - GWR Router back panel (GPRS and EDGE)	10
Figure 4 - GWR Router back panel (3G)	11
Figure 5 - GWR Router top panel side	11
Figure 6 - Declaration of conformity	
Figure 7 - User authentication	
Figure 8 - General router information	
Figure 9 - Network Information	
Figure 10 - WAN Information	17
Figure 11 - Network parameters configuration page	
Figure 12 - DHCP Server configuration page	
Figure 13 - WAN Settings configuration page	
Figure 14 – Routing configuration page	
Figure 15 – RIP configuration page	
Figure 16 – GRE tunnel parameters configuration page	
Figure 17 - IPSec Summary screen	
Figure 18 - IPSec Settings.	
Figure 19 – OpenVPN example	
Figure 20 – OpenVPN configuration page	
Figure 21 - IP Filtering configuration page	
Figure 22 - IP Filtering configuration example	
Figure 23 - IP Filtering settings	
Figure 24 - DynDNS settings	
Figure 25 - Serial Port Settings initial menu	
Figure 26 - Serial Port configuration page	
Figure 27 – Modbus gateway configuration page	
Figure 28 - Device Identity Settings configuration page	
Figure 29 - Administrator Password configuration page	
Figure 30 - Date/Time Settings configuration page	
Figure 31 - Diagnostic page	55
Figure 32 - Update Firmware page	
Figure 33 - File download	
Figure 33 - Default Settings page	
Figure 35 - System Reboot page	
Figure 36 – Command Line Interface	
Figure 37 – Remote Management	
Figure 38 – Connection Manager	
Figure 39 – Connection Wizard – Initial Step	
Figure 40 – Connection Wizard – Router Detection	
Figure 41 – Connection Wizard – LAN Settings	
Figure 42 – Connection Wizard – LAN Settings	
Figure 42 – Connection Wizard – WAN Settings Figure 43 - SNMP configuration page	
Figure 44 - Syslog configuration page	
Figure 45 - GWR Router as Internet router	
Figure 46 - GRE tunnel between two GWR Routers.	
Figure 47 - Network configuration page for GWR Router 1 Figure 48 - GRE configuration page for GWR Router 1	07 70
Figure 49 - Routing configuration page for GWR Router 1	
Figure 50 - Network configuration page for GWR Router 2	
Figure 51 - GRE configuration page for GWR Router 2	
Figure 52 - Routing configuration page for GWR Router 2	12
Figure 53 - GRE tunnel between Cisco router and GWR Router	13



Figure 54 - Network configuration page	74
Figure 55 - GRE configuration page	
Figure 56 - Routing configuration page	
Figure 57 - IPSec tunnel between two GWR Routers	
Figure 58 - Network configuration page for GWR Router 1	
Figure 59 - IPSEC configuration page I for GWR Router 1	
Figure 60 - IPSec configuration page II for GWR Router 1	
Figure 61 - IPSec configuration page III for GWR Router 1	80
Figure 62 – IPSec start/stop page for GWR Router 1	
Figure 63 – Default connection mode is <b>Wait</b>	80
Figure 64 - Network configuration page for GWR Router 2	81
Figure 65 - IPSEC configuration page I for GWR Router 2	82
Figure 66 - IPSec configuration page II for GWR Router 2	82
Figure 67 - IPSec configuration page III for GWR Router 2	83
Figure 68 – IPSec start/stop page for GWR Router 2	83
Figure 69 - IPSec tunnel between GWR Router and Cisco Router	
Figure 70 - Network configuration page for GWR Router	85
Figure 71 - IPSEC configuration page I for GWR Router	86
Figure 72 - IPSec configuration page II for GWR Router	86
Figure 73 - IPSec configuration page III for GWR Router	
Figure 74 – IPSec start/stop page for GWR Router	

## List of Tables

Table 1 - Technical parameters	7
Table 2 - GWR Router features	9
Table 3 - Network parameters	
Table 4 - DHCP Server parameters	19
Table 5 - WAN parameters	22
Table 6 – Advanced WAN Settings	
Table 7 – Routing parameters	
Table 8 – RIP parameters	
Table 9 – GRE parameters	31
Table 10 - IPSec Summary	33
Table 11 - IPSec Parameters	37
Table 12 – OpenVPN parameters	
Table 13 - IP filtering parameters	42
Table 14 – DynDNS parameters	45
Table 15 – Ser2IP parameters	
Table 16 - Serial port parameters	
Table 17 – Modbus gateway parameters	49
Table 18 - Device Identity parameters	51
Table 19 - Administrator password	53
Table 20 - Date/time parameters	54
Table 21 – Command Line Interface parameters	
Table 22 – Remote Management parameters	
Table 23 - SNMP parameters	
Table 24 - Syslog parameters	66

## **Description of the GPRS/EDGE/HSDPA Router**

Thank you for choosing Geneko GWR Router. The GWR Router is a compact electronic device based on different kind of GSM/UMTS modules which enables data transfers using GPRS/EDGE/HSDPA/HSUPA technologies. Primarily, the GWR Router expands the capabilities of GSM/UMTS module by the option of connecting entire LAN through the built-in Ethernet interface. The GWR Router provides automatic establishment and maintenance of GPRS/EDGE/HSDPA/HSUPA connection. Integrated DHCP server provides the users simple installation procedure and fast Internet access. Built-in VPN server provides VPN capabilities like GRE server/client, VPN IPSec/GRE pass through and VPN IPSec. Serial-to-IP and ModbusRTU-to-TCP conversions provide a wide variety of possible industry applications.



Figure 1 - GWR Router

## **Examples of Possible Application**

- mobile office;
- fleet management;
- security system;
- telemetric;
- remote monitoring;
- vending and dispatcher machines;



## **Technical Parameters**

		Directive	e 2004/108/EC			
	EMC	EN 301 489-1 V1.6.1(2005-09)				
	LIVIC		EN 301 489-7 V1.3.1(2005-11)			
	LVD		0-1:2001(1st Ed.) and/or EN 60950-1:2001			
Complies with		Directive 1999/05/EC				
standards	R&TTE		301 511 V9.0.2			
Standards	NOTIL		008-1 & EN 301 908-2(v2.2.1)			
			2002/95/EC			
	RoHS		mission 2005/618/EC, 2005/717/EC, 2005/747/EC,			
			D/EC, 2006/690/EC, 2006/691/EC and 2006/692/EC			
Ethernet interface	Connector F Standard: II Physical lay Speed: 10/1 Mode: full o	EEE 802.3 ver: 10/1001 100Mbps	J-45 EE 802.3 er: 10/100Base-T 00Mbps			
Other interfaces	1 x UART(RS-232C) 1 x USB Host					
	GWR202	GPRS	Tri-band: 900/1800/1900 GPRS multi-slot class 10, mobile station class B GPRS DL: 85.6Kbps, UL: 42.8Kbps			
	GWR252	GPRS EDGE	Quad band: GSM 850/900/1800/1900MHz GPRS/EDGE multi-slot class 12, mobile station class B EDGE DL: 236.8Kbps, UL: 236.8Kbps GPRS DL: 85.6Kbps, UL: 85.6Kbps			
RF characteristics	GWR352	GPRS EDGE UMTS HSDPA HSUPA	UMTS/HSDPA/HSUPA: Quad band, 850/900/1900/2100MHz GSM/GPRS/EDGE: Quad band, 850/900/1800/1900MHz GPRS/EDGE multi-slot class 12, mobile station class B HSUPA DL: 7.2Mbps, HSDPA: UL: 5.76Mbps UMTS DL: 384Kbps, UL: 384Kbps EDGE DL: 236.8Kbps, UL: 236.8Kbps GPRS DL: 85.6Kbps, UL: 85.6Kbps			
RF Connector	SMA, 50Ω					
Status LED	Ethernet activity / network traffic Power on GSM link activity Signal quality					
Power supply	9 – 12VDC .	/ 1000mA				
Temperature range	Operation: -5°C to +50°C Storage: -20°C to +85°C					
Physical characteristics	Width x Length x Height = 95 x 135 x 35 mm Weight 380g					

Table 1 - Technical parameters



## GWR Router features

Features	Short description
Network	
Routing	Static
DHCP Server:	
Static lease reservation	DHCP Server support
Address exclusions	
RIP	The Routing Information Protocol is a dynamic routing
RIP	protocol used in local and wide area networks
IP forwarding	IP, TCP, UDP packets from WAN to LAN
	DMZ, or De Militarized Zone, is a physical or logical
DM7 support	subnetwork that contains and exposes an organization's
DMZ support	external services to a larger untrusted network, usually
	the Internet.
	Simple Network Management Protocol is used in network
CNIMP: 1 2-	management systems to monitor network-attached
SNMPv1,2c	devices for conditions that warrant administrative
	attention
	The Network Time Protocol is a protocol for
NTP(RFC1305)	synchronizing the clocks of router
	Dynamic DNS (DDNS) is a domain name service allowing
DUEDNE	to link dynamic IP addresses to static hostname. To start
DynDNS	using this feature firstly you should register to DDNS
	service provider.
Firewall:	
• NAT	ID a dalara ( Naturala Ciltaria a
• PAT	IP address / Network filtering
IP filtering	
Ser2net	Serial to Ethernet converter
Modbus RTU-to-TCP gateway	Modbus to Ethernet converter.
VPN	
	Generic Routing Encapsulation is a tunneling protocol
GRE	that can encapsulate a wide variety of network layer
	protocol packet types inside IP tunnels
GRE Keepalive	Keepalive for GRE tunnels
IPSec pass-through	ESP tunnels
	Internet Protocol Security is a suite of protocols for
IPsec	securing IP communications by authenticating and
	encrypting each IP packet of a data stream
	OpenVPN site to site graphical user interface (GUI)
	implementation allows connecting two remote networks
OpenVPN	via point-to-point encrypted tunnel. OpenVPN
	implementation offers a cost-effective simply configurable
	alternative to other VPN technologies.
	Feature that allows a user to specify number of
IPSec IKE failover	unsuccessful retries to establish PPP connection before
	routers switches to another SIM.
IPSec tunnel failover	Quality control mechanism of IPSec tunnel.
Configuration	
WEB Application	HTTP based
Remote configuration	Access to web interface over mobile network
	basic functionality
Configuration via serial console	

## USER MANUAL

	full functionality
Default reset	external taster and configuration application
File Management	
Upload firmware	WEB/CLI
Backup configuration	WEB/CLI

Table 2 - GWR Router features



## **USER MANUAL**

#### Product Overview

## Front panel

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

- one RJ45 connector Ethernet port for connection into local computer network;
- one RJ45 connector for RS232 serial communication;
- reset button;
- one USB connector for connection of additional device;
- 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

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 in 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 blinks of the first and last signal strength LED on the top panel. This will restore the factory defaults and clear all custom settings of the GWR Router. You can also reset the GWR Router to factory defaults using the Maintenance > Default Settings screen.

## Back panel

On the back panel of device (Figure 3 and Figure 4) the following connectors are located:

- slot for SIM cards;
- SMA connector for connection of the GSM/UMTS antenna;



Figure 3 - GWR Router back panel (GPRS and EDGE)





Figure 4 - GWR Router back panel (3G)

## Top Panel

There is a sequence of 8 LED indicators on the top of this device by which the indication of the system current state, device power supply and presence of GSM/UMTS network as well as signal level is performed.



Figure 5 - GWR Router top panel side

LED Indicator Description:

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



- -107 or less dBm = Unacceptable (1 LED)
- -107 to -98 dBm = Weak (2 LED)
- -98 to -87 dBm = Moderate (3 LED)
- -87 to -76 dBm = Good (4 LED)
- -76 or better dBm = Excellent (5 LED).
- 0 is not known or not detectable (running LED)

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

#### Putting Into Operation

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

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

And finally, device should have power supply by power supply connector and the attached adaptor.

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



# USER MANUAL





Figure 6 - Declaration of conformity

## **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 gives administrator full set of privileges for configuring and monitoring. 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.

## 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 User name and Password. Default administration credentials are admin/admin.

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

	GWR ROUTER - CONFIGURATION CONSOLE	
Login		
	Username Password Login	
		-

Copyright © 2008 Geneko. All rights reserved http://www.geneko.co.rs/

Figure 7 - 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).



## NOTE

Add/Remove/Update manipulation in tables

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

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

To Update the row in the table:

• Change data directly in fields you want to change

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

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

#### Save/Reload changes

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

#### Status Information

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

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

### Status - General

**General Information** Tab provides general information about device type, device firmware version, kernel version, CPU vendor, Up Time since last reboot, hardware resources utilization and MAC address of LAN port. Screenshot of General Router information is shown at *Figure 8*. 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.



#### **GWR Series Router**

#### **USER MANUAL**

	GWR ROUTER - CONFIG	URATION CONSOLE	
Status General	General Information		
Network Information WAN Information	Router Information		
Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RP VPN Settings GRE PSec OpenVPN IP Filtering DynDNS Sanal Prot Maintenance Device Identity Settings	Model Firmware Version Kernel Version CPU Vendor UP Time Total Memory Used Memory Free Memory MAC Address SIM Card Detection	GWR252_test         21.9.30_252_test_2         2.6.21.5-geneko_v1         CirrusLogic ARM9 EP9302 200Mhz         00.11:55         296561K         24476K         5180K         00.1e-5c:00.90.red	
Administrator Password Diate/Time Settings Update Firmware Settings Backup Default Settings Rebod <b>Management</b> Command Line Interface Remote Management Connection Manager SNMP Logs Logout	Enable SIM Card Detection * SIM Card detection is performed only at times the second detection is disabled rooter be	ot up process will be faster.	Refresh

Figure 8 - General router information

Status - Network Information

**Network Information** Tab provides information about Ethernet port and Ethernet traffic statistics. Screenshot of Network Router information is shown in *Figure 9*.

