Content

| LIST OF FIGURES | 4 |
|--|------------|
| | / |
| Evamples of Dessible Application | 0 |
| Tochnical Parameters | 0 |
| CWD Doutor fosturos | 9 |
| Broduct Overview | .10 |
| Front nanol | .11 |
| FTUTIL parter | . 11 11 |
| Ton Panel | . 11 |
| Putting Into Operation | 13 |
| Declaration of conformity | 14 |
| Device Configuration. | 15 |
| DEVICE CONFIGURATION USING WEB APPLICATION | 15 |
| Add/Remove/Update manipulation in tables | .16 |
| Save/Reload changes | .16 |
| Status Information | .16 |
| Status - General | .16 |
| Status - Network Information | .17 |
| Status - WAN Information | .17 |
| Settings - Network | .19 |
| Settings - DHCP Server | .20 |
| Settings - WAN Setting | .22 |
| Settings - Routing | .25 |
| Port translation | . 27 |
| Settings – Dynamic Routing Protocol | .27 |
| Routing Information Protocol (RIP) | . 27 |
| RIP routing engine for the GWR Router | . 28 |
| Settings - VPN Settings | .30 |
| Generic Routing Encapsulation (GRE) | . 30 |
| GRE Keepalive | . 31 |
| Internet Protocol Security (IPSec) | . 32 |
| JD Eiltoring configuration example | .37 |
| | . 39 |
| Maintenance - Administrator Password | .40 |
| Maintenance - Automistrator Fassword | .40 |
| Maintenance - Device Identity Settings | .41 |
| Maintenance - Date/Time Settings | .42 |
| Maintenance - Undate Firmware | .44 |
| Maintenance - Settings Backup | .44 |
| Import Configuration File | .45 |
| Export Configuration File | . 45 |
| Maintenance - System Reboot | .46 |
| Maintenance - Default Settings | .47 |
| Management - Serial Port | .47 |
| Management - Simple Management Protocol (SNMP) | . 49 |
| Management - Logs | .50 |
| Wizards – Internet Access | .52 |
| Wizards – GRE Tunnel | .53 |
| Wizards – IPSec Tunnel | .55 |
| Logout | .59 |
| = | |



| DEVICE CONFIGURATION USING CONSOLE | 59 |
|--|------------|
| Network Settings | 60 |
| Static vs. Dynamic IP Addresses | |
| DHCP Server Settings | 61 |
| GPRS/EDGE/HSDPA Settings | 61 |
| Routing | 62 |
| Administration | 63 |
| Status | 64 |
| General System Information | 64 |
| Network Information | 65 |
| GPRS/EDGE Information | |
| Configuration Wizard | |
| CONFIGURATION EXAMPLE | |
| GWR Router as Internet Router | |
| GRE Tunnel configuration between two GWR Routers | 69 |
| GRE Tunnel configuration between GWR Router and third party router | 74 |
| IPSec Tunnel configuration between two GWR Routers | 78 |
| IPSec Tunnel configuration between GWP Pouter and Cisco Pouter | |
| IPSec Tunnel configuration between GWP Pouter and Juniner SSC firewall | |
| ADENDIX | |
| A How to Achieve Maximum Signal Strength with GWR Router? | |
| Antenna nlacement | 105 |
| Antenna Ontions | |
| B Mohile operator GPRS settings | 106 |
| Australia | |
| Austria | |
| Belgium | |
| Brasil | |
| Canada | |
| China | |
| Croatia | |
| Czech Republic Denmark | |
| Egynt | |
| Estonia | |
| Finland | |
| France | |
| Germany | |
| Greece | |
| нопдкопд Ниподпи | |
| India | |
| Indonesia | |
| Ireland | |
| Israel | |
| Italy | 110 |
| Japan | |
| Lithuania | |
| Luxembourg Macedonian | |
| Malausia | |
| Mexico | |
| Netherlands | |
| New Zeleand | |
| Norway | 111 |
| Poland | |
| Pnillipines Doutuool | |
| гогици Виссія | 111 112 |
| | |



| Serbia | |
|--------------|--|
| Singapore | |
| Slovakia | |
| Slovenia | |
| South Africa | |
| Spain | |
| Śweden | |
| Switzerland | |
| Taiwan | |
| Thailand | |
| Turkey | |
| UK | |
| Ukraine | |
| USA | |
| | |



List of Figures

| Figure 1 - GWR Router | 8 |
|---|----|
| Figure 2 - GWR Router front panel | 11 |
| Figure 3 - GWR Router back panel | 11 |
| Figure 4 - GWR Router top panel side | 12 |
| Figure 5 - Declaration of conformity | 14 |
| Figure 6 - User authentication | 15 |
| Figure 7 - General Router information | 17 |
| Figure 8 - Network Information | 18 |
| Figure 9 - WAN Information | 18 |
| Figure 10 - Network parameters configuration page | 19 |
| Figure 11 - DHCP Server configuration page | 21 |
| Figure 12 - WAN Settings configuration page | 22 |
| Figure 13 - Routing configuration page | 25 |
| Figure 14 - RIP configuration page | 27 |
| Figure 15 - GRE tunnel parameters configuration page | 31 |
| Figure 16 - IPSec Summary screen | 32 |
| Figure 17 - IPSec Settings part I | 33 |
| Figure 18 - IPSec Settings part II | 34 |
| Figure 19 - IP Filtering configuration page | 38 |
| Figure 20 - IP Filtering configuration example | 39 |
| Figure 21 - IP Filtering settings | 39 |
| Figure 22 - Administrator Password configuration page | 40 |
| Figure 23 - Device Identity Settings configuration page | 42 |
| Figure 24 - Date/Time Settings configuration page | 42 |
| Figure 25 - Diagnostic page | 44 |
| Figure 26 - Update Firmware page | 45 |
| Figure 27 - File download | 46 |
| Figure 28 - System Reboot page | 46 |
| Figure 29 - Default Settings page | 47 |
| Figure 30 - Serial Port configuration page | 48 |
| Figure 31 - SNMP configuration page | 50 |
| Figure 32 - Syslog configuration page | 51 |
| Figure 33 - Internet Access Wizard - page 1 of 3 | 52 |
| Figure 34 - Internet Access Wizard - page 2 of 3 | 52 |
| Figure 35 - Internet Access Wizard - page 3 of 3 | 53 |
| Figure 36 - GRE Tunnel Wizard - 1 of 4 | 53 |
| Figure 37 - GRE Tunnel Wizard - 2 of 4 | 54 |
| Figure 38 - GRE Tunnel Wizard - 3 of 4 | 54 |
| Figure 39 - GRE Tunnel Wizard - 4 of 4 | 55 |
| Figure 40 - IPSec Tunnel Wizard - 1 of 6 | 55 |
| Figure 41 - IPSec Tunnel Wizard - 2 of 6 | 56 |
| Figure 42 - IPSec Tunnel Wizard - 3 of 6 | 57 |
| Figure 43 - IPSec Tunnel Wizard - 4 of 6 | 57 |
| Figure 44 - IPSec Tunnel Wizard - 5 of 6 | 58 |
| Figure 45 - IPSec Tunnel Wizard - 6 of 6 | 58 |
| Figure 46 - Default serial port parameters | 59 |
| Figure 47 - Login menu | 59 |
| Figure 48 - Main configuration menu | 60 |
| Figure 49 - Network parameters | 60 |
| Figure 50 - Network parameters configuration | 61 |
| Figure 51 - DHCP Server configuration | 61 |
| Figure 52 - Primary DNS | 61 |
| | |