Status - WAN Information

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

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

Screenshot of WAN Router information is shown in Figure 10.

## **GWR Series Router**

## USER MANUAL

	O GWR ROUTER - CONFIGURATION CONSOLE				
Status General	Network Information				
Network Information WAN Information	Network Statistics				
Settings Network	Network Technology	Ethernet	MAC Address	00:1e:5c:00:0b:ed	
DHCP Server	IP Address	192.168.1.1	MTU Size	1500	
WAN Settings Routing	Netmask	255.255.255.0	Broadcast	192.168.1.255	
Dynamic Routing Protocol RIP	100 000 V. V				
VPN Settings GRE	Data Received	200910	RX Packets	1694	
IPSec .	RX Error Packets	0	RX Dropped Packets	0	
OpenVPN IP Filtering	Data Transmitted	1089270	TX Packets	1566	
DynDNS Serial Port	TX Error Packets	0	TX Dropped Packets	0	
Maintenance	DHCP Server status	stopped			
Device Identity Settings Administrator Password					
Date/Time Settings Diagnostics					Refresh
Update Firmware Settings Backup					
Default Settings					
Reboot Management					
Command Line Interface Remote Management					
Connection Manager					
SNMP Logs					
Logout					
		Consuir	aht © 2008 Geneko, All rights reserved.		
		Cobyrig	http://www.geneko.rs/		



	GWR ROUTER - CONFIGURATION CONSOLE
Status	WAN Information
General Network Information WAN Information	Mobile Information
Settings Network	Modern Manufacturer huewei
DHCP Server	Madem Madel EM770W
WAN Settings Routing	Modern Serial Number 357030025512662
Dynamic Routing Protocol	Revision 11.126.10.81.00
VPN Settings	Mobile Connection
ORE IPSec	
OpenVPN	Operator Vip SRB
IP Filtering DynDNS	Cell ID 363
Serial Port	Phone Number
Maintenance Device Identity Settings	Signal Strength -73dBm
Administrator Password Date/Time Settings	Mobile Statistics
Diagnostics	
Update Firmware Settings Backup	Protocol Point-Point Protocol Activity Time 00:01:30
Default Settings	WAN Address 10.85.98.239 PPP Address 10.64.64.64
Reboot Management	Primary DNS Address 195.78.6.36 Second DNS Address 10.11.12.13
Command Line Interface	
Remote Management Connection Manager	Data Received         1158         RX Packets         45         RX Error Packets         0         RX Dropped Packets         0
SNMP Logs	Data Transmitted     498     TX Packets     45     TX Error Packets     0     TX Dropped Packets     0
	Refresh
Logout	
	Copyright @ 2009 Generals. All rights reserved. Hits/Nervix.genetors/s

Figure 10 - WAN Information



## Settings - Network

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

Network Tab Parameters				
Label	Description			
Use the following IP address	Choose this option if you want to manually configure TCP/IP parameters of Ethernet port.			
IP Address	Type the IP address of your GWR 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.			
Local DNS	Type the IP address of your local DNS server.			
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.			
Save	Click <b>Save</b> button to save your changes back to the GWR Router. Whether you make changes or not, router will reboot every time you click <b>Save</b> .			

Table 3 - Network parameters

In the Figure 11 you can see screenshot of **Network** Tab configuration menu.

	GWR ROLITER - CO	NFIGURATION CONSOLE		
HARDWARE				
	C			
Status	Network			<ul> <li>Help</li> </ul>
General				
Network Information WAN Information	Network Settings			
Settings	O Obtain an IP address a			
Network	Output the following IP add			
DHCP Server WAN Settings	IP Address	192.168.1.1		
Routing	CERTOSIA CONSTRUCTION DAVIS			
Dynamic Routing Protocol	Subnet Mask	255.255.255.0		
RP VPN Settings	Local DNS	195.78.6.36		
GRE	Caution: Changes to IP Address, subr	et mask and local DNS require a reboot to take effect.		
IPSec OpenVPN				Reload Save
IP Filtering				
DynDNS				
Serial Port Maintenance				
Device Identity Settings				
Administrator Password				
Date/Time Settings Diagnostics				
Update Firmware				
Settings Backup Default Settings				
Reboot				
Management				
Command Line Interface Remote Management				
Connection Manager				
SNMP				
Logs				
Logout				
		Copyright @ 2008 Geneko. All rig	to received	
		http://www.geneko.r		

Figure 11 - Network parameters 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 <b>Enable DHCP Server</b> . To setup DHCP server fill in the IP Starting Address and IP Ending Address fields. Uncheck <b>Enable DHCP Server</b> check box to stop the GWR Router from acting as DHCP server. When Unchecked, you must have another DHCP server on your LAN, or else the computers must be manually configured.				
IP Starting Address (From)	This field specifies the first of the contiguous addresses in the IP address pool.				
IP Ending Address (To)	This field specifies last of the contiguous addresses in the IP address pool.				
Lease Duration	This field specifies DHCP session duration time.				
Primary DNS, Secondary DNS	This field specifies IP addresses of DNS server that will be assigned to systems that support DHCP client capability. Select <b>None</b> 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 <b>Used by ISP</b> 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 <b>Used Defined</b> to have the GWR Router assign DNS IP address to DHCP clients. DNS address is manually configured by user.				
Static Lease Reservation	This field specifies IP addresses that will be dedicated to specific DHCP Client based on MAC address. DHCP server will always assign same IP address to appropriate client.				
Address Exclusions	This field specifies IP addresses that will be excluded from the pool of DHCP IP address. DHCP server will not assign this IP to DHCP clients.				
Add	Click <b>Add</b> to insert (add) new item in table to the GWR Router.				
Remove	Click <b>Remove</b> to delete selected item from table.				
Save	Click <b>Save</b> to save your changes back to the GWR Router.				
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.				

Table 4 - DHCP Server parameters

## **USER MANUAL**

	GWR ROUTER - CONFIGURATION CONSOLE	
Status	DHCP Server	<ul> <li>Help</li> </ul>
General Network Information WAN Information	DHCP Server Settings	
Settings	Enable DHCP server	
Network DHCP Server	IP Address range Lease Duration 1 days 0 hrs 0 mins	
WAN Settings	From	
Routing Dynamic Routing Protocol	To	
RP	Primary DNS Secondary DNS	
VPN Settings ORE	None     One	
IPSec OpenVPN	O Used by ISP Used by ISP	
IP Filtering	User Defined	
DynDNS Serial Port	Static Lease Reservations	
Senal Port Maintenance		
Device Identity Settings	IP addresses that will be dedicated to specific DHCP Client based on MAC address	
Administrator Password Date/Time Settings	Enable IP Address MAC Address Action	
Diagnostics	Add	
Update Firmware Settings Backup	Address Exclusions	
Default Settings Reboot		
Management	Exclude these address from the DHCP IP address pool	
Command Line Interface	Enable Start Address End Address Action	
Remote Management Connection Manager	Add	
SNMP	MAC Address format: sociolociolociolocio	Reload Save
Logs	* The IP address pool must specify addresses that are in the subnetwork of the GWR Router. The DHCP server will not operate if this configuration does not meet this requirement. * A reservation IP address must not be the same as the IP address of the DHCP server itief. If must be a valid IP address in the subnetwork of the DHCP server. The DHCP server will ignore a	Reload Save
Logout	reservation that does not meet these requirements. * An IP address scokulson range must specify valid IP addresses in the subnetwork of the DHCP server. The DHCP server will ignore an exclusion that does not meet this requirement.	
	Copyright @ 2008 Geneko. All rights reserved.	
	cupying i e zoos de lacio. Anglis i esterveu. Http://www.cenekors/	

Figure 12 - DHCP Server configuration page



## Settings - WAN Setting

Click **WAN Settings** Tab, to open the Wireless screen. Use this screen to configure the GWR Router GPRS/EDGE/UMTS/HSDPA/HSUPA parameters (*Figure 13*).

Status General	WAN Settings						Q Help
Network Information WAN Information	SIM 1				SIM 2		
Settings Network	Enabled				Enabled		
DHCP Server WAN Settings	Provider Authentication	VIP	CHAP V		Provider Authentication	DTAC CHAP	
Routing Dynamic Routing Protocol	Username	vipm		1	Username	rd72@edcpp.com	
RIP VPN Settings	Password	vipm	bile	j	Password	password	
GRE IPSec	APN	ipmol		]	APN	edc.pp	
Open∿PN IP Filtering	Dial string Number of retry	ATD:	'99 <sup>~~</sup> 1#	1	Dial string Number of retry	ATD*99***1# 3	
DynDNS Serial Port	PIN enabled	1234		1	PIN enabled	1234	
Maintenance Device Identity Settings	Enable network locking			7	Enable network looking		
Administrator Password Date/Time Settings					Enable failover	after 150 mins	
Diagnostics Update Firmware	Advanced						
Settings Backup Default Settings Reboot	Connection settings						
Management Command Line Interface	Persistent connection						
Remote Management Connection Manager	Reboot after failed connection	15					
SNMP Logs	Enable SIM 1 keepalive						
Logout	Connection type		Auto 🗸				
							Reload Save
	Mobile status						
		Mobile communication	large to				
	Mobile device type EM770W	unknown	Mobile provider Vip SRB	ppp_0			
	Current SIM card Current WAN address	SIM 1 10.85	96.234				
	Connection up time Connection status	00:48 conne					
						[e	tch SIM Refresh Disconnect
						ow	icition and theresing Disconnect

Figure 13 - WAN Settings configuration page

WAN Settings				
Label	Description			
Provider	This field specifies name of GSM/UMTS ISP. You can setup any name for provider.			
Authentication	This field specifies password authentication protocol. Select the appropriate protocol from drop down list. (PAP, CHAP, PAP - CHAP).			
Username	This field specifies Username for client authentication at GSM/UMTS network. Mobile provider will assign you specific username for each SIM card.			
Password	This field specifies Password for client authentication at GSM/UMTS network. Mobile provider will assign you specific password for each SIM card.			
APN	This field specifies APN.			
Dial String	This field specifies Dial String for GSM/UMTS modem connection initialization. In most cases you have to change only APN field based on parameters obtained from Mobile Provider. This field cannot be altered.			
Enable Failover	Check this field in order to enable failover feature. This feature is used when both SIM are enabled. You specify the amount of time after which Failover feature brings down current WAN connection (SIM2) and brings up previous WAN connection (SIM1).			
Enable network locking	Option that allows a user to lock a SIM card for a desired operator by specifying PLMN id of the operator. This option is very useful in border areas since you can avoid roaming expenses.			



Persistent connection	Keep connection alive, after Do not exit after a connection is terminated. Instead try to reopen the connection				
Reboot after failed connections	Reboot after n consecutive failed connection attempts.				
Enable SIM1/SIM2 keepalive	Make some traffic periodically in order to maintain connection active. You can set keepalive interval value in minutes				
Ping target	This field specifies the target IP address for periodical traffic generated using ping in order to maintain the connection active.				
Ping interval	This field specifies ping interval for keepalive option.				
Advanced ping interval	This field specifies the time interval of advanced ping proofing.				
Advanced ping wait for a response	This field specifies the timeout for advanced ping proofing.				
Maximum number of failed packets	This field specifies maximum number of failed packets in percent before keepalive action is performed.				
Keepalive action	This menu provides a choice between two possible keepalive actions in case maximum number of failed packets is exceeded. If Switch SIM option is selected router will try to establish the connection using the other SIM card after the maximum number of failed packets is exceeded. If Current SIM option is selected router will only restart the PPP connection.				
Connection type	Specifies the type of connection router will try to establish. There are three available options: only GSM, only UMTS and AUTO. For example, if you select Only GSM option, router will not try to connect to UMTS, instead router will automatically try to connect to GSM. By selecting AUTO option, router will first try to establish UMTS connection and if it fails, router will go for GSM connection.				
Mobile status	Displays data related to mobile connection. (current WAN address, uptime, connection status)				
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.				
Save	Click <b>Save</b> to save your changes back to the GWR Router.				
Switch SIM	Click Switch SIM try to establish the connection using the other SIM card.				
Refresh	Click <b>Refresh</b> to see updated mobile network status.				
Connect/ Disconnect	Click <i>Connect/Disconnect</i> to connect or disconnect from mobile network.				

Table 5 - WAN parameters

*Figure 13* shows screenshot of GSM/UMTS tab configuration menu. GSM/UMTS menu is divided into two parts.

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

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

	WAN Settings(advanced)					
Label	Description					
Enable	This field specifies if Advanced WAN settings is enabled at the GWR Router.					
Accept Local IP Address	With this option, pppd will accept the peer's idea of our local IP address, even if the local IP address was specified in an option.					
Accept Remote IP Address	With this option, pppd will accept the peer's idea of its (remote) IP address, even if the remote IP address was specified in an option.					
Idle time before disconnect (sec)	Specifies that pppd should disconnect if the link is idle for <i>n</i> 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 <i>n</i> (default 10).					
CHAP restart interval sec	Set the CHAP restart interval (retransmission timeout for challenges) to <i>n</i> 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	<b>4Pv2</b> With this option, pppd will not agree to authenticate itself to the peer using MS CHAPv2.					
Refuse EAP	With this option, pppd will not agree to authenticate itself to the peer using EAP.					
Connection debugging	Enables connection debugging facilities. If this option is selected, pppd will log the contents of all control packets sent or received in a readable form.					
Maximum Transmit Unit (bytes)	Set the MTU (Maximum Transmit Unit) value to <i>n</i> . 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 <i>n</i> bytes through the PPP network interface.					
Maximum Receive Unit (bytes)	Set the MRU (Maximum Receive Unit) value to <i>n</i> . Pppd will ask the peer to send packets of no more than <i>n</i> bytes. The value of <i>n</i> must be between 128 and 16384; the default is 1500.					
VJ-Compression	Disable Van Jacobson style TCP/IP header compression in both directions.					
VJ-Connection-ID Compression	Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression. With this option, pppd will not omit the connection-ID byte from Van Jacobson compressed TCP/IP headers.					
Protocol Field Compression	Disable protocol field compression negotiation in both directions.					
Address/Control Compression	Disable Address/Control compression in both directions.					
Predictor-1 Compression	Disable or enable accept or agree to Predictor-1 compression.					
BSD Compression	Disable or enable BSD-Compress compression.					



Deflate Compression	Disable or enable Deflate compression.			
Compression Control Protocol negotiation	Disable CCP (Compression Control Protocol) negotiation. This option should only be required if the peer is buggy and gets confused by requests from pppd for CCP negotiation.			
Magic Number negotiation	Disable magic number negotiation. With this option, pppd cannot detect a looped-back line. This option should only be needed if the peer is buggy.			
Passive Mode	Enables the "passive" option in the LCP. With this option, pppd will attempt to initiate a connection; if no reply is received from the peer, pppd will then just wait passively for a valid LCP packet from the peer, instead of exiting, as it would without this option.			
Silent Mode	With this option, pppd will not transmit LCP packets to initiate a connection until a valid LCP packet is received from the peer (as for the "passive" option with ancient versions of pppd).			
Append domain name	Append the domain name <i>d</i> 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 <i>n</i> 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 <i>n</i> seconds. Normally the peer should respond to the echo-request by sending an echo-reply. This option can be used with the <i>lcp-echo-failure</i> option to detect that the peer is no longer connected.			
Use Peer DNS	With this option enabled, router resolves addresses using ISP's DNS servers.			
Modem Initialization String	This field provides an option to directly specify AT commands.			
Roaming Mode	By enabling this option router will be able to connect to roaming network.			

Table 6 – Advanced WAN Settings

## Settings – Routing

The static routing function determines the path that data follows over your network before and after it passes through the GWR 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 14* shows screenshot of Routing page.



Routing					
Routing	Table Settings				
0					
	nt static routes		-	1	
Enab		Netmask	Gateway	Metric	Interface
V	10.1.1.0	255.255.255.252		0	gre1
	192.168.1.0	255.255.255.0	0.0.0.0	0	eth0
Annis	the following static rout	tes to the routing table			
Enab	-	Netmask	Gateway	Metric	Interface Ac
	0.0.0.0	0.0.0.0	*	1	ppp_0 V R
					ethû 🝸 A
Forward	ing				
	nable Network Address	Translation (MAT)			
vord 🗹 E	lable Network Address	mansiation (NAT)			
	rd protocol connections	s from external network:	s to the following inter	nal devices	
Forw		ol Send to			
	le Tunneling Protoco				
	le Tunneling Protoco GRE	10.0.0.1			
		10.0.0.1			
Enat	GRE ESP	10.0.0.2			
Enat	GRE ESP and TCP/UDP connection	10.0.0.2 ns from external networ	•		
Enat	GRE ESP and TCP/UDP connection Ie Protocol Destin	10.0.0.2 ns from external networ	tion Netmask Dest	ernal devices ination Port	Forward to
face t Forw	GRE ESP and TCP/UDP connection	10.0.0.2 ns from external networ	•		Forward to 192.168.1.1

Figure 14 – 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 inside the network
- Port translation Reroute TCP and UPD packets to desired destination inside the network.

Routing Settings				
Label	Description			
Routing Table				
Enable	This check box allows you to activate/deactivate this static route.			
Dest Network	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.			
Netmask	This parameter specifies the IP netmask address of the final destination.			
Gateway	This is the IP address of the gateway. The gateway is a router or switch (next hope) on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their final destinations. For every routing rule enter the IP address of the gateway. Please notice that <i>ppp0</i> interface has only one default gateway (provided by Mobile operator) and because of that there is no option for gateway when you choose <i>ppp0</i> interface.			
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.			

Interface	Interface represents the "exit" of transmission for routing purposes. In this case <i>Eth0</i> represents LAN interface and <i>ppp0</i> represents GSM/UMTS mobile interface of the GWR Router.			
VPN Traffic redirection				
Enable	This check box allows you to activate/deactivate this static Protocol translation.			
ESP	Encapsulated Security Payload (ESP) protects the IP packet data from third party interference, by encrypting the contents using symmetric cryptography algorithms. Unlike AH, the IP packet header is not protected by ESP. ESP operates directly on top of IP, using IP protocol number 50.			
GRE	Generic Routing Encapsulation (GRE) is a tunneling protocol designed to encapsulate a wide variety of network layer packets inside IP tunneling packets. The original packet is the payload for the final packet. GRE creates a virtual point-to-point link with routers at remote points on an IP Internet work. GRE uses IP protocol number 47.			
Send to	This field specifies IP address of the VPN server on local area network. VPN tunnel ends at this VPN server. You must use VPN tunnel option when configuring VPN connection, because of NAT.			
	TCP/UDP Traffic forwarding			
Enable	This check box allows you to activate/deactivate this static port translation.			
Protocol	Choose between TCP and UDP protocol.			
Destination IP	This field specifies IP address of the incoming traffic.			
Destination Netmask	This field specifies netmask for the previous address.			
Destination Port	This is the TCP/UDP port of application.			
Forward to IP	This filed specifies IP address where packets should be forwarded.			
Forward to port	Specify TCP/UDP port on which the traffic is going to be forwarded.			
Interface				
Add	Click <b>Add</b> to insert (add) new item in table to the GWR Router.			
Remove	Click Remove to delete selected item from table.			
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.			
Save	Click <b>Save</b> to save your changes back to the GWR Router. After pressing <b>Save</b> <i>button</i> it make take more than 10 seconds for router to save parameters and become operational again.			

Table 7 – Routing parameters

## Port translation

For incoming data, the GWR 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.

#### Settings – Dynamic Routing Protocol

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

#### Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm. The Routing Information Protocol provides great network stability, guaranteeing that if one network connection goes down the network can quickly adapt to send packets through another connection.

Click *RIP* Tab, to open the Routing Information Protocol screen. Use this screen to configure the GWR Router RIP parameters (*Figure 15*).

Geneko	GWR ROUTER - CONFIGURA	ATTON CONSOLE	
Status General	Routing Information Protocol		🥑 Help
Network Information WAN Information	Routing Manager		
Settings Network DHCP Server WAN Settings	Hostname Password	Router zebra	
Routing Dynamic Routing Protocol RP	Enable log Port to bind at O User defined		
VPN Settings ORE IPSec OpenVPN	© Default [2601]		
IP Filtering DynDNS Serial Port	Hostname	ripd	
Maintenance Device Identity Settings Administrator Password Date/Time Settings Diagnostics Update Firmware	Password Port to bind at OUser defined Opfault [2602]	zebra	
Settings Backup Default Settings Reboot			Reload Save
Management Command Line Interface Remote Management Connection Manager	Routing Information Protocol Status Status	s stopped	
SNMP - Logs			Start Stop Restart
Logout		Copyright © 2008 Geneko. All rights reserved. bttp://www.geneko.rs/	

Figure 15 – RIP configuration page



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

Table 8 – RIP parameters

#### RIP routing engine for the GWR Router

Use telnet to enter in global configuration mode.

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

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

router# router rip

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

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

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

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

Disable route redistribution:

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



Disable RIP update (optional):

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

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

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

Configure interface for RIP protocol

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

Disable rip authentication at all interface.

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

Debug commands:

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



#### Settings – VPN Settings

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

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

#### Generic Routing Encapsulation (GRE)

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

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

Solution where you can use GRE protocol:

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

Click **VPN Settings** Tab, to open the VPN configuration screen. In the *Figure 16* you can see screenshot of **GRE** Tab configuration menu.

VPN Settings / GRE Tunneling Parameters		
Label	bel Description	
Enable	This check box allows you to activate/deactivate VPN/GRE traffic.	
Local Tunnel Address	This field specifies IP address of virtual tunnel interface.	
Local Tunnel Netmask	This field specifies the IP netmask address of virtual tunnel. This field is unchangeable, always 255.255.255.252	
Tunnel Source	This field specifies IP address or hostname of tunnel source.	
Tunnel Destination	This field specifies IP address or hostname of tunnel destination.	
Interface	This field specifies GRE interface. This field gets from the GWR Router.	
KeepAlive Enable	Check for keepalive enable.	
Period	Defines the time interval (in seconds) between transmitted keepalive packets. Enter a number from 3 to 60 seconds.	
Retries	Defines the number of times retry after failed keepalives before determining that the tunnel endpoint is down. Enter a number from 1 to 10 times.	

#### **GWR Series Router**

### **USER MANUAL**

Add	Click <b>Add</b> to insert (add) new item in table to the GWR Router.
Remove	Click <i>Remove</i> to delete selected item from table.
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.
Save	Click Save to save your changes back to the GWR Router.

#### Table 9 – GRE parameters



Figure 16 – GRE tunnel parameters configuration page

## **GRE Keepalive**

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



## Internet Protocol Security (IPSec)

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

Click **VPN Settings** Tab, to open the VPN configuration screen. At the *Figure 17* you can see IPSec Summary screen. This screen gathers information about settings of all defined IPSec tunnels. You can define up to 5 Device-to-Device tunnels.

Geneko	GWR ROUTER - CONFIGURATION CONSOLE
Status General	Internet Protocol Security
Network Information WAN Information Settings Network DHCP Server	Summary       Tunnels used:     1       Maximum number of tunnels:     5
WAN Settings Routing Dynamic Routing Protocol RP VPN Settings	No. Name     Enabled     Status     Enc/Auth/Grp     Advanced     Local Group     Remote Group     Remote Gateway     Action     Connection mode       3     Test     yes     stopped     ph:r3DES/SH422     N     192,188.10     212,62.38.106     Edit     Delete     Connection     Weit
GRE IPSec OpenVPN IP Filtering DynDNS Serial Port	3 Test yes stopped ph2:30ESS/HAT/hone N 256.255.0 212.62.38.106 Edit Delete Connect Weit     * Redwing the MTU size on the clientide, can help eliminate some connectivity problems occurring at the protocol level     ** Redwind the MTU size on disk taids description     * Recommended MTU size on disk taids description     ** Toronic taids description
Benar Polt Maintenance Device Identity Settings Administrator Password Date/Time Settings Update Firmware Settings Backup Default Settings Reboot	standed     - jese in running       stopped     - jese in strunning or tunnel is not enabled       connecting     - jese is trutning to stabilith connection       wailing for connection     - jese is trutning for other and to connect       established     - tunnel is up
Management Command Line Interface Remote Management Connection Manager SNMP Logs	
Logout	Copyright @ 2088 Geneka. All rights reserved. thtp://www.geneka.rsf

Figure 17 - 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.	
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 <b>Start</b> button, only enabled tunnels will be started.	
Status	Field indicates status of the IPSec tunnel. Click on <b>Refresh</b> 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.	



## **USER MANUAL**

Remote Gateway	Field shows the IP address of the Remote Device.
Delete	Click on this link to delete the tunnel and all settings for that particular tunnel.
Edit	This link opens screen where you can change the tunnel's settings.
Connect	Router initiates the IPSec connection.
Wait	Router waits for IPSec connection.
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 10 - 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.

Add New Tunnel		
Tunnel Number Tunnel Name Enable		
Local Group Setup		
Local Security Gateway Type IP Address Custom Peer ID	IP Only	
Local Security Group Type IP Address		
Remote Group Setup		
Remote Security Gateway Type IP Address Custom Peer ID	IP Only	
Remote Security Group Type IP Address		

## **USER MANUAL**

IPSec Setup		
Keying Mode	IKE with Preshared key	
Phase 1 DH Group	Group2 V	
Phase 1 Encryption	3DES V	
Phase 1 Authentication	MD5 V	
Phase 1 SA Life Time	28800 sec	
Perfect Forward Secrecy		
Phase 2 Encryption	DES	
Phase 2 Authentication	MD5 💌	
Phase 2 SA Life Time	3600 sec	
Preshared Key		
Failover		
Enable IKE Failover		
IKE SA Retry		
Restart PPP After IKE SA Retry Exceeds :	incrited Limit	
C Restait FFF Alter INC 3A Relif Exceeds	pecilieu Ennie	
Enable Tunnel Failover		
Ping IP		
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	Destand (IDComp))	
	rotocor (in comp))	
Dead Peer Detection (DPD) 20 sec		
NAT Traversal		
Send Initial Contact		
		Back Reload Save

Copyright @ 2008 Geneko. All rights reserved. http://www.geneko.rs/

Figure 18 - 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 the type you want to use: IP Only - Only a specific IP address will be able to establish a tunnel, SIM Card – Router automatically uses IP address on WAN interface. <u>NOTE:</u> The Local Security Gateway Type you select should match the Remote Security Gateway Type selected on the IPSec device at the other end of the tunnel	
IP Address	The WAN (or Internet) IP address of the Router automatically appears. If the Router is not yet connected to the GSM/UMTS network this field is without IP address.	
Custom Peer ID	How the of the participant should be identified for authentication; Can be an IP address or a fully-qualified domain name preceded by @ .	
Local Security Group Type	Select the local LAN user(s) behind the Router that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. <u>NOTE:</u> The Local Security Group Type you select should match the Remote Security Group Type selected on the IPSec device at the other end of the tunnel.	
IP Address	Only the computer with a specific IP address will be able to access the tunnel.	
Subnet Mask	Enter the subnet mask.	