| Figure 53 - Secondary DNS | 61 |
|--|--|
| Figure 54 - SIM card selection | 62 |
| Figure 55 - SIM card GSM/UMTS configuration | |
| Figure 56 - GSM/UMTS authentication | 62 |
| Figure 57 - Routing menu | 62 |
| Figure 58 - Routing table (list of all routes) | 63 |
| Figure 59 - Administration Menu | 63 |
| Figure 60 - Administrator password | 63 |
| Figure 61 - Network diagnostic utility | 63 |
| Figure 62 - Date/time parameters | 64 |
| Figure 63 - List of Restore option | 64 |
| Figure 64 - Status Menu | 64 |
| Figure 65 - List of basic system parameters | 65 |
| Figure 66 - Status of LAN network connection | 66 |
| Figure 67 - GSM/UMTS status | 67 |
| Figure 68 - Configuration wizard | 67 |
| Figure 69 - GWR Router as Internet router | 68 |
| Figure 70 - GRE tunnel between two GWR Routers | 69 |
| Figure 71 - Network configuration page for GWR Router 1 | 70 |
| Figure 72 - GRE configuration page for GWR Router 1 | 71 |
| Figure 73 - Routing configuration page for GWR Router 1 | 71 |
| Figure 74 - Network configuration page for GWR Router 2 | |
| Figure 75 - GRE configuration page for GWR Router 2 | 73 |
| Figure 76 - Routing configuration page for GWR Router 2 | 73 |
| Figure 77 - GRE tunnel between Cisco router and GWR Router | 74 |
| Figure 78 - Network configuration page | 76 |
| Figure 70 - GRE configuration page | 77 |
| Figure 80 - Routing configuration page | |
| Γ | |
| Figure 81 - IPSec tunnel between two GWR Routers | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page for GWR Router 2 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page I for GWR Router 2 Figure 87 - IPSEC configuration page I for GWR Router 2 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page for GWR Router 2 Figure 87 - IPSEC configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page for GWR Router 2 Figure 87 - IPSEC configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 Figure 89 - IPSec start/stop page I for GWR Router 2 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page for GWR Router 2 Figure 87 - IPSEC configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 Figure 89 - IPSec configuration page I for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 | |
| Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page I for GWR Router 2 Figure 87 - IPSEC configuration page I for GWR Router 2 Figure 88 - Network configuration page I for GWR Router 2 Figure 89 - IPSec configuration page I for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 90 - IPSec tunnel between GWR Router and Cisco Router Figure 91 - Network configuration page for GWR Router | 77 78 79 80 80 80 81 82 83 83 83 83 83 83 84 85 86 |
| Figure 80 - Routing configuration page Figure 81 - IPSec tunnel between two GWR Routers | 77 78 79 80 80 80 81 82 83 83 83 83 83 83 83 83 83 83 83 84 85 86 87 |
| Figure 80 - Routing configuration page Figure 81 - IPSec tunnel between two GWR Routers | 77 78 79 80 80 80 81 82 83 83 83 83 83 83 83 83 83 84 85 85 86 87 88 |
| Figure 80 - Routing configuration page Figure 81 - IPSec tunnel between two GWR Routers | 778 779 80 80 80 81 82 83 83 83 83 83 83 83 83 83 83 83 83 83 |
| Figure 80 - Routing configuration page Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page for GWR Router 1 Figure 83 - IPSEC configuration page I for GWR Router 1 Figure 84 - IPSec configuration page for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page for GWR Router 2 Figure 87 - IPSEC configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 Figure 89 - IPSec configuration page for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 90 - IPSec tunnel between GWR Router and Cisco Router Figure 91 - Network configuration page I for GWR Router Figure 92 - IPSEC configuration page I for GWR Router Figure 93 - IPSec configuration page I for GWR Router Figure 94 - IPSec configuration page I for GWR Router Figure 95 - IPSec start/stop page for GWR Router Figure 95 - IPSec configuration page I for GWR Router Figure 95 - IPSec configuration page I for GWR Router | 778 779 80 80 80 81 82 83 83 83 83 83 83 83 83 83 83 83 83 84 85 86 86 87 88 88 88 88 88 88 88 88 88 88 88 88 |
| Figure 80 - Routing configuration page for GWR Routers | 778 779 80 80 80 81 82 83 83 83 83 83 83 83 83 83 83 83 84 85 86 86 87 88 88 88 87 91 92 |
| Figure 80 - Routing configuration page | 778 779 80 80 80 81 82 83 83 83 83 83 83 83 83 83 83 83 83 83 |
| Figure 80 - Network configuration page for GWR Router 1 Figure 82 - Network configuration page If for GWR Router 1 Figure 83 - IPSEC configuration page If for GWR Router 1 Figure 84 - IPSec configuration page If for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page for GWR Router 2 Figure 87 - IPSEC configuration page If for GWR Router 2 Figure 88 - IPSec configuration page If for GWR Router 2 Figure 89 - IPSec configuration page If for GWR Router 2 Figure 89 - IPSec start/stop page for GWR Router 2 Figure 90 - IPSec tunnel between GWR Router and Cisco Router Figure 91 - Network configuration page If for GWR Router Figure 92 - IPSEC configuration page If for GWR Router Figure 93 - IPSec configuration page If for GWR Router Figure 94 - IPSec configuration page If for GWR Router Figure 95 - IPSec configuration page If for GWR Router Figure 96 - Network configuration page If for GWR Router Figure 97 - IPSec tunnel between GWR Router and Cisco Router Figure 97 - IPSec tunnel between GWR Router and Cisco Router Figure 98 - IPSec tunnel between GWR Router and Cisco Router Figure 95 - IPSec tunnel between GWR Router and Cisco Router Figure 95 - IPSec tunnel between GWR Router and Cisco Router Figure 95 - IPSec tunnel between GWR Router and Cisco Router Figure 96 - Network configuration page If for GWR Router Figure 97 - IPSEC configuration page I for GWR Router Figure 98 - IPSec tunnel between GWR Router and Cisco Router Figure 98 - IPSec tunnel between GWR Router and Cisco Router Figure 97 - IPSEC configuration page I for GWR Router Figure 98 - IPSec configuration page I for GWR Router Figure 98 - IPSec configuration page I for GWR Router Figure 98 - IPSec configuration page I for GWR Router | 778 779 80 80 80 81 82 83 83 83 83 83 83 83 83 83 83 83 83 83 |
| Figure 80 - Rothing Configuration page for GWR Routers | 77 78 79 80 80 80 81 82 83 83 83 83 83 83 83 83 83 83 83 83 84 85 86 87 88 88 88 91 92 92 93 94 94 |
| Figure 80 - Routing configuration page for GWR Routers | 778 779 80 80 80 81 82 83 83 83 83 83 83 83 83 84 85 85 86 87 87 88 88 88 91 92 92 93 94 94 |
| Figure 81 - IPSec tunnel between two GWR Routers | 778 779 80 80 80 81 82 83 83 83 83 83 83 84 85 86 86 87 87 88 88 88 91 92 92 93 94 94 95 95 |
| Figure 80 - Rotung configuration page | 778 779 80 80 80 81 82 83 83 83 83 83 83 83 83 84 85 86 86 87 88 88 88 87 91 92 92 93 94 94 95 95 95 |
| Figure 80 - Rotung configuration page | 778 779 80 80 80 81 82 83 83 83 83 83 84 85 86 87 88 88 87 91 92 92 93 94 94 95 95 96 97 |
| Figure 80 - Routing comparation page Figure 81 - IPSec tunnel between two GWR Routers Figure 82 - Network configuration page I for GWR Router 1 Figure 83 - IPSeC configuration page II for GWR Router 1 Figure 85 - IPSec start/stop page for GWR Router 1 Figure 86 - Network configuration page I for GWR Router 2 Figure 87 - IPSEC configuration page I for GWR Router 2 Figure 88 - IPSec configuration page I for GWR Router 2 Figure 89 - IPSec configuration page I for GWR Router 2 Figure 99 - IPSec tunnel between GWR Router and Cisco Router Figure 91 - Network configuration page I for GWR Router Figure 92 - IPSec configuration page I for GWR Router Figure 93 - IPSec configuration page I for GWR Router Figure 93 - IPSec configuration page I for GWR Router Figure 94 - IPSec configuration page I for GWR Router Figure 95 - IPSec configuration page I for GWR Router Figure 95 - IPSec configuration page I for GWR Router Figure 95 - IPSec configuration page I for GWR Router Figure 95 - IPSec configuration page I for GWR Router Figure 95 - IPSec tunnel between GWR Router and Cisco Router Figure 96 - Network configuration page for GWR Router Figure 97 - IPSEC configuration page I for GWR Router Figure 99 - IPSec tunnel between GWR Router and Cisco Router Figure 99 - IPSec tunnel between GWR Router and Cisco Router Figure 97 - IPSEC configuration page I for GWR Router Figure 97 - IPSEC configuration page I for GWR Router Figure 99 - IPSec configuration page I for GWR Router Figure 99 - IPSec configuration page I for GWR Router Figure 99 - IPSec configuration page I for GWR Router Figure 91 - Network Router faces (list) Figure 102 - Network Interfaces (list) Figure 103 - Gateway parameters Figure 103 - Gateway parameters | 778 779 80 80 80 81 82 83 83 83 83 84 85 86 87 88 88 88 88 91 92 92 93 94 94 95 95 96 97 97 |
| Figure 81 - IPSec tunnel between two GWR Routers | 778 779 80 80 80 81 82 83 83 83 84 85 86 87 88 88 87 91 92 93 94 94 95 95 96 97 98 80 91 92 93 95 96 97 98 98 |
| Figure 81 - IPSec tunnel between two GWR Routers. Figure 82 - Network configuration page for GWR Router 1. Figure 83 - IPSEC configuration page I for GWR Router 1. Figure 84 - IPSec configuration page I for GWR Router 1. Figure 85 - IPSec start/stop page for GWR Router 1. Figure 86 - Network configuration page I for GWR Router 2. Figure 87 - IPSEC configuration page I for GWR Router 2. Figure 88 - IPSec configuration page I for GWR Router 2. Figure 89 - IPSec configuration page I for GWR Router 2. Figure 90 - IPSec start/stop page for GWR Router 2. Figure 91 - Network configuration page for GWR Router 2. Figure 92 - IPSec configuration page I for GWR Router 2. Figure 93 - IPSec configuration page I for GWR Router . Figure 91 - Network configuration page I for GWR Router . Figure 92 - IPSEC configuration page I for GWR Router . Figure 93 - IPSec configuration page I for GWR Router . Figure 94 - IPSec configuration page I for GWR Router . Figure 95 - IPSec configuration page for GWR Router . Figure 96 - Network configuration page for GWR Router . Figure 96 - Network configuration page for GWR Router . Figure 97 - IPSEC configuration page I for GWR Router . Figure 98 - IPSec configuration page I for GWR Router . Figure 99 - IPSec configuration page I for GWR Router . Figure 99 - IPSec configuration page I for GWR Router . Figure 90 - Network configuration page I for GWR Router . Figure 90 - Network Interfaces (list) . Figure 100 - Network Interfaces (list) . Figure 101 - Network Interfaces (edit) . Figure 102 - AutoKey Advanced Gateway . Figure 103 - Gateway parameters . Figure 104 - Gateway advanced parameters . Figure 105 - AutoKey IKE . Figure 105 - AutoKey IKE . Figure 105 - AutoKey IKE . Figure 106 - AutoKey IKE . Figure 107 - AutoKey IKE . Figure 108 - Cateway advanced parameters . Figure 107 - AutoKey IKE . Figure 108 - Cateway advanced parameters . Figure 105 - AutoKey IKE . Figure 10 | 778 779 80 80 80 81 82 83 83 83 83 84 85 86 87 88 88 87 92 92 93 94 94 95 95 96 97 98 99 100 |
| Figure 81 - IPSec tunnel between two GWR Routers. Figure 82 - Network configuration page for GWR Router 1. Figure 82 - Network configuration page I for GWR Router 1. Figure 83 - IPSec configuration page I for GWR Router 1. Figure 85 - IPSec start/stop page for GWR Router 1. Figure 86 - Network configuration page I for GWR Router 2. Figure 87 - IPSEC configuration page I for GWR Router 2. Figure 88 - IPSec configuration page I for GWR Router 2. Figure 89 - IPSec start/stop page for GWR Router 2. Figure 90 - IPSec start/stop page for GWR Router 2. Figure 91 - Network configuration page I for GWR Router. Figure 92 - IPSEC configuration page I for GWR Router. Figure 93 - IPSec configuration page I for GWR Router. Figure 94 - IPSec configuration page I for GWR Router. Figure 95 - IPSec configuration page I for GWR Router. Figure 96 - Network configuration page I for GWR Router. Figure 97 - IPSec configuration page I for GWR Router. Figure 96 - Network configuration page I for GWR Router. Figure 97 - IPSec configuration page I for GWR Router. Figure 96 - Network configuration page I for GWR Router. Figure 97 - IPSec configuration page I for GWR Router. Figure 96 - Network configuration page I for GWR Router. Figure 97 - IPSec configuration page I for GWR Router. Figure 97 - IPSec configuration page I for GWR Router. Figure 98 - IPSec configuration page I for GWR Router. Figure 99 - IPSec start/stop page for GWR Router. Figure 99 - IPSec start/stop page for GWR Router. Figure 101 - Network Interfaces (list). Figure 102 - AutoKey Advanced Gateway. Figure 103 - Gateway parameters. Figure 104 - Gateway advanced parameters. Figure 105 - AutoKey IKE parameters. Figure 106 - AutoKey IKE parameters. Figure 106 - AutoKey IKE parameters. Figure 107 - AutoKey KE parameters. | 778 778 779 800 801 801 811 822 833 833 844 855 866 877 888 888 887 91 922 933 94 94 95 95 95 96 97 988 99 100 100 |



| Figure 108 - Routing parameters | |
|--|--|
| Figure 109 - Policies from untrust to trust zone | |
| Figure 110 - Policies from trust to untrust zone | |