Remote Security Gateway Type	Select the remote LAN user(s) behind the Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. <u>NOTE:</u> The Remote Security Group Type you select should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.	
IP Address	Only the computer with a specific IP address will be able to access the tunnel.	
Custom peer ID	How the of the participant should be identified for authentication; Can be an IP address or a fully-qualified domain name preceded by @ .	
Remote Security Group Type	Select the remote LAN user(s) behind the Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. <u>NOTE:</u> The Remote Security Group Type you select should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.	
IP Address	Only the computer with a specific IP address will be able to access the tunnel.	
Subnet Mask	Enter the subnet mask.	
IPSec Setup	In order to establish an encrypted tunnel, the two ends of an IPSec tunnel must agree on the methods of encryption, decryption and authentication. This is done by sharing a key to the encryption code. For key management, the Router uses only IKE with Preshared Key mode.	
Keying Mode	IKE with Preshared Key IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Preshared Key to authenticate the remote IKE peer. Both ends of IPSec tunnel must use the same mode of key management.	
Phase 1 DH Group	Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol used during Phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits and Group 5 is 1536 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.	
Phase 1 Encryption	Select a method of encryption: DES (56-bit), 3DES (168-bit) or AES-128 (128-bit). The method determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Make sure both ends of the IPSec tunnel use the same encryption method.	
Phase 1 Authentication	Select a method of authentication: MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the IPSec tunnel use the same authentication method.	
Phase 1 SA Life Time	Configure the length of time IPSec tunnel is active in Phase 1. The default value is 28800 seconds. Both ends of the IPSec tunnel must use the same Phase 1 SA Life Time setting.	
Perfect Forward Secrecy	If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys. Both ends of the IPSec tunnel must enable this option in order to use the function.	
Phase 2 DH Group	If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits, and Group 5 is 1536 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You do not have to use the same DH Group that you used for Phase 1, but both ends of the IPSec tunnel must use the same Phase 2 DH Group.	
Phase 2 Encryption	Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec	



	sessions. Select a method of encryption: NULL, DES (56-bit), 3DES (168-bit) or AES-128 (128-bit). It determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Both ends of the IPSec tunnel must use the same Phase 2 Encryption setting. <u>NOTE:</u> 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. <u>NOTE:</u> If you select a NULL method of authentication, the previous Phase 2 Encryption method cannot be NULL.		
Phase 2 SA Life Time	Configure the length of time an IPSec tunnel is active in Phase 2. The default is 3600 seconds. Both ends of the IPSec tunnel must use the same Phase 2 SA Life Time setting.		
Preshared Key	This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., Ay_%4222 or 345fa929b8c3e. This field allows a maximum of 1023 characters and/or hexadecimal values. Both ends of the IPSec tunnel must use the same Preshared Key. <u>NOTE</u> : It is strongly recommended that you periodically change the Preshared Key to maximize security of the IPSec tunnels.		
Enable IKE failover	Enable IKE failover option which will try periodically to reestablish security association.		
IKE SA retry	Number of IKE retries before failover.		
Restart PPP After IKE SA Retry Exceeds Specified Limit	The router will restart PPP connection on the same provider after IKE SA retry exceeds specified limit.		
Enable tunnel failover	Enable tunnel failover. If there is more than one tunnel defined, this option will failover to other tunnel in case that selected one fails to established connection.		
Ping IP	IP address on other side of tunnel which will be pinged in order to determine current state.		
Ping interval	Specify time period in seconds between two ping		
Packet size	Specify packet size for ping message		
-	Time interval between advanced ping packets.		
Advanced Ping Wait For A Response	Advanced ping proofing timeout.		
Maximum numbers of failed packets	Set percentage of failed packets until failover action is performed.		
Compress (IP Payload Compression Protocol (IP Comp))	This option if you want the Router to propose compression when it initiates a		
Dead Peer Detection (DPD)	When DPD is enabled, the Router will send periodic HELLO/ACK messages to check the status of the IPSec tunnel (this feature can be used only when both peers or IPSec devices of the IPSec tunnel use the DPD mechanism). Once a dead peer has been detected, the Router will disconnect the tunnel so the connection can be re-established. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent). The default interval is 20 seconds.		
NAT Traversal	Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947. <u>NOTE:</u> If you select this mode the Aggressive mode will be automatically selected because it is obligatory option for NAT-T to work properly. <u>NOTE:</u> Keep-alive for NAT-T function is enabled by default and cannot be disabled. The default interval for keep-alive packets is 20 seconds.		
---	--	--	--
Send initial contact	The initial-contact status message may be used when one side wishes to inform the other that this is the first SA being established with the remote system. The receiver of this Notification Message might then elect to delete any existing SA's it has for the sending system under the assumption that the sending system has rebooted and no longer has access to the original SA's and their associated keying material.		
Back	Click <b>Back</b> to return on IPSec Summary screen.		
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.		
SaveClick Save to save your changes back to the GWR Router. After automatically goes back and begin negotiations of the tunnels by clic Start button.			

Table 11 - 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.





OpenVPN			
Label	Description		
IP Filtering			
Tunnel Number	Automatically assigned number of the tunnel.		
Tunnel Name	This field specifies tunnel name.		
Enable	Check this setting in order to enable OpenVPN tunnel.		
	Allow access from the following devices		
Authenticate Mode	<ul> <li>Choose one of the following options:</li> <li>none (Select this option if you do not want to use any kind of authentication)</li> <li>pre-shared secret (Select this option if you want to use PSK as a authentication method)</li> <li>username/password (Select this option if you want to use username/password along with CA Certificate as a authentication method)</li> <li>X.509 cert. (client) (Select this option if you want to use X.509 certificates as a authentication method in client mode)</li> <li>X.509 cert. (server) (Select this option if you want to use X.509 certificates as a authentication method in client mode)</li> </ul>		



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

Table 12 – OpenVPN parameters

Specify the IP address of the remote VPN tunnel endpoint.



Remote Interface IP

Address

## **GWR Series Router**

	GWR ROUTER - CONFIC	GURATION CONSOLE		
tus	OpenVPN			<ul> <li>Help</li> </ul>
Ceneral Network Information WAN Information HCP Server WAN Settings Routing Opnamic Routing Protocol RP VPN Settings GRE PSac OpnorVPN (PF Filtering DynDNS Sarial Port	Add New Tunnel Tunnel Number Tunnel Name Enable OpenVPN Setup Authenticate Mode Protocol UDP Port	1 none V UDP connect V 1194	]	
intenance Device Identity Settings Administrator Password Date/Time Settings Diagnostics	LZO Compression NAT Rules Keep Alive Max Fragment Size	          1300	bytes	
Update Firmware Settings Backup Default Settings Reboot	On some ©SM/UMTS networks, re- Local / Remote Group Setup	commended time for Keepalive Ping Interval is grater t	nan 10 seconds.	
Report anagement Command Line Interface Remote Management Connection Manager SNMP Logs igout	Remote Host or IP Adress Redirect Gateway Tunnel Interface Configuration Local Interface IP Address Remote Interface IP Address	manual configuration	] ]	
		Consulate @ 2009. Cons	sko, All richts reserved.	Back Reload Save

Figure 20 – OpenVPN configuration page



### Settings - IP Filtering

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

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

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

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

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



Service	This field specifies service of the host allow access to the GWR Router.		
Protocol	This field specifies protocol of the host allow access to the GWR Router.		
Port	This field specifies port of the host allow access to the GWR Router.		
Add	Click <b>Add</b> to insert (add) new item in table to the GWR Router.		
Remove	ove Click <i>Remove</i> to delete selected item from table.		
	Demilitarized Zone Host Settings		
DMZ Private IP Address	Demilitarized Zone Host Settings This check box allows/forbidden host to access to the GWR Router.		

## Table 13 - IP filtering parameters

	GWR ROUTER - CONFIGURATION CONSOLE
Status General	IP Filtering
Network Information WAN Information	General Settings
Settings Network DHCP Server	© Disable all ◎ Enable firewall
WAN Settings Routing	© Enable DMZ
Dynamic Routing Protocol RIP	Firewall Settings
VPN Settings OpenVPN PSec OpenVPN IP Filering DynONS Serial Port Maintenance Device Identity Settings Administrator Password Date/Time Settings Diagnostics Update Firmware Settings Backup	Automatically allow access from all devices on the local subnet         Allow access from the following devices         Enable       IP Address         Service       Protocol         Port       Action         Allow access from the following networks         Enable       IP Address         Subnet Mask       Service         Protocol       Port         Action         Allow access from the following networks
Default Settings Reboot <b>Management</b> Command Line Interface	Cuclion: Carefully review settings before applying changes. Incorrect settings can make the GWR Router inaccessible from the network. Demilitarized Zone Host Settings
Remote Management Connection Manager SNMP Logs	DMZ private IP address
Logout	Reload Save
	Copyright © 2008 Genetio. All rights reserved. <u>http://www.geneto.rs/</u>

Figure 21 - IP Filtering configuration page

## IP Filtering configuration example

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





	GWR ROUTER - CONFIGURATION CONSOLE	
Status General	IP Filtering	🕐 Help
Network Information WAN Information	General Settings	
Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol	<ul> <li>○ Disable all</li> <li>④ Enable firewall</li> <li>○ Enable DMZ</li> </ul> Firewall Settings	
RP VPN Settings GRE PSec OpenVPN IP Filtering DynDNS	Automatically allow access from all devices on the local subnet Allow access from the following devices Enable IP Address Service Protocol Port Action	
Serial Port	☑         192.168.1.1         ICMP         Rem	
Maintenance Device Identity Settings Administrator Password	Image: Wight of the state of the s	
Date/Time Settings Diagnostics Update Firmware	Image: Width Interface         Custom         UDP         69         Rem           Image: All Traffic interface         All Traffic interface         TCP/UDP         1-65535         Add	
Settings Backup Default Settings Reboot <b>Management</b>	Allow access from the following networks	
Command Line Interface Remote Management	Enable IP Address Subnet Mask Service Protocol Port Action	
Connection Manager SNMP	All Traffic V TCP/UDP 1-65535 Add	
Logs	Coudion: Carefully review settings before applying changes. Incorrect settings can make the OWR Router inaccessible from the network.	
Logout	Demilitarized Zone Host Settings	
	DMZ private IP address	
		Reload Save

Figure 23 - IP Filtering settings



## Settings – DynDNS

Dynamic DNS is a domain name service allowing to link dynamic IP addresses to static hostname. To start using this feature firstly you should register to DDNS service provider. Section of the web interface where you can setup DynDNS parameters is shown in figure 24.

	GWR ROUTER - CONFIGU	JRATION CONSOLE		
Status General	Dynamic DNS			Help
General Network Information WAN Information Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RP UPS Settings GRE PSec Open/PR IP Filtering Dyn0NS Sarial Port	DynDNS Settings DynDNS Cilent Service Hostname Username Password Maximum interval Number of tries Timeout Period	dyndns vork.com geneko317 ••••• 86400 10 120 5	96C 58C	
Maintenance Device Identity Settings Administrator Password Data Frime Settings Update Firmware Settings Backup Default Settings Rebod Management Command Line Interface Romute Management Connection Manager SMMP Logs	Status	started		Reload Seve
Logout		Copyright @ 2008 Genetic. All http://www.geneti		

Figure 24 - DynDNS settings

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



Period	Time between update retry attempts, default value is 1800.	
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.	
Save	Click <b>Save</b> to save your changes back to the GWR Router.	

Table 14 – DynDNS parameters

Settings - Serial Port

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 25 - Serial Port Settings initial menu

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	ndicates the number of bits in a transmitted data package.			
Parity	Checks for the parity bit. None is the default.			
Stop bits	The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission. The default is 1.			
Flow control	Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data. None is the default.			
Protocol	Choose which protocol to use [TCP/UDP].			
Mode	Select server mode in order to listen for incoming connection, or client mode to establish one.			
Bind to TCP/UDP port	Number of the TCP/UDP port to accept connections for this device. (Only on server side)			
Server IP address	Specify server IP address. (Only on client side)			
Connect to TCP/UDP port	Number of the TCP/UDP port to accept connections from this device. (Only c client side)			
Type of socket	Either <i>raw or telnet</i> . Raw enables the port and transfers all data like between the port and the log. Telnet enables the port and runs the telnet protocol on the port to set up telnet parameters.			
Check TCP connection	Enable connection checking.			
Kepalive idle time	Set keepalive idle time in seconds.			
Kepalive interval	Set time period between checking.			
Log level	Set importance level of log messages.			
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.			
Save	Click <b>Save</b> button to save your changes back to the GWR Router and activate/deactivate serial to Ethernet converter.			

Table 15 – Ser2IP parameters

Click Serial Port Tab to open the Serial Port Configuration screen. Use this screen to configure the GWR Router serial port parameters (*Figure 26*).



	GWR ROUTER - CONFIGURATION CONSOLE	
Status General Network Information WAN Information WAN Information Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RIP VPN Settings GRE IP Filtering Maintenance Administrator Password Device Identity Settings	Serial Port  Serial Port Settings  Enable configuration console  Enable serial-othernet converter  Bits per second: 57600  Data bits: 8  Parity: None  Parity: None  Flow control: None  Bind to port: 223	
Date/Time Settings Diagnostics Update Firmware Settings Backup Reboot Default Settings Management Senal Port SMP Logs	Type of socket:       raw         * Port: Valid value: [1-65535]         Copyright (a) 2008 Geneko. All rights reserved.         bttp://www.geneko.co.rs/	Reload Save

Figure 26 - Serial Port configuration page



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

Table 16 - Serial port parameters

## Modbus Gateway settings

The serial server will perform conversion from Modbus/TCP to Modbus/RTU, allowing polling by a Modbus/TCP master. The Modbus IPSerial Gateway carries out translation between Modbus/TCP and Modbus/RTU. This means that Modbus serial slaves can be directly attached to the unit's serial ports without any external protocol converters.

Click Serial Port Tab to open the Modbus Gateway configuration screen. Choose Modbus Gateway options to configure Modbus. At the Figure 27 you can see screenshot of Modbus Gateway configuration menu.

Modbus Gateway Parameters			
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. Valid data bits are: 8 and 7.		
Parity	Checks for the parity bit. Valid parity are: none, even and odd. None is the default.		
Stop bits	The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission. Valid stop bits are: 1 and 2. The default is 1.		
Flow control	Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data. None is the default.		
TCP accept port	This field determines the TCP port number that the serial server will listen for connections on. The value entered should be a valid TCP port number. The default Modbus/TCP port number is 502.		
Connection timeout	When this field is set to a value greater than 0, the serial server will close connections that have had no network receive activity for longer than the specified period.		
Transmission mode	Select RTU, based on the Modbus slave equipment attached to the port.		
Response timeout	This is the timeout (in milliseconds) to wait for a response from a serial slave device before retrying the request or returning an error to the Modbus master.		
Maximum number of retries	Should no valid response be received from a Modbus slave, the value in this field determines the number of times the serial server will retransmit request before giving up.		
Log level	Set importance level of log messages.		
Reload	Click <i>Reload</i> to discard any changes and reload previous settings.		
Save	Click <b>Save</b> button to save your changes back to the GWR Router and activate/deactivate serial to Ethernet converter.		

Table 17 – Modbus gateway parameters

#### **GWR Series Router**

	Serial Port			
eral work Information	0.110.00			
work information	Serial Port Settings			
S	Convert Settinger		(	
work	General Settings			
P Server	O Disable all			
N Settings ting	O Serial port over TCP/UDP settings			
mic Routing Protocol	Modbus gateway settings			
RP	Serial Port Settings			
Settings GRE	Bits per second	115200		
IPSec	Data bits			
OpenVPN				
iltering	Parity	none		
DNS al Port	Stop bits	1 💌		
nance	Flow control	none 💌		
ce Identity Settings	Modbus Gateway Settings			
ninistrator Password		500		
e/Time Settings nostics	TCP accept port	502		
ate Firmware	Connection timeout	60 sec		
ings Backup	Modbus Serial Settings		i de la companya de l	
ault Settings oot	Transmission mode	RTU		
ement				
nmand Line Interface	Response timeout	10 ms		
note Management	Maximum number of retries	3		
nection Manager //P	Log Settings			
3	Log level	level 3 💌		
	Logiever	IBVBI J		
	Status	stopped		
				Reload

Figure 27 – Modbus gateway configuration page



#### 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 - 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 28*.

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 <b>Save</b> button to save your changes back to the GWR Router.		
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.		

Table 18 - Device Identity parameters

	GWR ROUTER - CONFIG	URATION CONSOLE	
<b>Status</b> General	Device Identity Settings		<ul> <li>Help</li> </ul>
Network Information WAN Information	Settings		
Settings Network DHCP Server	Name Description	Test241 TestNewFW	
WAN Settings Routing <b>Dynamic Routing Protocol</b>	Location	PPLab	
RIP VPN Settings GRE			Reload Save
IPSec OpenVPN IP Filtering DynDNS Senial Port			
Setton Pills Maintenance Device Identity Settings Administrator Password Data/Time Settings Update Firmware Settings Backup Default Settings Reboot			
Management Command Line Interface Remote Management Connection Manager SNMP Logs			
Logout			
		Copyright © 2008 Geneko. All rights reserved. http://www.geneko.rs/	

Figure 28 - Device Identity Settings configuration page



Maintenance - Administrator Password

By **Administrator Password** Tab it is possible to activate and deactivates device access system through **Username** and **Password** mechanism. Within this menu change of authorization data Username/Password is also done. **Administer Password** Tab window is shown on *Figure 29*.

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.

	GWR ROUTER - CONFIGURATION	N CONSOLE	
<b>Status</b> General	Administrator Password		@ Help
Network Information WAN Information	Password		
Settings Network	Enable Password Authentication	admin	
DHCP Server WAN Settings	Old Password		
Routing Dynamic Routing Protocol	New Password		
RP VPN Settings	Confirm Password		
GRE IPSec	9		Reload Save
OpenVPN IP Filtering			
DynDNS Serial Port			
Maintenance Device Identity Settings			
Administrator Password Date/Time Settings			
Diagnostics Update Firmware			
Settings Backup Default Settings			
Reboot Management			
Command Line Interface Remote Management			
Connection Manager SNMP			
Logs			
Logout			
		Copyright © 2008 Geneko. All rights reserved. http://www.geneko.rs/	

Figure 29 - Administrator Password configuration page



Administrator Password			
Label	Description		
Enable Password Authentication	By this check box you can activate or deactivate function for authentication when you access to web/console application.		
Username	This field specifies Username for user (administrator) login purpose.		
Old Password	Enter the old password. The default is <i>admin</i> when you first power up the GWR Router.		
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.		
Save	Click <b>Save</b> button to save your changes back to the GWR Router.		
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.		

Table 19 - Administrator password

## Maintenance - Date/Time Settings

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

	GWR ROUTER - CONFIGURATION CONSOLE	
Status General	Date/Time Settings	@ Help
Network Information WAN Information	Current Date and Time	
Settings Natwork DHCP Server WAN Settings	Date         2011 / 07 / 16           Time         11 : 33 : 45	
Routing Dynamic Routing Protocol RIP	Date and Time Setup	
NP VPN Settings GRE PSec OpenVPN IP Fittering	Update router date and time ◯ Manually ⓒ From time server	
DynDNS Serial Port Maintenance	Date         2011 v / 07 v / 16 v           Time         11 v : 33 v : 45 v	
Device Identity Settings Administrator Password (Date/Time Settings) Diagnostics Ugdate Firmware Settings Backup Default Settings Reboot Management Command Line Interface Remote Management Connection Manager	Time protocol     NTP (RFC-1305)        Time server address     77.105.37.0       Time zone     (GMT +1:00 hours) CET (Centrel Europe Time). Belgrade. Copenhagen. Madrid, Paris       Automatically synchronize NTP       Update time every     min	~
SNMP Logs		Sync Clock Reload Save
Logout	Copyright © 2008 Genetio. All rights reserved. kttp://www.agreko.rs/	

Figure 30 - Date/Time Settings configuration page



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

Table 20 - 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.

	GWR ROUTER	- CONFIGURATION CONSOLE	
Status General	Diagnostics		@ Help
Network Information WAN Information	Ping Utility		
Settings Network	Ping the IP address	of a device in order to communicate with it.	
DHCP Server WAN Settings	IP Address	192.168.1.20	
Routing Dynamic Routing Protocol RIP VPN Settings GRE IPSec	Response	Average response time is 2.6ms Average response time is 1ms Average response time is 1.2ms Average response time is 1.8ms	
OpenVPN IP Filtering DynDNS Serial Port			Ping
Maintenance Device Identity Settings Administrator Password Date/Time Settings Update Firmware Settings Backup Default Settings Reboot Management Command Line Interface Remote Management Connection Manager SMMP Logs			
Logout			2009 Genelio. Al rights reserved. Its://www.genelio.rs/

Figure 31 - 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.

	GWR ROUTER - CONF	FIGURATION CONSOLE	
Status General	Update Firmware		
Network Information WAN Information	Update		
Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RP VPN Settings	2. Please don't close the wind 3. In order to activate new firm 4. Clear browser cache after Current firmware version	2.1.9.30_352_test_2	
GRE IPSec	Select firmware	Browse_	
OpenVPN IP Filtering DynDNS Serial Port		Upic	oad
Maintenance Davice Identity Settings Administrator Password DiagOTime Settings Diagnostics Update Firmware Settings Backup Default Settings Rebool Management Command Line Interface Remote Management Connection Manager SIMMP Logs Logout			
		Copyright © 2008 Ceneto. All rights reserved. Ithu //www.aereko.rs/	

Figure 32 - Update Firmware page

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

Maintenance - Settings Backup

This feature allows you to make a backup file of your preferences file for the GWR Router. To save the backup file, you need to export the configuration file. To use the backup preferences file, you need to import the configuration file that you previously exported.

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, click *Export*.



Opening confFile.b	kg	×
You have chosen to op	en	
📄 confFile.bkg		
which is a: BKG	file	
from: http://10	0.10.150	
What should Firefox	do with this file?	-
Open with	Notepad (default)	
◯ FlashGot		
Save File		
Do this autor	natically for files like this from now on.	
6		
	OK Cancel	

Figure 33 - File download

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

### Maintenance - Default Settings

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

	GWR ROUTER - CONFIGURATION CONSOLE	
Status General Network Information WANI Information WANI Information Settings DHCP Sener WAN Settings Dynamic Routing Protocol Routing Dynamic Routing Protocol Routing Dynamic Routing Protocol	Default Settings         Settings         Be carefull when restoring factory default settings. The factory settings will clear all current settings and reboot the system.         Keep network settings	store
	Copyright © 2008 Geneto. All rights reserved. title/Avvew.geneto.rs/	

Figure 34 - 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.

	GWR ROUTER - CONFIGURATION CONSOLE
Conception Concep	Control - Control Control Control -
	rtin.//www.aeneko.ts/
	Figure 35 - System Reboot page



#### Management – Command Line Interface

CLI (command line interface) is a user text-only interface to a computer's operating system or an application in which the user responds to a visual prompt by typing in a command on a specified line and then receives a response back from the system.

In other words, it is a method of instructing a computer to perform a given task by "entering" a command. The system waits for the user to conclude the submitting of the text command by pressing the "Enter" or "Return" key. A command-line interpreter then receives, parses, and executes the requested user command.

On router's Web interface, in Management menu, click on Command Line Interface tab to open the Command Line Interface settings screen. Use this screen to configure CLI parameters (Figure 36).

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

Table 21 – Command Line Interface parameters

	GWR ROUTER - CONFIG	IRATION CONSOLE
Status General Network Information WAN Information Settings Utwork. DHCP Sener WAN Sattings Routing Dynamic Routing Protocol RP OPEN GRE PSes OpenVPN IP Filtering DynONS Serial Port	Command Line Interface CLI Settings CLI on View Mode Username View Mode Deseword Confirm Password View Mode Timeout Edit Mode Timeout	Teinet ▼         admin         •••••         180         180         sec
Beneration of Maintenance Maintenance Device Identity Settings Administrator Password Diagnostics Update Firmware Settings Backup Default Sattings Rebod Management Command Line Interface Remote Management Conscion Manager SIMP Logs	Console Type	Tother
		Copyright @ 2009 Genetio. All rights reserved. <u>http://www.genetio.rs/</u>

Figure 36 – Command Line Interface



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

### Management – Remote Management

Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of GWR routers. More information about this utility can be found in other document (Remote\_Management.pdf). In order to use this utility user has to enable Remote Management on the router (Figure 37).

	GWR ROUTER - CONFIGURATION CONSOLE	
Status General Network Information WAN Information Settings Network DHCP Server	Remote Management  Remote Management Settings  Enable Remote Management Protocol Geneko	Help
WAN Settings Routing RP RP VPN Settings GRE PSec Open/PN	Bind to     ppp       TCP port	
IP Filtering DynDNS Serial Port <b>Maintenance</b> Device Identity Settings	Status requesting status	Reload Save
Administrator Password Date/Time Settings Diagnostics Update Firmware Settings Backup Default Settings Reboot		
Management Command Line Interface Remote Management Connection Manager SNMP Logs		
Logout	Copyright © 2009 Geneko. All rights reserved. <u>Inter/Ivwww.geneko.rs/</u>	

Figure 37 – Remote Management

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

Table 22 – Remote Management parameters



#### Management - Connection Manager

Enabling Connection Manager will allow Connection Wizard (located on setup CD that goes with the router) to guide you step-by-step through the process of device detection on the network and setup of the PC-to-device communication. Thanks to this utility user can simply connect the router to the local network without previous setup of the router. Connection Wizard will detect the device and allow you to configure some basic functions of the router. Connection Manager is enabled by default on the router and if you do not want to use it you can simply disable it. (Figure 38).

Status	Connection Mana	ager			@ Help
General Network Information WAN Information	Connection Manage	er			
Settings Network	Enable Connection	ı Manager			
DHCP Server WAN Settings	Connection Manage	er Status			
Routing Dynamic Routing Protocol	Status	started			
RIP VPN Settings					Reload Save
GRE IPSec OpenVPN					
IP Filtering DynDNS					
Serial Port Maintenance					
Device Identity Settings Administrator Password Date/Time Settings					
Date/Time Settings Diagnostics Update Firmware					
Settings Backup Default Settings					
Reboot Management					
Command Line Interface Remote Management					
Connection Manager SNMP					
Logs					
Logout			Copyright @ 2008 Geneko. All rights resi	erveri	
			http://www.geneko.rs/	un Yhada	

Figure 38 – Connection Manager

Getting started with the Connection Wizard:

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

- **GWR 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/HSDPA/HSUPA network connection** Selecting this option you can configure parameters for LAN and WAN interface





Figure 39 – 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 40 – Connection Wizard – Router Detection



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

	Gen	eko Wirel	ess Route	r Conne	ction Wiz	ard
	IP address: Subnet mask:	192.168.1.1 255.255.255.0				
🕞 сепеко			Refresh	Back	Finish	Cancel

Figure 41 – 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.