List of Tables

| Table 1 - Technical parameters | 9 |
|---------------------------------------|----|
| Table 2 - GWR Router features | |
| Table 3 - Network parameters | |
| Table 4 - DHCP Server parameters | |
| Table 5 - WAN parameters | |
| Table 6 - Advanced WAN Settings | |
| Table 7 - Routing parameters | |
| Table 8 - RIP parameters | |
| Table 9 - GRE parameters | |
| Table 10 - IPSec Summary | |
| Table 11 - IPSec Parameters | |
| Table 12 - IP filtering parameters | |
| Table 13 - Administrator password | 41 |
| Table 14 - Device Identity parameters | 41 |
| Table 15 - Date/time parameters | |
| Table 16 - Serial port parameters | |
| Table 17 - SNMP parameters | |
| Table 18 - Syslog parameters | 51 |
| | |



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 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 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 trough and VPN IPSec.



Figure 1 - GWR Router

Examples of Possible Application

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



Technical Parameters

| | | Directive 2004/108/EC | | |
|-----------------------|---|---|--|--|
| | EMC | EN 301 489-1 V1.6.1(2005-09) | | |
| | | EN 301 489-7 V1.3.1(2005-11) | | |
| | LVD | EN 60950-1:2001(1st Ed.) and/or EN 60950-1:2001 | | |
| Complies with | R&TTE | Directive 1999/05/EC | | |
| standards | | ETSI EN 301 511 V9.0.2 | | |
| | | EN 301 908-1 & EN 301 908-2(v2.2.1) | | |
| | | Directive 2002/95/EC | | |
| | RoHS | EU Commission 2005/618/EC, 2005/717/EC, 2005/747/EC, | | |
| | | 2006/310/EC, 2006/690/EC, 2006/691/EC and 2006/692/EC | | |
| | Connector R | J-45 | | |
| | Standard: IE | EE 802.3 | | |
| Ethernet interface | Physical laye | er: 10/100Base-T | | |
| | Mode: full o | r half duplex | | |
| | Wiode. Full 6 | | | |
| Other interfaces | 1 x UART(R | S-232C) | | |
| | 1 x USB Hos | | | |
| | | Tri-band: 900/1800/1900 | | |
| | GPRS | GPRS multi-slot class 10, mobile station class B | | |
| | | · | | |
| RF characteristics of | GPRS | Quad band: GSM 850/900/1800/1900MHz | | |
| GSM module | EDGE | EDGE multi-slot class 10, mobile station class B | | |
| Gold moune | CDDC | | | |
| | GPKS | UMTS/HSDPA: Triple band, 850/1900/2100MHz | | |
| | UMTS | GPRS multi-slot class 10, mobile station class B | | |
| | HSDPA | EDGE multi-slot class 10, mobile station class B | | |
| RF Connector | SMA, 50Ω | | | |
| | Ethernet act | ivity / network traffic | | |
| Status I FD | Power on | | | |
| Status LED | GSM link activity / attached network(GSM, UMTS) | | | |
| | Signal qualit | y | | |
| Power supply | 9 - 12VDC / | 1000mA | | |
| T | Operation: -5°C to +50°C | | | |
| Temperature range | Storage: -20°C to +85°C | | | |
| Physical | Width x Length x Height = 95 x 135 x 35 mm | | | |
| characteristics | Weight 380g | | | |

Table 1 - Technical parameters

*Advanced version: GWR201, GWR202, GWR251, GWR252, GWR301, GWR302 **Base version: GWR201-B, GWR202-B, GWR251-B, GWR252-B



GWR Router features

| Feature | Short description | Base version* | Advanced version** | | | |
|-----------------------------|---|---------------|-----------------------|--|--|--|
| Main Ethernet Configuration | | | | | | |
| Static IP / DHCP Client | Static and dynamic IP address | \checkmark | | | | |
| DHCP Server | DHCP Server support | \checkmark | \checkmark | | | |
| Routing | Static | òtatic √ | | | | |
| IP filtering | P address / Network filtering $$ | | | | | |
| NAT | NAT on WAN interface | \checkmark | | | | |
| IP forwarding | IP, TCP, UDP packets from WAN to LAN | | \checkmark | | | |
| GRE | Generic Routing Encapsulation is a tunneling protocol that can encapsulate a wide variety of network layer protocol packet types inside IP | | | | | |
| GRE Keepalive | Keepalive for GRE tunnels | \checkmark | \checkmark | | | |
| IPSec pass-through | ESP tunnels | \checkmark | | | | |
| IPsec | Internet Protocol Security is a suite of protocols for securing IP communications by authenticating and encrypting each IP packet of a data stream | - | \checkmark | | | |
| SNMP | Simple Network Management Protocol is used in network management systems to monitor network- attached devices for conditions that warrant administrative attention | \checkmark | \checkmark | | | |
| RIP | The Routing Information Protocol is a dynamic routing protocol used in local and wide area networks | \checkmark | | | | |
| NTP | The Network Time Protocol is a protocol for synchronizing the clocks of router | \checkmark | \checkmark | | | |
| Failover | Failover Failover | | \checkmark | | | |
| Ser2net | Serial to Ethernet converter $$ | | | | | |
| Configuration | | | | | | |
| WEB Application | HTTP based | \checkmark | \checkmark | | | |
| Remote configuration | Access to web interface over mobile network | \checkmark | \checkmark | | | |
| Configuration via | basic functionality | \checkmark | \checkmark | | | |
| serial console | full functionality | - | \checkmark | | | |
| | Internet access | \checkmark | \checkmark | | | |
| Wizards | GRE Tunnel | \checkmark | \checkmark | | | |
| | IPSec Tunnel | - | \checkmark | | | |
| Default reset | by external taster and configuration application | | | | | |
| File Management | | | | | | |
| Upload firmware | by WEB | | | | | |
| Backup configuration | by WEB | \checkmark | | | | |

Table 2 - GWR Router features



Product Overview

Front panel

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

- one RJ45 connector Ethernet port for connection into local computer network;
- one RJ45 connector for RS232 serial communication;
- 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*) the following connectors are located:

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



Figure 3 - GWR Router back panel



USER MANUAL

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 4 - 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:
 - -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)

Signal strength LED will blink when GPRS/EDGE/UMTS/HSDPA 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.



Declaration of conformity



Figure 5 - 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
- Console port

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 console port (RJ45 serial interface). This method has limited option for configuring the GWR Router.

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 of 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.

For administration by web interface 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 reserve http://www.geneko.co.rs/

Figure 6 - User authentication

After successfully finished process of authentication of *Username/Password* you can access *Main Configuration Menu* – which is shown at *Figure 7*.

You can set all parameters of the GWR Router using web application. All functionality and parameters are grouped through a few main tabs (windows).



Add/Remove/Update manipulation in tables

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

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

To *Update* the row in the table:

• Change data directly in fields you want to change

To *Remove* the row from the table:

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

Save/Reload changes

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

Status Information

The GWR Router's Status menu provides general information about router as well as real-time network information. Status menu has three parts:

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

Status - General

General Information Tab provides general information about device type, device firmware version, OS version, hardware resources utilization, MAC address of LAN port and Up Time since last reboot. Screenshot of General Router information is shown at *Figure 7*. Data in Status menu are read only and can not 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.



USER MANUAL

| | GWR ROUTER - | CONFIGURATION CONSOLE | |
|--|---|--|---------|
| Status General | Status: General | | |
| WAN Information Settings Network DHCP Server | Model Firmware Version CPU Vendor | GWR252-B 2.1.0_252 Cirruct agis ADM9 ED9302 200Mb | |
| WAN Settings Routing Dynamic Routing Protocol RIP VPN Settings | UP Time Mac Address | 00:05:26 00:1e:5c:00:02:8d | |
| GRE IP Filtering Maintenance Administrator Password | SIM Card Detection | | |
| Device Identity Settings Date/Time Settings Diagnostics Update Firmware | | SIM 1 SIM 2 Sim card not inserted. Sim card checking. Sim card damaged. | |
| Secongs Backup Reboot Default Settings Management | * SIM Card detection is performed o | only at time of booting the system. | Refresh |
| SNMP Logs | | | |
| | , č | Copyright © 2008 Geneko. All rights reserved. | |

Figure 7 - 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 at *Figure 8*.

Status - WAN Information

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

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

Screenshot of WAN Router information is shown at Figure 9.



USER MANUAL

| | GWR ROUTER - | CONFIGURATION CO | ONSOLE | | |
|--|----------------------------|-----------------------------------|---------------------|-------------------------|---------|
| Status General Network Information WAN Information | Status: Network Info | prmation | | | |
| Settings Network | Network Ethernet | | MAC Address | 00:1e:5c:00:02:8d | |
| DHCP Server WAN Settings | IP Address 10.0.10.15 | 0 | MTU Size | 1500 | |
| Routing Dynamic Routing Protocol RIP | Netmask 255.255.25 | 55.0 | Broadcast | 10.0.10.255 | |
| VPN Settings GRE IR Filtering | Data Received 174432 | RX 1540 Packets | RX Error Packets | 0 RX Dropped Packets | 0 |
| Maintenance Administrator Password Device Identity Settings | Data 312877 Transmitted | 7 TX 567 Packets | TX Error Packets | 0 TX Dropped Packets | 0 |
| Date/Time Settings Diagnostics Update Firmware | DHCP Server | stopped | | | |
| Settings Backup Reboot Default Settings | | | | | Refresh |
| Management | | | | | |
| SNMP Logs | | | | | |
| Logout | | | | | |
| | | Copyright © 2008 Geneko. All rigi | nts reserved. | | |

Figure 8 - Network Information

| Status | Status: WAN Information | i | | | | | | | | |
|--|---|------------------------------------|--|--|---------|--|--|--|--|--|
| Network Information | Mobile Information | Mobile Information | | | | | | | | |
| Settings Network | Modem Manufacturer | SIEMENS | | | | | | | | |
| DHCP Server WAN Settings | Modern Model | SIEMENS MC75 | | | | | | | | |
| Routing Dynamic Routing Protocol RIP | Revision | 355634006265786 REVISION 04.001 | | | | | | | | |
| VPN Settings GRE | Mobile Connection | | | | | | | | | |
| IP Filtering Maintenance | Operator | | | | | | | | | |
| Administrator Password Device Identity Settings Date/Time Settings Diagnostics Update Firmware | Cell ID | 04C6 | | | | | | | | |
| | Signal Strength | | | | | | | | | |
| Reboot Default Settings | Mobile Statistics | | | | | | | | | |
| Management Serial Port | Protocol Point-Point Proto | looc | Activity Time | 00:04:40 | | | | | | |
| SNMP Logs | WAN 172.29.8.6 Address | | PPP Address | 10.0.0.1 | | | | | | |
| Logout | Primary 192.168.111.100 DNS Address | | Second DNS Address | unknown | | | | | | |
| | Data Received 52 Data 101 | RX 4 Packets TX 6 Packets | RX Error Packets TX Error Packets | 0 RX Dropped Packets 0 TX Dropped Packets | 0 | | | | | |
| | | | 1940-1940 - 1940 | BUR VICING & | Refresh | | | | | |

Figure 9 - 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 <i>Reload</i> to discard any changes and reload previous settings. | | | | |
| Save | Click <i>Save</i> button to save your changes back to the GWR Router. Whether you make changes or not, router will reboot every time you click <i>Save</i> . | | | | |

Table 3 - Network parameters

At the *Figure 10* you can see screenshot of *Network* Tab configuration menu.

| | GWR ROUTER | - CONFIGURATION CONSOLE |
|---|---|---|
| Status General Network Information WAN Information Betrings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RIP VPN Settings GRE IP Filtering Maintenance Administrator Password Device Identity Settings Date/Time Settings Diagnostics Update Firmware Settings Backup Reboot Default Settings Management Serial Port SNMP Logs | Network O Obtain an IP addr O Use the following IP Address Subnet Mask Local DNS | PECONFECTRATION CONSULE ess automatically using DHCP IP address: |
| LUGUUL | | Copyright © 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ |

Figure 10 - 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 computer 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 <i>Enable DHCP Server</i> . To setup DHCP server fill in the IP Starting Address and IP Ending Address fields. Uncheck <i>Enable DHCP Server</i> check box to stop the GWR Router from acting as a DHCP server. When Unchecked, you must have another DHCP server on your LAN, or else the computers must be manually configured. | | | | |
| IP Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. | | | | |
| IP Ending Address | 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 assigns to systems that support DHCP client capability. Select <i>None</i> 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 <i>Used by ISP</i> to have the GWR Router assigns DNS IP address to DHCP clients. DNS address is provided by ISP (automatically obtained from WAN side). This option is available only if GPRS connection is active. Please establish GPRS connection first and then choose this option. Select <i>Used Defined</i> to have the GWR Router assigns DNS IP address to DHCP clients. DNS address is manually configured by user. | | | | |
| Static Lease Reservation | This field specifies IP addresses that will be dedicated to specific DHCP Client based on MAC address. DHCP server will always assign same IP address to appropriate client. | | | | |
| Address Exclusions | This field specifies IP addresses that will be excluded from the pool of DHCP IP address. DHCP server will not assign this IP to DHCP clients. | | | | |
| Add | Click <i>Add</i> to insert (add) new item in table to the GWR Router. | | | | |
| Remove | Click <i>Remove</i> to delete selected item from table. | | | | |
| Save | Click <i>Save</i> to save your changes back to the GWR Router. | | | | |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. | | | | |

Table 4 - DHCP Server parameters



| us | DHCP Server | | | | | | | | | |
|--|--|--|---|---|--|--|--|--|--------|--|
| eneral atwork Information AN Information ings atwork -QP Server AN Settings | Enable Dynamic IP Address range: From | : Host (| Configuration | Protocol (DHCP) Se | rver Le | ase Dura | tion: 0 days | 8 hrs 0 mins | | |
| outing volamic Routing Distance | То | 10.0 | 0.10.160 | | | | | | | |
| RIP | Primary DNS | | | | S | econdary I | DNS | | | |
| PN Settings | None | | | | | None | | | | |
| GRE | O Used by ISP | | | | | O Used I | by ISP | | | |
| P Filtering | Olleer Defined | | | | Î I | | -, | | | |
| dministrator Password | C COCI DONNOG | | | | | 0 0001 2 | | | | |
| evice Identity Settings ate/Time Settings | | Statia I. | anaa Daaawuu | tions - | | A delega | - Fuchaciones | | | |
| iagnostics | i i i i i i i i i i i i i i i i i i i | | TD Address | uons: | 0 | Auuress | S EXClusions: | Const Andrewson | 0 | |
| ettings Backup | | nable | IP Address | mac Audress | Action | Enable | 10.0.10.152 | 10.0.10.152 | Retion | |
| eboot | | | | | Add | | 10.0.10.152 | 10.0.10.153 | Kem | |
| efault Settings | | | | | | | | | Add | |
| erial Port NMP ogs | * Mac Address format: xx:xx * The IP address pool must s does not meet this requirement * A reservation IP address DHCP server. The DHCP serv * An IP address exclusion rar | pecify ac nt. ust not b ver will ig nge must | xixx ddresses that are i pe the same as the gnore a reservatio t specify valid IP a | n the subnetwork of the IP address of the DHCP n that does not meet the addresses in the subnetw | GWR Router. Th server itself. It n se requirements. ork of the DHCP | e DHCP serv iust be a vali server. The | ver will not operate if this (id IP address in the subnet DHCP server will ignore a | configuration twork of the in exclusion that | Reload | |

Figure 11 - 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 parameters (*Figure 12*).

| | WAN Calibra | | | | | | |
|--|-----------------------------|--------------------------------|------------|-----------------|-----------------|------------------|--------|
| atus | WAN Settings | | | | | | |
| General Network Information WAN Information | SIM 1 | | | SIM 2 | | | |
| ttings | Fnabled | | | Enabled | | | |
| Network | Providor | tolonor | | Provider | tolokom | | |
| DHCP Server | Flovider | DAD | | Flovidei | IEIEKOIII | 1 | |
| Routing | Autnentication | PAP | | Autnentication | PAP-CHAP V |] | |
| Dynamic Routing Protocol | Username | geneko | | Username | mts | | |
| RIP /DN Settings | Password | geneko | | Password | 064 | | |
| GRE | Dial string | ATD*99***1# | | Dial string | ATD*99***1# | | |
| IPSec | Initial string | at and control "ID" "goopolko" | | Initial string | ot adapt=1 " | D" "aaro ganaka0 | |
| P Filtering | Indai su ing | at+cgdcont=1, IP, geneko | | unual suring | at+cgucont-1, 1 | F, corpgenekou | |
| Administrator Password | Number of retry | 1 | | Number of retry | 6 | | |
| Device Identity Settings | Pin Enabled | 1234 | | Pin Enabled | 1234 | | |
| Date/Time Settings | | | | Enable Failover | After 15 v m | in | |
| Magnostics Ipdate Firmware Settings Backup Reboot | Advanced | | | Advanced | | Poload | |
| Default Settings | | | | | | Reload | Jesave |
| agement Serial Port | Wireless Module Status | | | | | | |
| DODS | Mobile Device Type | Mobile Communication | Mobile Pro | vider Port | t | | |
| ards | SIEMENS MC75 | EDGE Attached | | pppl | 0 | | |
| nternet Access GRE Tunnel PSec Tunnel | Connection Status: Connecte | ad . | | ^ | | | |
| | | | | | | | |

Figure 12 - 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. From the pop up window choose appropriate protocol (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. | | | | |
| 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. | | | | |
| Initial String | This field specifies Initial String for GSM/UMTS modem initialization. In most cases you can leave this field at default values. | | | | |
| Enable Failover | Mark this option in order to enable failover feature. This feature is used when both SIM have been enabled. You specify the amount of time after which Failover feature brings down current WAN connection (SIM2) and brings up previous WAN connection (SIM1). | | | | |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. | | | | |



| Save | Click <i>Save</i> to save your changes back to the GWR Router. | | | |
|------------------------|---|--|--|--|
| Refresh | Click <i>Refresh</i> 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 12 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 enables 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 n (default 10). |
| CHAP restart interval sec | Set the CHAP restart interval (retransmission timeout for challenges) to n seconds (default 3). |
| Refuse MS-CHAP | With this option, pppd will not agree to authenticate itself to the peer using MS-CHAP. |
| Refuse MS-CHAPv2 | With this option, pppd will not agree to authenticate itself to the peer using MS-CHAPv2. |
| Refuse EAP | With this option, pppd will not agree to authenticate itself to the peer using EAP. |
| Connection debugging | Enables connection debugging facilities. If this option is given, pppd will log the contents of all control packets sent or received in a readable form. |
| Maximum Transmit Unit 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 n . Pppd will ask the peer to send packets of no more than n bytes. The value of n must be between 128 and 16384; the default is 1500. |
| VJ-Compression | Disable Van Jacobson style TCP/IP header compression in both directions. |
| VJ-Connection-ID Compression | Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression. With this option, pppd will not omit the connection-ID byte from Van Jacobson compressed TCP/IP headers. |
| Protocol Field Compression | Disable protocol field compression negotiation in both directions. |
| Address/Control Compression | Disable Address/Control compression in both directions. |
| Predictor-1 Compression | Disable or enable accept or agree to Predictor-1 compression. |
| BSD Compression | Disable or enable BSD-Compress compression. |
| Deflate Compression | Disable or enable Deflate compression. |
| Compression Control Protocol negotiation | Disable CCP (Compression Control Protocol) negotiation. This option should only be required if the peer is buggy and gets confused by requests from pppd for CCP negotiation. |
| Magic Number negotiation | Disable magic number negotiation. With this option, pppd cannot detect a looped-back line. This option should only be needed if the peer is buggy. |
| Passive Mode | Enables the "passive" option in the LCP. With this option, pppd will attempt to initiate a connection; if no reply is received from the peer, pppd will then just wait passively for a valid LCP packet from the peer, instead of exiting, as it would without this option. |
| Silent Mode | With this option, pppd will not transmit LCP packets to initiate a connection until a valid LCP packet is received from the peer (as for the "passive" option with ancient versions of pppd). |
| Append domain name | Append the domain name d to the local host name for authentication purposes. |
| Show PAP password in log | When logging the contents of PAP packets, this option causes pppd to show the password string in the log message. |
| Time to wait before re- initiating the link sec | Specifies how many seconds to wait before re-initiating the link after it terminates. The holdoff period is not applied if the link was terminated because it was idle. |
| LCP-Echo-Failure | If this option is given, pppd will presume the peer to be dead if n LCP echo- requests are sent without receiving a valid LCP echo-reply. If this happens, pppd will terminate the connection. This option can be used to enable pppd to terminate after the physical connection has been broken (e.g., the modem has hung up) in situations where no hardware modem control lines are available. |
| LCP-Echo-Interval | If this option is given, pppd will send an LCP echo-request frame to the peer every <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. |
| Add a default route | Add a default route to the system routing tables, using the peer as the gateway, when IPCP negotiation is successfully completed. This entry is removed when the PPP connection is broken. |