	Genel	ko Wireless Route	r Conne	ction Wiz	ard
1	WAN Settings				
	Enabled				
12 -	Provider:	VIP			
Come and	Authentication:	PAP-CHAP	~		
201	Username:	vipmobile			
	Password:	vipmobile			
	Dial string:	ATD*99***1#			
	Initial string:	at+cgdcont=1,\"IP\",\"vipmobile\"			
	Number of retry:	3			
<b>С</b> сепеко	Establish connec	tion			
Geneko					
		Refresh	Back	Finish	Cancel
		nellesh	Dack	FILISTI	Cancer

Figure 42 – Connection Wizard – WAN Settings

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



Management - Simple Management Protocol (SNMP)

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

	GWR ROUTER - CONFIG	JRATION CONSOLE	
<b>Status</b> General	Simple Network Manageme	nt Protocol	🕑 Help
Network Information WAN Information	SNMP Settings		
Settings Network	Enable SNMP		
DHCP Server WAN Settings	Get Community	public	
Routing Dynamic Routing Protocol RP	Service Port		
VPN Settings ORE	<ul> <li>Default [161]</li> </ul>		
IPSec OpenVPN	Service Access	All	
IP Filtering DynDNS	SNMP Status		
Serial Port Maintenance	Status	started	
Device Identity Settings Administrator Password Date/Time Settings Diagnostics Update Firmware Settings Backup Default Settings Reboot			Reload Save
Management Command Line Interface Remote Management Connection Manager SNMP Logs			
Logout			
		Copyright © 2008 Geneko. Al http://www.gene	

Figure 43 - 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 <b>public</b> . It supports up to 64 alphanumeric characters.				
Service Port	Sets the port on which SNMP data has been sent. The default is 161. You can specify port by marking on user defined and specify port you want SNMP data to be sent.				
Service Access	Sets the interface enabled for SNMP traps. The default is Both.				
Reload	Click <b>Reload</b> to discard any changes and reload previous settings.				
Save	Click <b>Save</b> button to save your changes back to the GWR Router and enable/disable SNMP.				

Table 23 - SNMP parameters

#### Management - Logs

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

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

	GWR ROUTER - CONFI	CURATION CONSOLE	
Status General	System Logger		🕐 Help
Network Information WAN Information	Syslog Status		
Settings Network	O Disable		
DHCP Server WAN Settings	<ul> <li>Remote syslog</li> <li>Local syslog</li> </ul>		
Routing Dynamic Routing Protocol			
RIP VPN Settings	Status	started	
GRE	Remote Syslog		
OpenVPN IP Filtering	Service server IP	192.168.23.106	
DynDNS Serial Port	Service port		
Maintenance Device Identity Settings	Default [514]		
Administrator Password Date/Time Settings	Local Syslog		
Diagnostics Update Firmware	Syslog file size	1024 💌 KB	
Settings Backup Default Settings	Event log	All	
Reboot Management	Enable syslog saver		
Command Line Interface Remote Management	Save log every	1 hours	
Connection Manager SNMP			Reload Save
Logs	System Log		
Logout	- , ,		
	I.		

#### Figure 44 - 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.
Remote syslog	Mark this option in order to enable logging on remote machine.
Local syslog	Start logging facility locally.
Remote Syslog	Description
Service Serve IP	The GWR Router can send a detailed log to an external Syslog server. The Router's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP service, and number of bytes transferred. Enter the Syslog server name or IP address.
Service Port	Sets the port on which Syslog data has been sent. The default is 514. You can specify port by marking on user defined and specify port you want Syslog data to be sent.



User defined	Set manually port number.
Default	Use standard port number for this service. [514]
Local syslog	Description
Syslog file size	Set log size on one of the six predefined values. [10/20/50/100/200/500]kb
Event log	Choose which events to be stored. You can store System, Ipsec events or both of them.
Enable syslog saver	Save logs periodically on filesystem.
Save log every	Set time duration between two saves.
Reload	Click <i>Reload</i> to discard any changes and reload previous settings.
Save	Click <b>Save</b> button to save your changes back to the GWR Router and enable/disable Syslog.

Table 24 - Syslog parameters

### Logout

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



# **Configuration Examples**

GWR 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 45 - GWR Router as Internet router

- Click *Network* Tab, to open the LAN NETWORK screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP address: 10.1.1.1
  - Netmask: 255.255.255.0
- Press *Save* to accept the changes.
- Use SIM card with a dynamic/static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider's network default gateway).
- Click **WAN** Settings Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be provided by your mobile operator.
- Check the status of GSM/UMTS connection (WAN Settings Tab). If disconnected please click Connect button.
- Check *Routing* Tab to see if there is default route (should be there by default).
- Router will automatically adds default route via ppp0 interface.
- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.
- Configure the GWR 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 isn't a secure tunneling method. Simple network with two GWR Routers is illustrated on the diagram below (*Figure 46*). Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.



Figure 46 - 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 *Network* Tab, to open the LAN NETWORK screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
  - IP Address: 192.168.4.1
  - Subnet Mask: 255.255.255.0
  - Press Save to accept the changes.



	GWR ROUTER - CO	INFIGURATION CONSOLE	
Status General Network Information WAN Information Settings	Network Network Settings O Obtain an IP address -	aufomatically using DHCP	💽 Help
Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RP VPN Settings	<ul> <li>Use the following IP ad IP Address</li> <li>Subnet Mask</li> <li>Local DNS</li> </ul>		
GRE IPSec Open/VPN IP Filtering DynDNS Serial Port Maintenance	Caution: Changes to IP Address, sut	onet mask and local DNS require a reboot to take effect.	Reload Save
Dexice Identity Settings Administrator Password Date/Time Settings Diagnostics Update Firmware Settings Backup Default Settings Reboot <b>Management</b> Command Line Interface Remote Manager SIMMP			
Logs Logout		Copyrigit © 2008 Genetio. A http://www.gene	

Figure 47 - 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 **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.
- Click **VPN Settings** > **GRE** to configure GRE tunnel parameters:
  - Enable: yes
  - Local Tunnel Address: 10.10.10.1
  - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252)
  - Tunnel Source: 10.251.49.2 (select HOST from drop down menu if you want to use host name as peer identifier)
  - Tunnel Destination: 10.251.49.3 (select HOST from drop down menu if you want to use host name as peer identifier)
  - KeepAlive enable: no
  - Period:(none)
  - Retries:(none)
  - Press ADD to put GRE tunnel rule into GRE table.
  - Press Save to accept the changes.



#### **GWR Series Router**

#### **USER MANUAL**

s																<b>?</b> +
eneral																
etwork Information AN Information	Generic Rout	ting Encapsulatio	on (GRE) Tu	inneling												
1gs	Enable	Local Tunnel A	Address	Local Tunnel Netn	nask		Tunne	Source		Tunn	el Destination	Interface	KeepAlive Enable	Period	Retries	Actio
stwork		10.10.10.1		255,255,255,252		IP	<ul><li>10</li></ul>	.251.49.2	IP	~	10.259.49.3	gre1				Rem
ICP Server			_		_	_				~						
AN Settings uting				255.255.255.252		IP	*		IP	~						Add
amic Pouting Protocol				10.0												
		ss: IP Address of virtual sk: (Unchangeable, ah												R	eload	Sav
Settings	Funnel Source: IP a	ddress of tunnel source	e													
OPE		IP address of tunnel de	lestination													
	Period: Valid values Retries: Valid values															
OpenVPN	setties, valid values	[1-10]														
Filtering																
DNS																
IDNS																
DNS al Port																
DNS al Port <b>nance</b> ice Identity Settings																
DNS ial Pont m <b>ance</b> ice Identity Settings																
DNS <sup>®</sup> lal Port m <b>ance</b> ice Identity Settings ninistrator Password																
DNS al Port nance ce Identity Settings imistrator Password «Time Settings inostics																
DNS <sup>°</sup> al Port <b>nance</b> ce Identity Settings inistrator Password //Time Settings nostics at Firmware																
DNS <sup>*</sup> al Port nance ninistrator Password //ime Settings prostics ate Firmware ings Backup																
DNS al Port nance ce Identity Settings inisistator Password /Time Settings mostics ate Firmware ngs Backup ull Settings																
DNS al Port nance ce Identity Settings inisistator Password /Time Settings mostics ate Firmware ngs Backup ull Settings																
DNS a Port tance te Identity Settings inistrator Password Trime Settings nostics te Firmware ngs Backup ult Settings tot																
INIS I Fort I Fort e Identity Settings mistrator Password Trime Settings nositics te Firmware ngs Backup it Settings ot ment Initerface																
DNS a Port tance so Identity Settings inistrator Password Trime Settings nostics the Firmware ngs Backup uit Settings bot sment ment Interface																
DNS al Port nance ce Identity Sattings yrinne Sattings mostice ate Firmware date Firmware hings Backup ult Sattings oot ement mand Line Interface note Managerment nection Manager																
IDNS ala Port mance la Port inistrator Password PTime Settings gnostics late Firmware litage Sackup aud Settings not rement mmand Line Interface note Manager MP																
nDNS iai Port enance derntity Settings ministrator Password e/Time Settings ganostics fate Firmware tate Settings aud Settings soot gement mmand Line Interface mote Manager MP																
nDNS inai Port snance inai Port ministrator Password diministrator Password diministrator Password formas for Settings satistic Settings soot soot soot soot soot soot hanagement meedion Manager MP																
IDNS ital Port inal Port ininistrator Password //Time Settings gnostics fate Firmware tings Backup ault Settings boot Jement mmand Line Interface note Manager MP is																
Fiteining moNS miai Pont <b>enance</b> <b>enance</b> ministrator Password lef/Time Settings fitmings Backup fault Settings <b>gement</b> mmand Line Interface mmote Manager IMP gs																

Figure 48 - GRE configuration page for GWR Router 1

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

Figure 49 - Routing configuration page for GWR Router 1

- Optionally configure IP Filtering and TCP service port settings 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 **Network** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.



- IP Address: 192.168.2.1
  - Subnet Mask: 255.255.255.0
- Press **Save** to accept the changes.

	GWR ROUTER - CO	INFIGURATION CONSOLE		
Status	Network			🕑 Help
General Network Information WAN Information Settings	Network Settings			
Network DHCP Server	<ul> <li>O Obtain an IP address</li> <li>O Use the following IP at</li> </ul>			
WAN Settings Routing	IP Address	192.168.2.1		
Dynamic Routing Protocol	Subnet Mask	255.255.255.0		
RIP VPN Settings	Local DNS			
GRE IPSec	Changes to IP Address, su	net mask and local DNS require a reboot to take effect.		Reload Save
OpenVPN IP Filtering				
DynDNS Serial Port				
Maintenance Device Identity Settings				
Administrator Password Date/Time Settings				
Diagnostics Update Firmware				
Settings Backup Default Settings				
Reboot Management				
Command Line Interface				
Remote Management Connection Manager SNMP				
Logs				
Logout				
		Copyright © 2008 Geneko. All r		
		http://www.geneko	<u>0.15/</u>	

Figure 50 - 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
  provider's network default gateway).
- Click **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.
- Click **VPN Settings** > **GRE** to configure GRE tunnel parameters:
  - Enable: yes
  - Local Tunnel Address: 10.10.10.2
  - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252)
  - Tunnel Source: 10.251.49.3 (select HOST from drop down menu if you want to use host name as peer identifier)
  - Tunnel Destination: 10.251.49.2 (select HOST from drop down menu if you want to use host name as peer identifier)
  - KeepAlive enable: no
  - Period:(none)
  - Retries:(none)
  - Press ADD to put GRE tunnel rule into GRE table.
  - Press **Save** to accept the changes.