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 full functional router with static routing capability. *Figure 13* show screenshot of Routing Menu.

| | GWR RC | OUTER - CONF | FIGURATION CON | NSOLE | | | | | |
|--|------------|---------------------|-----------------------------------|---|-------------|-----------|--------|--------|------|
| Status General | Routing | | | | | | | | |
| Network Information WAN Information | Routina ta | ible (Local network |); | | | | | | |
| Network | Enable D | est Network | Netmask | Gateway | Metric | Interface | | | |
| DHCP Server | ☑ 11 | 0.0.0.1 | 255.255.255.255 | * | 0 | v 0qqq | | | |
| WAN Settings Routing | 2 1 | 0.0.10.0 | 255 255 255 0 | * | n | ethî v | | | |
| Dynamic Routing Protocol | | 0.0.10.0 | 200.200.200.0 | | , ° | Calo | | | |
| RIP | Routing ta | ible: | | - | | | | | |
| VPN Settings | Enable D | est Network | Netmask | Gateway | Metric | Interface | Action | | |
| GRE | ☑ 0. | .0.0.0 | 0.0.0.0 | | 1 | ррр0 💌 | Rem | | |
| IP Filtering Maintenance | ✓ 1: | 92.168.1.0 | 255.255.255.0 | | 1 | gre1 💌 | Rem | | |
| Administrator Password | | | İ. | | 1 | eth0 💌 | Add | | |
| Device Identity Settings | | | | | | | | | |
| Date/Time Settings | | | | | | | | | |
| Update Firmware | Forward n | rotocol connection | e from ovternal notwo | rke to the following intr | anal devic | 201 | | | |
| Settings Backup | Enable T | unneling Protoco | Cond to | | aniai uevio | 50. | | | |
| Reboot Default Settings | | | 10001 | | | | | | |
| Management | | | 10.0.0.1 | | | | | | |
| Serial Port | | SP | 10.0.0.2 | | | | | | |
| SNMP | Forward T | CP/UDP connection | ns from external netwo | orks to the following in | ernal devid | ies: | | | |
| Logs | Enable Pi | rotocol Source P | Port Dest IP / | Address Destinat | ion Port | Action | | | |
| Logout | ПГ | | | | | Add | | | |
| | | | | | | | | | |
| | | | | | | | | Reload | Save |
| | | | Copyright © 2008 Ge http://www | eneko. All rights reserved. w. geneko.co. rs <u>/</u> | | | | | |

Figure 13 - Routing configuration page

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

- Create/Edit/Remove routes (including default route),
- Reroute GRE and IPSEC packet to dedicated destination at inside network
- Port translation Reroute TCP and UPD packets to desire destination at inside 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> represent LAN interface an <i>ppp0</i> represent 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. | | | | |
| Sent 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 redirection | | | | |
| Enable | This check box allows you to activate/deactivate this static port translation. | | | | |
| Protocol | This is the IP protocol type. | | | | |
| Source Port | This is the TCP/UDP port of incoming traffic. | | | | |
| Dest IP address | This field specifies IP address of the Virtual server (Computer on the LAN where traffic is redirected). | | | | |
| Destination Port | This is the TCP/UDP port of application. | | | | |
| Add | Click <i>Add</i> to insert (add) new item in table to the GWR Router. | | | | |
| Remove | Click Remove to delete selected item from table. | | | | |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. | | | | |
| Save | Click <i>Save</i> to save your changes back to the GWR Router. After pressing <i>Save button</i> it make take more then 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 14*).

| | | IN IGONATION CONSOLL | | | |
|--|---|--|----------|------------|---------|
| Status General | Routing Information Pro | otocol | | | |
| Network Information WAN Information | Routing Manager | | | | |
| Settings Network | Hostname | Router |] | | |
| DHCP Server | Password | zebra |] | | |
| WAN Settings Routing | Enable log | | | | |
| Dynamic Routing Protocol RIP | Port to Bind At | | | | |
| VPN Settings | O User Defined | | | | |
| GRE IP Filtering | Oefault [2601] | | | | |
| Maintenance administrator Password | ⁶ Hostname: Prompt name that will be dis | played on telnet console. | | | |
| Date/Time Settings | RIPD | | | | |
| Diagnostics Update Firmware | Hostname | ripd |] | | |
| Settings Backup Reboot | Password | zebra | 7 | | |
| Default Settings | Port to Bind At | | | | |
| Management Serial Port | O User Defined | | | | |
| SNMP Logs | Oefault [2602] | | | | |
| * | * Hostname: Prompt name that will be dis | played on telnet console for the Routing Information Protocol will listen to | Manager. | | |
| Logout | . er te en e at este por tre service | | | Reload | Save |
| | | | | | |
| | Routing Information Protoc | col Status | | | |
| | Status: stopped | | | Start Stop | Restart |

Figure 14 - 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 <i>Save</i> to save your changes back to the GWR Router. | | | |
| Reload | Click <i>Reload</i> 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 for a specific network. One common application is secure communications 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.

| VPN Settings / GRE Tunneling Parameters | | | |
|---|---|--|--|
| Label | Description | | |
| Enable | This check box allows you to activate/deactivate VPN/GRE traffic. | | |
| Local Tunnel Address | This field specifies IP address of virtual tunnel interface. | | |
| Local Tunnel Netmask | This field specifies the IP netmask address of virtual tunnel. This field is unchangeable, always 255.255.255.252 | | |
| Tunnel Source | This field specifies IP address of tunnel source. | | |
| Tunnel Destination | This field specifies IP address 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. | | |

Click *VPN Settings* Tab, to open the VPN configuration screen. At the *Figure 15* you can see screenshot of *GRE* Tab configuration menu.



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

Table 9 - GRE parameters

| ation (GRE) Tunneling | ling | | | | | | |
|--|-----------------|-----------------------|-----------|---|---|---|---|
| Local Tunnel Netmask | Tunnel Source | Tunnel Destination | Interface | KeepAlive Enable | Period | Retries | Action |
| 255.255.255.252 | 52 172.27.76.82 | 172.27.76.80 | gre1 | | | | Rem |
| | | | | | | | Add |
| ual tunnel interface (ways 255,255,255,252) rce destination | | | | | Re | load | Save |
| | | | | Canualists (N 2008 Canalas All sinks assaured | Convicts @ 2009 Canalis . All victors researced | Copyright © 2008 Geneko, All rights reserved. | Copyright @ 2008 Geneko. All rights reserved. |

Figure 15 - 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 to 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 16* 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.

| | GWR ROU | JTE | ER – CONFI | IGURAT | 10N C | ONSOLE | | | | | | |
|--|--|--|---|--------------------------------------|---|---|--------------------------------|-------------|--------------|----------------|-------------|---------|
| Status General Network Information WAN Information | Internet Pr Summary | roto | ocol Securit | y | | | | | | | | |
| Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RIP | Tunnels Used Tunnels Avaib Add New T | ole Tunn | el | 1 | 5 | | | | | | | |
| VPN Settings | Γ | No. | Name | Enabled | Status | Enc/Auth/Grp | Advanced Setup | Local Group | Remote Group | Remote Gateway | Action | |
| GRE IPSec IR Filtering | [| 1 | ipsec_wizard | yes | started | Ph1: DES/MD5/1 Ph2: DES/NULL/none | none | 10.10.10.11 | 10.10.10.13 | 10.10.10.12 | Delete Edit | |
| Maintenance Administrator Password Device Identity Settings Date/Time Settings Ubgonetics Update Firmware Settings Backup Reboot Default Settings Management Serial Port SMMP Logs Wizards Intermet Access GRE Tunnel IPSec Tunnel | Reducing the MTU Recommended M Press Refresh be entropy of the status of the | I size o ITU siz utton descri is run innel el is di c is no | on the clent side, a ce on client side 13 to re-check IPSec ption: ning and tunnel's: is up own ot running or tunn | can help elim 00 waiting for o | inate some us ther end to oled | connectivity problems occur | ing at the protocol level | | | Start | Stop | Refresh |
| Logout | | | | | | | | | | | | |
| | | | | | Сору | right © 2008 Geneko. All ri http://www.geneko. | ghts reserved. . rs/ | | | | | |

Figure 16 - IPSec Summary screen

| VPN Settings / IPSec Summary | | | |
|------------------------------|--|--|--|
| Label | Description | | |
| Tunnels Used | This is the number of IPSec tunnels being defined. | | |
| Tunnels Available | This is the number of available, not yet defined, IPSec tunnels. | | |
| No | This filed indicates the number of the IPSec tunnel. | | |
| Name | Field shows the Tunnel Name that you gave to the IPSec tunnel. | | |
| Enable | This field shows if tunnel is enabled or disabled. After clicking on <i>Start</i> button, only enabled tunnels will be started. | | |
| Status | Field indicates status of the IPSec tunnel. Click on <i>Refresh</i> 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 Setup | Field shows the chosen options from IPSec Advanced section by displaying the first letters of enabled options. | | |
| Local Group | Field shows the IP address and subnet mask of the Local Group. | | |
| Remote Group | Field displays the IP address and subnet mask of the Remote Group. | | |
| Remote Gateway | Field shows the IP address of the Remote Device. | | |



| Delete | Click on this link to delete the tunnel and all settings for that particular tunnel. |
|----------------|--|
| Edit | This link opens screen where you can change the tunnel's settings. |
| Add New Tunnel | Click on this button to add a new Device-to-Device IPSec tunnel. After you have added the tunnel, you will see it listed in the Summary table. |
| Start | This button starts the IPSec negotiations between all defined and enabled tunnels. If the IPSec is already started, Start button is replaced with Restart button. |
| Stop | This button will stop all IPSec started negotiations. |
| Refresh | Click on this button to refresh the Status field in the Summary table. |