#### **GWR Series Router**

### **USER MANUAL**

tus															? ⊦
General															
Network Information	Generic Rout	ting Encapsulation	ion (GRE) T	unneling											
WAN Information	[ water and ]								-						
tings	Enable	Local Tunnel A	Address	Local Tunnel Net			nnel Sour			nel Destination	-	KeepAlive Enable	Period	Retries	
letwork IHCP Server	<b>V</b>	10.10.10.2		255.255.255.252	2	IP 💌	10.251.49	9.3	IP 💌	10.251.49.2	gre1				Rem
ACH Settings				255,255,255,255	2	IP 🗸			IP V						Add
outing				200.200.200.202	2				IP Y						Aug
amic Routing Protocol				19.10											
		s: IP Address of virtua sk: (Unchangeable, al											B	eload	Save
		idress of tunnel source		.200.202)											
OPE		IP address of tunnel d	destination												
	Period: Valid values Retries: Valid values														
OpenVPN	Netries: Valid values	[1-10]													
Filtering nDNS															
Filtering nDNS															
Filtering nDNS mal Port															
Filtering nDNS rrial Port <b>cenance</b>															
Filtering InDNS Irrial Port <b>enance</b> vice Identity Settings															
Filtering nDNS mial Port <b>enance</b> vice Identity Settings ministrator Password Ier/Time Settings															
Filtering nDNS anal Port enance vice Identity Settings ministrator Password ter/Time Settings signostics															
Filtering nDNS aia Port enance vice Identy Settings ministrator Password te/Time Settings agnostics date Firmware															
Filtering nDNS enance vice Identity Settings ministrator Password te/Time Settings sgnostics date Firmware tings Backup															
Filieinig noINS rial Port enance vice Identity Settings vice Identity Settings Holf Time Settings ugnostics date Firmware ttings Backup fault Settings															
Fillering nDNS enance ice Identity Settings ministrator Password Ie/Time Settings geostice date Firmware tinge Backup Maut Settings boot															
Filtering nDNS enance woo Identity Settings ministrator Password Ite/Time Settings date Firmware tings Backup tauft Settings boot															
Filtering nDNS enance wice Identity Settings wice Identity Settings (Filtmes Settings sugnostics date Firmware titings Backup fault Settings boot gement mmand Line Interface															
Fiteing nDNS rial Pont enance wice Identity Settings refines Settings agnostics date Firmware ttings Backup fault Settings boot gement mmand Line Interface mote Management															
Filtering noINS noI Port enance vice Identity Settings wice Identity Settings ugnostics date Firmware trings Backup fault Settings boot gement monte Management mote Management mote Management															
Filieining DNS mail Port enance enance elfrime Settings ugostics date Firmware titings Backup datit Settings boot gement mmand Line Interface motel Management nnection Manager MP															
Fitering nDNS rial Port <b>enance</b> wrice Identity Settings wrice Identity Settings agnostics date Firmware titlings Backup date Firmware titlings Backup date Firmware titlings boot <b>gement</b> mmand Line Interface monted Managerent MP															
Fitering nDNS mal Port enance wice Identty Settings immistrator Password telfTims Settings agnostics date Firmware tittings Backup fault Settings boot gement immand Line Interface mote Managernent MP gg gg															
Fitering nDNS mal Port enance wice Identty Settings immistrator Password telfTims Settings agnostics date Firmware tittings Backup fault Settings boot gement immand Line Interface mote Managernent MP gg gg															
I Filtening I Filtening tenance tenance dministrator Password addrime Settings lagnostics patae Firmware ettings Backup afault Settings bebot septent ommand Line Interface emote Management onnection Manager NMP Pgs ut							All rights resea								

Figure 51 - GRE configuration page for GWR Router 2

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

GENEKO GWRI	ROUTER - CONFIG	GURATION CONS	BOLE								
Routing	(										
formation Routing	Table Settings										
0.0000000	nt static routes										
		Netmask	Gateway	Metric	Interface						
ver Enab	10.64.64.64	255.255.255.255	sateway	O	ppp_0						
			*		and the second se						
outing Protocol	10.10.10.0	255.255.255.252	*	0	gre1						
15	192.168.3.0	255.255.255.0		1	gre1						
	192.168.2.0	255.255.255.0	0.0.0.0	0	eth0						
PN	0.0.0.0	0.0.0.0	*	1	ppp_0						
ntity Settings tor Password	e Dest Network 0.0.0.0 192.168.4.0	Netmask 0.0.0.0 255.255.255.0	Gateway *	Metric 1	Interface ppp_0 v gre1 v	Action Rem Rem					
tity Settings tor Password	0.0.0.0	0.0.0.0		Metric 1 1	ppp_0 💌	Rem Rem					
ntity Settings V tor Password V Settings V mware	0.0.0.0	0.0.0.0		Metric 1 1	ppp_0 🛩 gre1 💌	Rem					
ntity Settings	0.0.0.0	0.0.0.0		Metric 1 1	ppp_0 🛩 gre1 💌	Rem Rem					
ntity Settings tor Password Settings s mware ackup tings V E	0.0.0.0	0.0.0		Metric 1 1	ppp_0 🛩 gre1 💌	Rem Rem					 
ntty Settings	0.0.0.0 192.168.4.0 ing nable Network Address	0.0.0           255.255.255.0           Translation (NAT)			ppp_0 🛩 gre1 💌	Rem Rem					
tity Settings tor Password Settings ackup Ings Line Interface angeomet	Ing nable Network Address	0.0.0.0           255.255.255.0           Translation (NAT)           from external network			ppp_0 🛩 gre1 💌	Rem Rem					
tity Settings tor Password Settings ackup tings Line Interface anagement Manager Enab	0.0.0.0 192.168.4.0 ing nable Network Address rd protocol connections e Tunneling Protoco	0.0.0.0           255 255.255.0           Translation (NAT)           from external network           Send to			ppp_0 🛩 gre1 💌	Rem Rem					
ntty Sattings for Password Settings satkup Titings in Interface anagement Manager	0.0.0.0 192.158.4.0 ing nable Network Address rd protocol connections le Tunneling Protoco GRE	0.0.0.0           255 255.255.0           Translation (NAT)           from external network           Send to           10.0.0.1			ppp_0 🛩 gre1 💌	Rem Rem					
tity Settings tor Password Settings ackup tings Line Interface anagement Manager Enab	0.0.0.0 192.168.4.0 ing nable Network Address rd protocol connections e Tunneling Protoco	0.0.0.0           255 255.255.0           Translation (NAT)           from external network           Send to			ppp_0 🛩 gre1 💌	Rem Rem					
tity Settings tor Password Settings s mware ackup tings Line Interface anagement Manager □	0.0.0.0 192.158.4.0 ing nable Network Address rd protocol connections le Tunneling Protoco GRE	0.0.0.0           255.255.255.0           Translation (NAT)           from external network           Send to           10.0.0.1           10.0.0.2	s to the following intern	al devices	ppp_0 🛩 gre1 💌	Rem Rem					
ntty Sattings for Password Settings armare ackup things Eine Interface anagement Manager Forwar Eine Interface Eine Interface Base Forwar Eine Interface Base Forwar	0.0.0     192.158.4.0     192.158.4.0     ing     nable Network Address rd protocol connections     GRE     ESP rd TCP/UDP connection	0.0.0.0           255.255.255.0           Translation (NAT)           from external network           Send to           [10.0.0.1           10.0.0.2           hs from external network	s to the following intern	al devices	ppp_0 🛩 gre1 💌	Rem Add	rward to port	Interfa	ice Action	]	

Figure 52 - Routing configuration page for GWR Router 2

- Optionally configure IP Filtering and TCP service port settings 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 53*) is illustrated simple network with two sites. Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.