Table 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 | 2 | |
| Local Group Setup | | |
| Local Security Gateway Type IP Address | IP Only 172.29.8.4 | |
| Local Security Group Type IP Address | | |
| Remote Group Setup | | |
| Remote Security Gateway Type | IP Only 💌 | |
| IP Address | | |
| Remote Security Group Type IP Address | IP V | |

Figure 17 - IPSec Settings part I



USER MANUAL

| IPSec Setup | |
|--|---|
| Keying Mode Phase 1 DH Group Phase 1 Encryption Phase 1 Authentication Phase 1 SA Life Time Perfect Forward Secrecy | IKE with Preshared key Group1 DES MD5 28800 seconds |
| Phase 2 Encryption Phase 2 Authentication Phase 2 SA Life Time Preshared Key | DES MD5 MD5 MD5 MO5 MD5 MD5 MD5 MD5 MD5 MD5 MD5 MD |
| Advanced | |
| Aggressive Mode Compress (Support IP F Dead Peer Deection (DP NAT Traversal | Payload Compression Protocol (IPComp)) D) 20 sec |



| | 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. <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. | | | |
| 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. | | | |
| 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> <i>If you select a NULL method of encryption, the next Phase 2 Authentication method cannot be NULL and vice versa.</i> |
| 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. |
| Aggressive Mode | There are two types of Phase 1 exchanges, Main Mode and Aggressive Mode. Aggressive Mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, don't use this option (Main Mode will be used). If network speed is preferred, select Aggressive Mode. Both ends of the IPSec tunnel must use the same mode of exchanges. <u>NOTE:</u> If the GWR Router is at both ends, it is sufficient to enable Aggressive mode only at one end and the other end will automatically detect that Aggressive mode is proposed and switch to this mode. |
| Compress (IP Payload Compression Protocol (IP Comp)) | IP Payload Compression is a protocol that reduces the size of IP datagram. Select this option if you want the Router to propose compression when it initiates a connection. |
| Dead Peer Detection (DPD) | When DPD is enabled, the Router will send periodic HELLO/ACK messages to check the status of the IPSec tunnel (this feature can be used only when both peers or IPSec devices of the IPSec tunnel use the DPD mechanism). Once a dead peer has been detected, the Router will disconnect the tunnel so the connection can be re-established. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent). The default interval is 20 seconds. |
| NAT Traversal | Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947. <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. |
| Back | Click <i>Back</i> to return on IPSec Summary screen. |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. |
| Save | Click <i>Save</i> to save your changes back to the GWR Router. After that router automatically goes back and begin negotiations of the tunnels by clicking on the Start button. |

Table 11 - IPSec Parameters


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 <i>Add</i> to insert (add) new item in table to the GWR Router. |
| Remove | Click <i>Remove</i> 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 <i>Add</i> to insert (add) new item in table to the GWR Router. | | | | |
| Remove | Click <i>Remove</i> to delete selected item from table. | | | | |
| | Demilitarized Zone Host Settings | | | | |
| MZ Private IP Address | This check box allows/forbidden host to access to the GWR Router. | | | | |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. | | | | |
| Save | Click <i>Save</i> to save your changes back to the GWR Router. | | | | |

Table 12 - IP filtering parameters

| | GWR R | OUTER - CON | FIGURATION | CONSC | DLE | | | | | | | |
|---|------------------------------|--|---------------------------------|-----------------|-----------------------------|-----------------------------|-------------------|--------------|-----|--|--------|--------|
| Status General | [IP Filter | ing | | | | | | | | | | |
| Network Network Network Network | ○ Disable | all Firewall DMZ | | | | | | | | | | |
| WAN Settings Routing Dynamic Routing Protocol RIP VPN Settings GRE | Firewall Aut | Settings omatically allow acc ccess from the follo | cess from all devices: | ces on the | local subne | t | | | | | | |
| IPSec Contification | Enable | IP Address | Service | Protoco | Port | Action | | | | | | |
| My Certificates | V | 10.0.10.24 | HTTP 🔽 | TCP | 80 | Rem | | | | | | |
| Trusted CAs IP Filtering | | 10.0.10.24 | Telnet 🔽 | TCP | 23 | <u>Rem</u> | | | | | | |
| Maintenance | | | All Traffic 🚩 | TCP/UDP | 1-65535 | Add | | | | | | |
| Administrator Password Device Identity Settings Date/Time Settings Diagnostics | Allow a | ccess from the follo | wing networks: | | | | | | | | | |
| Update Firmware | Enable | IP Address | Subnet Mas | k S | ervice | Protoco | l Port | Action | | | | |
| Settings Backup Reboot | | 10.0.10.24 | 255.255.255.0 |) C | ustom 🔽 | TCP 🔽 | 56 | <u>Rem</u> | | | | |
| Default Settings | | | | A | II Traffic 🔽 | TCP/UDF | 1-65535 | Add | | | | |
| Serial Port SNMP Logs | Caution: Carefu Demilitar | ly review settings before ized Zone Host Se | applying changes. In attings | correct setting | s can make th | e GWR Route | r inaccessible fr | om the netwo | rk. | | | |
| Logout | DMZ Privat | e IP Address | 10.0. | 10.88 | | | | | | | | |
| | | | | Copyright © | 2008 Geneko ttp://www.ge | . All rights re neko.rs/ | served. | | | | Reload | d Save |

Figure 19 - 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.



Figure 20 - IP Filtering configuration example

| | GWR F | OUTER - COM | FIGURATION | CONSC |)LE | | | | | |
|---|-----------------|--|------------------------|--------------------------|----------------------------|-----------------------------|-----------------|-----------------|--|--------|
| Status General | IP Filter | ing | | | | | | | | |
| Network Information WAN Information Settings Network | ○ Disable | all Firewall DMZ | | | | | | | | |
| UHCP Server WAN Settings Routing Dynamic Routing Protocol RIP VPN Settings GRE | Firewall Aut | Settings omatically allow ac ccess from the foll | cess from all device | es on the l | ocal subne | E. | | | | |
| IPSec | Enable | IP Address | Service | Protocol | Port | Action | | | | |
| Certificates My Certificates | | 192.168.1.1 | ICMP 💌 | | | Rem | | | | |
| Trusted CAs | | 192.168.2.1 | All Traffic 💌 | TCP/UDP | 1-65535 | Rem | | | | |
| IP Filtering | | 192 168 3 1 | Custom ¥ | TCP V | 222 | Rem | | | | |
| Administrator Password | | 102 168 4 1 | Custom | | 69 | Pom | | | | |
| Device Identity Settings | | 132.100.4.1 | | | 1.05505 | <u>ixeili</u> | | | | |
| Dater me Securgs Diagnostics Update Firmware Settings Backup Reboot Default Settings | Allow a | ccess from the foll | owing networks: | (Se | ervice | Protoco | Port | Action | | |
| Management | | | oublice Mast | | II Traffic 🔽 | TCP/UDF | 1-65535 | Add | | |
| Serial Port | | | | | | 1.0700 | . 00000 | | | |
| Logs | Caution: Carefu | ly review settings befor | applying changes. Inco | orrect setting | s can make th | GWR Router | inaccessible fr | om the network. | | |
| 1000000 | Demilitar | ized Zone Host S | ettings | - | | | | | | |
| Logout | DMZ Priva | te IP Address | | | | | |] | | |
| | | | | | | | | | | Reload |
| | | | C | Copyright © <u>hi</u> | 2008 Geneko tp://www.ge | . All rights re neko.rs/ | served. | | | |

Figure 21 - IP Filtering settings



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 - 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 22*.

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 - CONFIGL | JRATION CONSOLE | |
|---|--|---|---|
| Status General Network 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 Date/Time Settings Date/Time Settings Date/Time Settings Date/Time Settings Date/Time Settings Date/Time Settings Default Settings | Administration: Administrator Password User Name Old Password Enable Password Authentication New Password Confirm Password | Password admin •••••• ••••••• | |
| Serial Port SNMP Logs | | | |
| Logout | | Copyright © 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ | |

Figure 22 - Administrator Password configuration page



| | Administrator Password | | | | | |
|-----------------------------------|--|--|--|--|--|--|
| Label | Description | | | | | |
| 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. | | | | | |
| Enable Password Authentication | By this check box you can activate or deactivate function for authentication when you access to web/console application. | | | | | |
| 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 <i>Save</i> button to save your changes back to the GWR Router. | | | | | |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. | | | | | |

Table 13 - Administrator password

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 23*.

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

Table 14 - Device Identity parameters



| | GWR ROUTER - C | ONFIGURATION CONSOLE | |
|--|-----------------------|---|-------------|
| Status General | Administration: Devic | e Identity Settings | |
| Network Information | Settings | | |
| Settings Network | Name | GWR252-B | |
| DHCP Server | Description | Geneko test | |
| WAN Settings Routing | Location | Beograd | |
| Dynamic Routing Protocol RIP | | 4 2 | |
| VPN Settings | | | Reload Save |
| GRE IP Filtering | | | |
| Maintenance | | | |
| Administrator Password Device Identity Settings | | | |
| Date/Time Settings Diagnostics | | | |
| Update Firmware | | | |
| Settings Backup Reboot | | | |
| Default Settings Management | | | |
| Serial Port | | | |
| SNMP Logs | | | |
| Logout | | | |
| | | | |
| | | Copyright © 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ | |

Figure 23 - Device Identity Settings configuration page

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 - C | CONFIGURATION CONSOLE |
|---|------------------------|---|
| Status | Administration: Date/ | /Time Settings |
| Network Information | Current Date and Time | |
| Settings | Date: | 2009/02/07 |
| Network DHCP Server | Time: | 13:53:51 |
| WAN Settings Routing | Date and Time Setup | |
| Dynamic Routing Protocol RIP | Set Manually | |
| VPN Settings GRE | Date: | 2009 🗸 / 02 👻 / 07 👻 |
| IP Filtering | Time: | 13 💌 : 53 💌 : 51 💌 |
| Maintenance Administrator Password Device Identity Settings Date/Time Settings | Sync Clock With Client |] |
| Diagnostics Undate Eirmware | O From Time Server | |
| Settings Backup Reboot | Time Protocol | NTP (RFC-1305) 💌 |
| Default Settings | Time Server Address | |
| Serial Port | | (GMT) Western Europe Time, London, Lisbon, Casablanca, Monrovia |
| SNMP Logs | | Reload Save |
| Logout | | |
| | | Copyright © 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ |

Figure 24 - Date/Time Settings configuration page



| | Date/Time Settings | | | | | |
|------------------------|--|--|--|--|--|--|
| Label | Description | | | | | |
| Set Manually | Sets date and time manually as you specify it. | | | | | |
| 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. | | | | | |
| From Time Server | Sets the local time using the Network Time Protocol (NTP) automatically. | | | | | |
| Time Server Address | Enter the URL or IP address of the NTP server. | | | | | |
| Time Zone | Select your time zone. | | | | | |
| Save | Click <i>Save</i> button to save your changes back to the GWR Router. | | | | | |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. | | | | | |

Table 15 - 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 conect 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.

| | GWR ROUT | ER - CONFIGURATION CONSOLE | |
|---|---|---|------|
| Status General Network Information WAN Information Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RIP VPN Settings | Administration: Ping Utility Ping the IP addres IP Address Response | Diagnostics is of a device in order to communicate with it. 10.0.10.88 Average response time is 1.ms Average response time is 0.9ms Average response time is 0.9ms | |
| GRE IP Filtering Maintenance Administrator Password Device Identity Settings Diagnostics Update Firmware Settings Backup Reboot Default Settings Management Senal Port SNMP Logs | | | Ping |
| Logout | | Copyright @ 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ | |

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

Figure 25 - Diagnostic page

Maintenance - Update Firmware

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

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

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





Figure 26 - 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 | ien | |
| which is a: BKG from: http://10 What should Firefox | file .0.10.150 do with this file? | _ |
| Open with | Notepad (default) | |
| FlashGot Grup File | | |
| Do this gutor | natically for files like this from now on. | |
| | OK Cancel | |

Figure 27 - 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 - 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.





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 | Administration: Default Settings | |
| Network Information WAN Information | Settings | |
| Settings Network DHCP Server WAN Settings | Be carefull when restoring factory default settings. The factory settings will clear all current settings and reboot the system. | |
| Routing Dynamic Routing Protocol | | Restore |
| VPN Settings GRE | | |
| P Filtering Maintenance Administrator Password Device Identity Settings Date/Time Settings Update Firmware Settings Backup Reboot Default Settings | | |
| Management Serial Port SNMP Logs | | |
| Logout | | |
| | Copyright (b) 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ | |

Figure 29 - Default Settings page

Management - Serial Port

There are two methods which can be used to configure router serial port. Administrator can use following serial port settings:

- Configuration console
- Serial to Ethernet converter

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).

Configuration may be performed by serial RS-232C port (DB-9 interface), using following credentials: user "*admin*" and initial password "*admin*". Console port allows partial administration, configuration and control options.

The GWR Router serial port configuration:

- 1. Read and follow the User Manual.
- 2. Connect a serial console cable to the RJ45 console port.



- 3. Serial port parameters:
 - Baud rate: 57600,
 - Data bits: 8,
 - Parity: None,
 - Stop bits: 1,
 - Flow control: None.

Click *Serial Port* Tab to open the Serial Port Configuration screen. Use this screen to configure the GWR Router serial port parameters (*Figure 30*).

| | GWR ROUTER | - CONFIGU | URATION (| CONSOLE | | | | | |
|--|---|-----------------|----------------|------------------|-----------------|--|---|-------------|---|
| Status General | Serial Port | | | | | | | | |
| Network Information WAN Information | Serial Port Settings | | | | | | | | |
| Settings | O Enable configurati | ion console | | | | | | | |
| DHCP Server | Enable serial-ether | ernet converter | r | | | | | | |
| WAN Settings | Bits per second: | 57600 | ~ | | | | | | |
| Routing Dynamic Routing Protocol | Data bits: | 8 | ~ | | | | | | |
| RIP | Parity: | None | ~ | | | | | | |
| VPN Settings | Stop bits: | 1 | ~ | | | | | | |
| IP Filtering | Elow control: | None | ~ | | | | | | |
| Maintenance | Bind to port: | 140116 | | | | | | | |
| Administrator Password Device Identity Settings | The operation | 223 | | | | | | | |
| Date/Time Settings | Type of socket: | raw | × | | | | | | _ |
| Diagnostics Update Firmware Settings Backup | * Port: Valid values [1-65535] | | | | | | ſ | Beload Save | |
| Reboot | | | | | | | L | | |
| Default Settings Management | | | | | | | | | |
| Serial Port | | | | | | | | | |
| SNMP Logs | | | | | | | | | |
| 2095 | | | | | | | | | |
| Logout | | | | | | | | | |
| | | Ċ | Copyright © 20 | 8 Geneko. All ri | ights reserved. | | | | |
| | | | http:/ | (www.geneko.c | :0.rs/ | | | | |

Figure 30 - 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 <i>Reload</i> to discard any changes and reload previous settings. |
| Save | Click <i>Save</i> button to save your changes back to the GWR Router and activate/deactivate serial to ethernet converter. |

Table 16 - Serial port parameters

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 - CO | ONFIGURATION CONSOLE | |
|---|----------------------|---|-------------|
| Status General | Simple Network Manaç | gement Protocol | |
| Network Information | SNMP Settings | | |
| Settings Network | Enable SNMP | | |
| DHCP Server WAN Settings | Get Community | test | |
| Routing Dynamic Routing Protocol | Service Port | | |
| RIP | O User Defined | | |
| VPN Settings | O Default [161] | | |
| IP Filtering | Service Access | Both 👻 | |
| Maintenance | | | |
| Administrator Password Device Identity Settings | | | Reload Save |
| Date/Time Settings | SNMP Status | | |
| Diagnostics Update Firmware Settings Backup Reboot | Status: started | | |
| Default Settings | | | |
| Management | | | |
| SNMP | | | |
| Logs | | | |
| Logout | | | |
| | | Copyright © 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ | |

Figure 31 - SNMP configuration page

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

Table 17 - 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 - CO | DNFIGURATION CONSOLE |
|--|-----------------|---|
| Status | System Logger | |
| Network Information WAN Information | Syslog Settings | |
| Settings Network | Enable Syslog | |
| WAN Settings | Service Server | 10.0.10.88 |
| Routing Dynamic Routing Protocol | Service Port | |
| RIP | O User Defined | |
| VPN Settings GRE | Oefault [514] | |
| IP Filtering Maintenance | | Reload Save |
| Administrator Password | Syslog Status | |
| Device Identity Settings Date/Time Settings Diagnostics Update Firmware | Status: stopped | |
| Settings Backup Reboot Default Settings | | |
| Management | | |
| Serial Port | | |
| Logs | | |
| Logout | | |
| | | Copyright (g) 2008 Geneko. All hights reserved. http://www.geneko.co.rs/ |

Figure 32 - Syslog configuration page

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

| | Syslog Settings |
|----------------|---|
| Label | Description |
| Enable Syslog | Mark this option in order to enable Syslog feature. |
| Service Server | 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. |
| Reload | Click <i>Reload</i> to discard any changes and reload previous settings. |
| Save | Click <i>Save</i> button to save your changes back to the GWR Router and enable/disable Syslog. |

Table 18 - Syslog parameters



Wizards - Internet Access

This wizard helps you to easily configure the Internet connection. You will be asked through three pages about the parameters for the Internet connection. Click *Internet Access* Tab to open the wizard. Use those screens to configure the GWR Router.

Step 1

This screen (*Figure 33*) enables you to configure the LAN settings.

- *IP Address* In this field you must enter the local LAN address of the router.
- Netmask This is the netmask of the local LAN address of the router.
- Local DNS This field holds the address of the local DNS server that you want to use.

| This wizard helps you to easily | IP Address | 10.0.10.150 | |
|---|-------------|---------------|--|
| configure the Internet conflection. | Subnet Mask | 255.255.255.0 | |
| This screen enables you to configure the LAN settings. | Local DNS | | |

Figure 33 - Internet Access Wizard - page 1 of 3

Step 2

This screen (*Figure 34*) enables you to configure the GSM settings.

- *Provider* Enter the name for the Internet connection.
- *Authentication* In this menu you can choose the type of the PPP authentication.
- *Username* Enter the username for your Internet connection. This username is provided by your GSM mobile provider.
- *Password* Enter the password for your Internet connection. This password is provided by your GSM mobile provider.
- *Dial string* Enter the dial string for your Internet connection. This dial string is provided by your GSM mobile provider. In most cases you do not need to change this field.
- *Initial string* Enter the initial string for your Internet connection. This initial string is provided by your GSM mobile provider. In most cases you do not need to change this field, except the APN string which is the Access Point Name of your GSM Internet connection.
- *Pin enabled* If you have enabled the PIN code on your mobile card, check this box and enter the PIN code.

| Internet Access wizard - page 2 of 3 | | |
|---|--|--|
| This screen enables you to configure the GSM settings. | Provider Authentication Username Password Dial string Initial string Pin Enabled | telekom PAP-CHAP v mts 064 ATD*99***1# at+cgdcont=1,"IP","atest 1234 |
| | | Cancel Back Next Finish |

Figure 34 - Internet Access Wizard - page 2 of 3



This screen (*Figure 35*) is a summary of entered parameters on previous pages. If the settings are correct, click on the *Finish* button. If some of parameters are show in red color that parameters are not entered correctly. Please use the *Back* button to enter parameters correctly.

| Internet Access wizard - page 3 of 3 | | | | | | |
|--|----------------|---------------------------|--------|------|------|--------|
| | | | | | | |
| This screen is a summary of entered parameters in previous steps. | Network Se | ttings | | | | |
| If the settings are correct, click on the | IP Address | 10.0.10.150 | | | | |
| Finish button. | Subnet Mask | 255.255.255.0 | | | | |
| | Local DNS | | | | | |
| | | | | | | |
| | Wan Setting | S | | | | |
| | Provider | telekom | | | | |
| | Authentication | PAP-CHAP | | | | |
| | Username | mts | | | | |
| | Password | 064 | | | | |
| | Dial String | ATD*99***1# | | | | |
| | Initial String | at+cgdcont=1,"IP","atest" | | | | |
| | PIN Enabled | х | | | | |
| | PIN Value | 1234 | | | | |
| | | | | | | |
| | | | Cancel | Back | Next | Finish |

Figure 35 - Internet Access Wizard - page 3 of 3

Wizards - GRE Tunnel

This wizard helps you to easily configure the GRE tunnels. You will be asked through four pages about the parameters for the GRE tunnel. Click *GRE Tunnel* Tab to open the wizard. Use those screens to configure the GWR Router.