Figure 53 - 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 have 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 10.1.1.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 172.29.8.5
ip route 10.1.1.0 255.255.255.0 tunnel0
```

The GWR Router Sample Configuration:

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

		INFIGURATION CONSOLE		
Status	Network			<ul> <li>Help</li> </ul>
General Network Information WAN Information Settings Network	Network Settings	utomatically using DHCP		
DHCP Server WAN Settings Routing Dynamic Routing Protocol	Ouse the following IP ad IP Address Subnet Mask	10.1.1.1 255.255.255.0		
RP VPN Settings GRE IPSec	Local DNS Caution: Changes to IP Address, sul	net mask and local DNS require a reboot to take effect.		Reload Save
OpenVPN IP Filtering DynDNS Serial Port Maintenance				
Device Identity Settings Administrator Password Date/Time Settings Diagnostics Update Firmware Settings Backup Default Settings Reboot				
Management Command Line Interface Remote Management Connection Manager SNMP Logs				
Logout		Copyright © 2008 Genetico. Al rights r http://www.aeneko.re/	sserved.	

Figure 54 - Network configuration page

- Use SIM card with a dynamic/static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider's network default gateway).
- Click WAN Settings Tab to configure parameters necessary for GSM/UMTS connection. All



parameters necessary for connection configuration should be required from mobile operator.

- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.
- Click VPN Settings > GRE Tunneling to configure new VPN tunnel parameters:
  - Enable: yes
  - Local Tunnel Address: 10.1.1.1
  - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252)
  - Tunnel Source: 172.29.8.5
  - Tunnel Destination: 172.29.8.4
  - KeepAlive enable: no
  - Period:(none)
  - Retries:(none)
  - Press ADD to put GRE tunnel rule into VPN table.
  - Press *Save* to accept the changes.



Figure 55 - GRE configuration page

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



	Routing								0
neral									
work Information	Routing Ta	ble Settings							
gs	Current	static routes							
work	Enable	Dest Network	Netmask	6.1	Metric	Interface			
CP Server N Settings		10.64.64.64	255.255.255.255	Gateway	Metric	1			
uting					U	ppp_0			
amic Routing Protocol		10.10.10.0	255.255.255.252	*	0	gre1			
RP	<b>V</b>	192.168.3.0	255.255.255.0	*	1	gre1			
Settings GRE	1	192.168.2.0	255.255.255.0	0.0.0.0	0	eth0			
IPSec		0.0.0.0	0.0.0.0	×	1	ppp_0			
OpenVPN			11.00000			Ince=-			
Filtering hDNS	Apply the	e following static rout	es to the routing table						
ial Port	Enable	Dest Network	Netmask	Gateway	Metric	Interface Ad	tion		
enance		0.0.0.0	0.0.0	*	1		em		
rice Identity Settings		10.2.2.0		*					
ministrator Password e/Time Settings		10.2.2.0	255.255.255.0	-			em		
gnostics						eth0 🖌 🤞	dd		
date Firmware									
tings Backup ault Settings	Forwarding	g							
poot	🗹 Enat	ble Network Address	Translation (NAT)						
jement									
mmand Line Interface	Forward	protocol connections	from external network	s to the following intern	al devices				
	Enable	<b>Tunneling Protoco</b>	I Send to						
note Management		005	10.0.0.1						
note Management nnection Manager MP		GRE							
mote Management nnection Manager									
note Management mection Manager MP is		ESP	10.0.0.2						
note Management nnection Manager MP		ESP	10.0.0.2	rks to the following inte	rnal devices				

Figure 56 - 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 57*. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.



Figure 57 - 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

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.



#### **GWR Series Router**

#### **USER MANUAL**

	GWR ROUTER - C	ONFIGURATION CONSOLE	
Status General	Network		🕐 Help
Network Information WAN Information	Network Settings		
Settings Network		automatically using DHCP	
DHCP Server	Use the following IP a US a LU		
WAN Settings Routing	IP Address Subnet Mask	10.0.10.1	
Dynamic Routing Protocol RIP	Local DNS	255.255.255.0	
VPN Settings			
GRE IPSec	Caution: Changes to IP Address, su	bnet mask and local DNS require a reboot to take effect.	Reload Save
OpenVPN IP Filtering			
DynDNS Serial Port			
Maintenance			
Device Identity Settings Administrator Password			
Date/Time Settings Diagnostics			
Update Firmware			
Settings Backup Default Settings			
Reboot Management			
Command Line Interface			
Remote Management Connection Manager			
SNMP Logs			
Logout			
		Copyright © 2008 Geneko. All right http://www.geneko.rs.	

Figure 58 - Network configuration page for GWR Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (WAN Settings Tab). If disconnected please click Connect button.
- Click VPN Settings > IPSEC to configure IPSEC tunnel parameters. Click Add New Tunnel button to create new IPSec tunnel. Tunnel parameters are:
  - Add New Tunnel
    - Tunnel Name: test
    - Enable: true
  - Local Group Setup
    - Local Security Gateway Type: SIM card
    - IP Address From: SIM 1 (WAN connection is established over SIM 1)
    - Local Security Group Type: Subnet
    - IP Address: 10.0.10.1
    - Subnet Mask: 255.255.255.0
  - Remote Group Setup
    - Remote Security Gateway Type: IP Only
    - IP Address: 172.29.8.5
    - Remote Security Group Type: IP
    - IP Address: 192.168.10.1
  - IPSec Setup
    - Keying Mode: IKE with Preshared key
    - Phase 1 DH group: Group 2
    - Phase 1 Encryption: 3DES
    - Phase 1 Authentication: MD5
    - Phase 1 SA Life Time: 28800
    - Perfect Forward Secrecy: true
    - Phase 2 DH group: Group 2
    - Phase 2 Encryption: DES
    - Phase 2 Authentication: MD5
    - Phase 2 SA Life Time: 3600



- Preshared Key: 1234567890
- Failover
  - Enable IKE Failover: false
  - Restart PPP After IKE SA Retry Exceeds Specified Limit: false
  - Enable Tunnel Failover: false
- Advanced
  - Compress(Support IP Payload Compression Protocol(IPComp)): false
  - Dead Peer Detection(DPD): false
  - NAT Traversal: true
  - Send Initial Contact: true

Device 2 Device Tunnel		0 He
Add New Tunnel		
Tunnel Number Tunnel Name Enable	1 fest	
Local Group Setup		
Local Security Gateway Type	SIM Card 💌	
Custom Peer ID	SIM1 v	
Local Security Group Type IP Address Subnet Mask	Subnet            10.010.1         255.255.255.0	
Remote Group Setup		
Remote Security Gateway Type	IP Only	
IP Address	172.29.8.5	
Remote Security Group Type IP Address	IP V 192.168.10.1	

Figure 59 - IPSEC configuration page I for GWR Router 1

IPSec Setup	
Keying Mode	IKE with Preshared key 💙
Phase 1 DH Group	Group2 👻
Phase 1 Encryption	3DES 💌
Phase 1 Authentication	MD5 💌
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	
Phase 2 DH Group	Group2 💌
Phase 2 Encryption	DES 💌
Phase 2 Authentication	MD5 💌
Phase 2 SA Life Time	3600 sec
	1234567890
Preshared Key	

Figure 60 - IPSec configuration page II for GWR Router 1



F	ailover		
	Enable IKE Failover		
	IKE SA Retry		
	Restart PPP After IKE SA Retry Exceeds Specifie	d Limit	
	Enable Tunnel Failover		
	Ping IP		
	Ping Interval	sec	
	Packet Size		
	Advanced Ping Interval	sec	
	Advanced Ping Wait For A Response	sec	
	Maximum Number Of Failed Packets	%	
A	dvanced		
C	Compress (Support IP Payload Compression Protoco	ol (IPComp))	
	Dead Peer Detection (DPD) 20 sec		
	NAT Traversal		
	Send Initial Contact		

Figure 61 - IPSec configuration page III for GWR Router 1

- Click Start button on Internet Protocol Security page to initiate IPSEC tunnel
- When you click *Start* button you can choose one of two modes of IPSec tunnel: *Connect* or *Wait*. One router has to be in *Connect* mode while router on the opposite side is in *Wait* mode. WAN IP address of the router in *Wait* mode has to be reachable from the other router
- Here you can define log level of IPSec process from the dropdown menu on the right side

	GWR ROUTER	- CON	IFIGURA	ATION C	ONSOLE								
Status General	Internet Protocol	l Secur	ity									<b>0</b> H	elp
Network Information WAN Information	Summary												
Settings	Tunnels used:				1								
Network DHCP Server	Maximum number o	of tunnels			5								
WAN Settings Routing Dynamic Routing Protocol	Add New Tunnel										Log levi	el none	
RP	No	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action	Connection mod		
VPN Settings					Ph1:3DES/MD5/2		10.0.10.1					raw	
GRE	1	test	yes	stopped	Ph2:DES/MD5/1	N/I	255.255.255.0	192.168.10.1	172.29.8.5	Edit Delete	Connect Wait	crypt	
IPSec							•					parsing emitting	
OpenVPN IP Filtering	* Reducing the MTU size on	the client	side can bel	n eliminate	some connectivity probl	ems occurring	at the protocol leve	i .			Start	att control	
DvnDNS	** Recommended MTU size	on client si		p continues	some connectivity probi	enis occurring i	at the protocol leve					lifecycle	_
Serial Port	*** Tunnel status description started	: • ipsec is										klips	
Maintenance	stopped			or tunnel is	not enabled							dns debug-oppo	
Device Identity Settings	connecting		trying to est.									private	
Administrator Password Date/Time Settings	waiting for connection		waiting for o	other end to	connect							Linuara	
Dater Time Settings Diagnostics	established	- tunnel	is up										
Update Firmware													
Settings Backup													
Default Settings													
Reboot Management													
Command Line Interface													
Remote Management													
Connection Manager													
SNMP													
Logs													
Logout													

Figure 62 – IPSec start/stop page for GWR Router 1

Summary												
Tunnels used:					1							
Maximum num	ber o	f tunnel	s:		5							
Add New Tu	innel										Log level n	one 💌
	No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action	Connection mode	
	1	test	yes	waiting for connection	Ph1:3DES/MD5/2 Ph2:DES/MD5/1		10.0.10.1 255.255.255.0	192.168.10.1	172.29.8.5	Edit Delete	Connect Wait	
												-

Figure 63 – Default connection mode is Wait



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

The GWR Router 2 configuration:

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

Press Save to accept the changes.

	GWR ROUTER - C	CONFIGURATION CONSOLE			
Status	Network				🕐 Help
General Network Information WAN Information WAN Settings Detection WAN Settings Routing Dynamic Routing Protocol RP UN Settings GRE PSec Open/PN IP Fittering DynDNS	Use the following IP a IP Address Subnet Mask Local DNS	s automatically using DHCP address 192.168.10.1 255.255.55.0 195.78.6.36 subnet mask and local DNS require a reboot to tak	z effect.		Reload Save
Sérial Port Maintenance Device Identity Settings Administrator Password Date/Time Settings Diganositos Update Firmware Settings Backup Default Settings Reboot Management Commend Line Interface Remote Management Commedion Manager SIMIP Logo					
		Сору	right © 2008 Geneko, All rights n http://www.geneko.rs/	eserved.	

Figure 64 - Network configuration page for GWR Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click **WAN** Settings Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (WAN Settings Tab). If disconnected please click Connect button.
- Click VPN Settings > IPSEC to configure IPSEC tunnel parameters. Click Add New Tunnel button to create new IPSec tunnel. Tunnel parameters are:
  - Add New Tunnel
    - Tunnel Name: test
    - Enable: true
  - Local Group Setup
    - Local Security Gateway Type: SIM card
    - IP Address From: SIM 1 (WAN connection is established over SIM 1)
    - Local Security Group Type: IP
    - IP Address: 192.168.10.1
  - Remote Group Setup
    - Remote Security Gateway Type: IP Only
    - IP Address: 172.29.8.4
    - Remote Security Group Type: Subnet
    - IP Address: 10.0.10.1
    - Subnet: 255.255.255.0



# IPSec Setup

- Keying Mode: IKE with Preshared key
- Phase 1 DH group: Group 2
- Phase 1 Encryption: 3DES
- Phase 1 Authentication: MD5
- Phase 1 SA Life Time: 28800
- Perfect Forward Secrecy: true
- Phase 2 DH group: Group 2
- Phase 2 Encryption: DES
- Phase 2 Authentication: MD5
- Phase 2 SA Life Time: 3600
- Preshared Key: 1234567890
- Failover
  - Enable IKE Failover: false
  - Enable PPP After IKE SA Retry Exceeds Specified Limit: false
  - Enable Tunnel Failover: false
- Advanced
  - Compress(Support IP Payload Compression Protocol(IPComp)): false
  - Dead Peer Detection(DPD): false
  - NAT Traversal: true
  - Send Initial Contact: true
  - Press *Save* to accept the changes.

Device 2 Device Tunnel		Q
Add New Tunnel		
Tunnel Number	1	
Tunnel Name Enable	test 🗸	
Local Group Setup		
Local Security Gateway Type	SIM Card	
Custom Peer ID IP Address From	SIM 1	
Local Security Group Type IP Address	IP V 192.168.10.1	
Remote Group Setup		
Remote Security Gateway Type	IP Only	
IP Address	172 29 8.4	
Remote Security Group Type IP Address Subnet Mask	Subnet  10.0.10.1 255.255.50	



IPSec Setup	
Keying Mode Phase 1 DH Group	IKE with Preshared key V Group2 V
Phase 1 Encryption	3DES 💌
Phase 1 Authentication	MD5 🛩
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	
Phase 2 DH Group	Group2 🔽
Phase 2 Encryption	DES 💌
Phase 2 Authentication	MD5 💌
Phase 2 SA Life Time	3600 sec
	1234567890
Preshared Key	

Figure 66 - IPSec configuration page II for GWR Router 2



Failover		
Enable IKE Failover		
IKE SA Retry		
Restart PPP After IKE SA Retry Exceeds S	Specified Limit	
Enable Tunnel Failover		
Ping IP		
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))	
	. Interest (in a striktly	
Dead Peer Detection (DPD) sec		
NAT Traversal		
Send Initial Contact		

Figure 67 - IPSec configuration page III for GWR Router 2

- Click Start button on Internet Protocol Security page to initiate IPSEC tunnel
- If on the previous router default mode *Wait* is selected, here you choose *Connect* mode

Internet Proto	col	Secur	rity									🕜 Help
Summary												
Tunnels used:					1							
Maximum numb	er of	tunnels	s:		5							
Add New Tun	nel	]									Log level no	ne 💌
1	No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action	Connection mode	
	1	test	yes	connecting	Ph1:3DES/MD5/2 Ph2:DES/MD5/1	N/I	192.168.10.1	10.0.10.1 255.255.255.0	172.29.8.4	Edit Delete	Connect Wait	
Fortuing the MTU size on the client side, can help eliminate some connectivity problems occurring at the protocol level     Foremmended MTU size on client side is 1500     Toron (attack description:									Start Stop	Refresh		
started		- ipsec is running										
stopped			- ipsec is not running or tunnel is not enabled									
connecting			- ipsec is trying to establish connection									
waiting for connec	tion	<ul> <li>ipseo is</li> </ul>	s waiting for	other end to cor	nect							
established		- tunnel is up										

Figure 68 – IPSec start/stop page for GWR Router 2

• 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 *Figure 69* 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 69 - 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.



#### **GWR Series Router**

#### **USER MANUAL**

	GWR ROUTER - C	ONFIGURATION CONSOLE								
Status	Network			🕐 Help						
General Network Information WAN Information	Network Settings									
Settings	O Obtain an IP address	automatically using DHCP								
Network DHCP Server										
WAN Settings	IP Address	192.168.10.1								
Routing	Subnet Mask	255,255,255,0								
Dynamic Routing Protocol										
RIP VPN Settings	Local DNS	195.78.6.36								
GRE	Caution: Changes to IP Address su	ibnet mask and local DNS require a reboot to take effect.								
IPSec .	Control . Changes to it statical, se		Reload	Save						
OpenVPN IP Filtering										
DynDNS										
Serial Port										
Maintenance										
Device Identity Settings Administrator Password										
Date/Time Settings										
Diagnostics										
Update Firmware										
Settings Backup Default Settings										
Reboot										
Management										
Command Line Interface										
Remote Management Connection Manager										
SNMP										
Logs										
1 minut										
Logout										
		Copyright @ 2008 Geneko. All righ								
		http://www.geneko.rs	<u>s/</u>							

Figure 70 - Network configuration page for GWR Router

- Click **WAN** Settings Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (WAN Settings Tab). If disconnected please click Connect button.
- Click VPN Settings > IPSEC to configure IPSEC tunnel parameters. Click Add New Tunnel button to create new IPSec tunnel. Tunnel parameters are:
  - Add New Tunnel
    - Tunnel Name: test
    - Enable: true
    - Local Group Setup
      - Local Security Gateway Type: SIM card
      - 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 Security Group Type: Subnet
- IP Address: 10.10.10.0
- Subnet Mask: 255.255.255.0

#### • IPSec Setup

- Keying Mode: IKE with Preshared key
- Phase 1 DH group: Group 2
- Phase 1 Encryption: 3DES
- Phase 1 Authentication: SHA
- Phase 1 SA Life Time: 28800
- Perfect Forward Secrecy: true
- Phase 2 DH group: Group 2
- Phase 2 Encryption: 3DES
- Phase 2 Authentication: SHA1
- Phase 2 SA Life Time: 3600

- Preshared Key: 1234567890
- Failover
  - Enable IKE Failover: false
  - Enable PPP After IKE SA Retry Exceeds Specified Limit: false
  - Enable Tunnel Failover: false
- Advanced
  - Compress(Support IP Payload Compression Protocol(IPComp)): false
  - Dead Peer Detection(DPD): false
  - NAT Traversal: true
  - Send Initial Contact Notification: true

Press *Save* to accept the changes.

Device 2 Device Tunnel	0	) Help
Add New Tunnel		
Tunnel Number Tunnel Name Enable	1 test	
Local Group Setup		
Local Security Gateway Type	SIM Card	
Custom Peer ID IP Address From Local Security Group Type	SIM 1 V Subnet V	
IP Address	192.168.10.0	
Subnet Mask	255.255.255.0	
Remote Group Setup		
Remote Security Gateway Type	IP Only 💌	
Custom Peer ID		
Remote Security Group Type	Subnet	
IP Address	10.10.10.1	
Subnet Mask	255.255.255.0	

#### Figure 71 - IPSEC configuration page I for GWR Router

IPSec Setup	
Keying Mode	IKE with Preshared key 💙
Phase 1 DH Group	Group2 💌
Phase 1 Encryption	3DES 💌
Phase 1 Authentication	SHA 🔽
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	
Phase 2 DH Group	Group2 💌
Phase 2 Encryption	3DES 🗸
Phase 2 Authentication	SHA1 💌
Phase 2 SA Life Time	3600 sec
	1234567890
Preshared Key	

Figure 72 - 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									
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)     sec									
NAT Traversal									
Send Initial Contact									
Send Initial Contact									

Figure 73 - IPSec configuration page III for GWR Router

- Click Start button on Internet Protocol Security page to initiate IPSEC tunnel
- Click *Connect* button choose mode where router initiate connection

Internet Protocol Security										<ul> <li>Help</li> </ul>	
Summary											
Tunnels used:			1								
Maximum number o	Maximum number of tunnels:			5							
Add New Tunnel										Log level none	~
No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action	Connection mode	
1	test	yes	connecting	Ph1:3DES/SHA/2 Ph2:3DES/SHA1/1	NZ	192.168.10.0 255.255.255.0	10.10.10.1 255.255.255.0	150.160.170.1	Edit Delete	Connect Wait	
↑ Reducing the MTU size on the ellent side, can help eliminate some connectivity problems occurring at the protocol level ™ Recommended MTU size on client side is 1300 ™ Tunnet status description:										Start Stop F	Refresh
started		- ipsec is running									
stopped connecting		- ipsec is not running or tunnel is not enabled - ipsec is trying to establish connection									
waiting for connection			rother end to c								
established		el is up	, ource and to o	since.							

Figure 74 – 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
1
hostname Cisco-Router
boot-start-marker
boot-end-marker
1
!
!
no aaa new-model
!
no ip domain lookup
1
!--- Keyring that defines wildcard pre-shared key.
!
crypto keyring remote
   pre-shared-key address 0.0.0.0 0.0.0.0 key 1234567890
1
!--- ISAKMP policy
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
  lifetime 28800
1
!--- 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
!
1
crypto ipsec transform-set testGWR esp-3des esp-sha-hmac
!--- Instances of the dynamic crypto map
!--- reference previous IPsec profile.
crypto dynamic-map dynGWR 5
 set transform-set testGWR
set isakmp-profile L2L
!
!--- Crypto-map only references instances of the previous dynamic crypto map.
1
crypto map GWR 10 ipsec-isakmp dynamic dynGWR
1
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
T
ip route 0.0.0.0 0.0.0.0 150.160.170.2
1
ip http server
no ip http secure-server
ip nat inside source list nat_list interface FastEthernet0/0 overload
ip access-list extended nat list
deny ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
permit ip 10.10.10.0 0.0.0.255 any
!
access-list 23 permit any
1
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.

# Apendix

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

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

RSSI information is available from several sources:

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

Signal strength LED indicator:

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

## Antenna placement

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

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

- Simply install the GWR 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.