Step 1

This screen (*Figure 36*) enables you to configure the LAN settings.

- IP Address In this field you must enter the local LAN address of the router.
- Netmask This is the netmask of the local LAN address of the router.
- Local DNS This field holds the address of the local DNS server that you want to use.

| GRE Tunnel wizard - page 1 of 4 | | |
|---|---------------------------|-------------------------------------|
| This wizard helps you to easily configure the GRE tunnels. This screen enables you to configure the | IP Address Subnet Mask | 10.0.10.150 255.255.255.0 |
| LAN settings. | LOCALDINS | Cancel Back Next Finish |

Figure 36 - GRE Tunnel Wizard - 1 of 4

Step 2

This screen (Figure 37) enables you to configure the GSM settings.

- *Provider* Enter the name for the Internet connection.
- Authentication In this menu you can choose the type of the PPP authentication.
- *Username* Enter the username for your Internet connection. This username is provided by your GSM mobile provider.



- *Password* Enter the password for your Internet connection. This password is provided by your GSM mobile provider.
- *Dial string* Enter the dial string for your Internet connection. This dial string is provided by your GSM mobile provider. In most cases you do not need to change this field.
- *Initial string* Enter the initial string for your Internet connection. This initial string is provided by your GSM mobile provider. In most cases you do not need to change this field, except the APN string which is the Access Point Name of your GSM Internet connection.
- *Pin enabled* If you have enabled the PIN code on your mobile card, check this box and enter the PIN code.

| GRE Tunnel wizard - page 2 of 4 | | |
|--|--|--|
| This screen enables you to configure the GSM settings. | Provider Authentication Username Password Dial string Initial string Pin Enabled | telekom PAP-CHAP ♥ mts 064 ATD*99***1# at+cgdcont=1,"[P"."atest 1234 |
| | | Cancel Back Next Finish |

Figure 37 - GRE Tunnel Wizard - 2 of 4

This screen (Figure 38) enables you to configure the GRE settings.

- Local Tunnel Address Enter the local IP address of GRE interface.
- Local Tunnel Netmask This field is automatically generated.
- *Tunnel Source* Enter the IP address of the local WAN interface. If the GSM connection is already established, this field will be automatically generated.
- Tunnel Destination Enter the IP address of the remote WAN interface.
- **Destination** Network Enter the remote network address which will be available through the GRE tunnel. The route to this address will be inserted automatically.
- *Destination Network Netmask* Enter the remote network address netmask.

| This screen enables you to configure the | Local Tunnel Address | 10.10.10.1 | | |
|--|-----------------------------|-----------------|--|--|
| GRE settings. | Local Tunnel Netmask | 255.255.255.252 | | |
| | Tunnel Source | 172.29.8.6 | | |
| | Tunnel Destination | 172.29.8.5 | | |
| | Destination Network | 10.0.10.0 | | |
| | Destination Network Netmask | 255.255.255.0 | | |

Figure 38 - GRE Tunnel Wizard - 3 of 4

Step 4

This screen (*Figure 39*) is a summary of entered parameters on previous pages. If the settings are correct, click on the *Finish* button. If some of parameters are show in red color that parameters are not entered correctly. Please use the *Back* button to enter parameters correctly.



| GRE Tunnel wizard - page 4 of 4 | | | |
|---|---|-----------------|-------------------------|
| | | | |
| This screen is a summary of entered | Network Settings | | |
| If the settings are correct, click on the Finish button. | IP Address 10.0.10.150 Subnet Mask 255.255.255. Local DNS | 0 | |
| | Wan Settings | | |
| | Provider telekom | | |
| | Authentication PAP-CHAP | | |
| | Username mts | | |
| | Password 064 | | |
| | Dial String ATD*99*** | '1 <i>#</i> | |
| | Initial String at+cgdcont= | =1,"IP","atest" | |
| | PIN Enabled x | | |
| | PIN Value 1234 | | |
| | GRE Settings | | |
| | Local Tunnel Address | 10.10.10.1 | |
| | Local Tunnel Netmask | 255.255.255.252 | 2 |
| | Tunnel Source | 172.29.8.6 | |
| | Tunnel Destination | 172.29.8.5 | |
| | Destination Network | 10.0.10.0 | |
| | Destination Network Netmas | k 255.255.255.0 | |
| | | | |
| | | | Cancel Back Next Finish |

Figure 39 - GRE Tunnel Wizard - 4 of 4

Wizards - IPSec Tunnel

This wizard helps you to easily configure the IPSec tunnels. You will be asked through six pages about the parameters for the IPSec tunnel. Click *IPSec Tunnel* Tab to open the wizard. Use those screens to configure the GWR Router.

Step 1

This screen (Figure 40) enables you to configure the LAN settings.

- IP Address In this field you must enter the local LAN address of the router.
- *Netmask* This is the netmask of the local LAN address of the router.
- Local DNS This field holds the address of the local DNS server that you want to use.

| IPSec Tunnel wizard - page 1 of 6 | | | |
|--|-------------|---------------|------------------|
| This wizard helps you to easily | IP Address | 10.0.10.150 |] |
| configure the IPSec tunnels. | Subnet Mask | 255.255.255.0 | |
| This screen enables you to configure the LAN settings. | Local DNS | | |
| | | Cancel | Back Next Finish |

Figure 40 - IPSec Tunnel Wizard - 1 of 6

Step 2

This screen (Figure 41) enables you to configure the GSM settings.

- *Provider* Enter the name for the Internet connection.
- *Authentication* In this menu you can choose the type of the PPP authentication.
- *Username* Enter the username for your Internet connection. This username is provided by your GSM mobile provider.



- *Password* Enter the password for your Internet connection. This password is provided by your GSM mobile provider.
- *Dial string* Enter the dial string for your Internet connection. This dial string is provided by your GSM mobile provider. In most cases you do not need to change this field.
- *Initial string* Enter the initial string for your Internet connection. This initial string is provided by your GSM mobile provider. In most cases you do not need to change this field, except the APN string which is the Access Point Name of your GSM Internet connection.
- *Pin enabled* If you have enabled the PIN code on your mobile card, check this box and enter the PIN code.

| IPSec Tunnel wizard - page 2 of 6 | | |
|--|--|--|
| This screen enables you to configure the GSM settings. | Provider Authentication Username Password Dial string Initial string Pin Enabled | telekom PAP-CHAP V mts D64 ATD*99***1# at+cgdcont=1."IP"."atest 1234 |
| | | Cancel Back Next Finish |

Figure 41 - IPSec Tunnel Wizard - 2 of 6

This screen (*Figure 42*) enables you to configure the Local and Remote Group parameters of the IPSec tunnel.

Local Group Setup:

- *Gateway Type IP Address* Enter the IP address of the local WAN interface. If the GSM connection is already established, this field will be automatically generated.
- *Local Security Group Type* You can choose IP or Subnet. In case you want only one host on the local network behind the tunnel you will choose IP. If you want to use a range of addresses choose Subnet.

Remote Group Setup:

- Gateway Type IP Address Enter the IP address of the local WAN interface.
- *Remote Security Group Type* You can choose IP or Subnet. In case there is only one host on the remote network behind the tunnel you will choose IP. If there is a range of addresses choose Subnet.



| IPSec Tunnel wizard - page 3 of 6 This screen enables you to configure the Local and Remote Group parameters of the IPSec tunnel. | Local Group Setup |
|--|----------------------------|
| | Gateway Type IP Address |
| | Local Security Group Type |
| | IP Address |
| | Remote Group Setup |
| | Gateway Type IP Address |
| | Remote Security Group Type |
| | IP Address |
| | Cancel Back Next Finish |

Figure 42 - IPSec Tunnel Wizard - 3 of 6

This screen () enables you to configure the Phase 1, Phase 2 and Pre-Shared Key parameters of the IPSec tunnel.

- *Phase 1 DH Group* You can choose Group1, Group2 or Group5. Please read the IPSEC section of documentation for the details.
- *Phase 1 Encryption* You can choose DES, 3DES or AES-128. Please read the IPSEC section of documentation for the details.
- *Phase 1 Authentication* You can choose MD5 or SHA1. Please read the IPSEC section of documentation for the details.
- *Perfect Forward Secrecy* Check this box to enable a Perfect Forward Secrecy method. Please read the IPSEC section of documentation for the details.
- *Phase 2 Encryption* You can choose NULL, DES, 3DES or AES-128. Please read the IPSEC section of documentation for the details.
- *Phase 2 Authentication* You can choose NULL, MD5 or SHA1. Please read the IPSEC section of documentation for the details.
- *Preshared Key* Use this field to enter the PreShared Key string. Please read the IPSEC section of documentation for the details.

| This screen enables you to configure the Phase 1, Phase 2 and Pre-Shared Key parameters of the IPSec tunnel. | Phase 1 DH Group Phase 1 Encryption Phase 1 Authentication Perfect Forward Secrecy | Group1 V DES V MD5 V |
|--|---|----------------------------|
| | Phase 2 Authentication | NULL V |
| | Preshared Key | |

Figure 43 - IPSec Tunnel Wizard - 4 of 6



This screen (*Figure 44*) enables you to configure advanced parameters of the IPSec tunnel. You can choose a various advanced parameters for the tunnel. Please read IPSEC section of the documentation for the details.

| IPSec Tunnel wizard - page 5 of 6 | |
|--|--|
| This screen enables you to configure the Advanced parameters of the IPSec tunnel. | Aggressive Mode Compress (Support IP Payload Compression Protocol (IPComp)) Dead Peer Deection (DPD) Sec NAT Traversal |
| | Cancel Back Finish |

Figure 44 - IPSec Tunnel Wizard - 5 of 6

Step 6

This screen (*Figure 45*) is a summary of entered parameters on previous pages. If the settings are correct, click on the *Finish* button. If some of parameters are show in red color that parameters are not entered correctly. Please use the *Back* button to enter parameters correctly.

| IPSec Tunnel wizard - page 6 of 6 | |
|--|--|
| | |
| This screen is a summary of entered parameters in previous steps. | Network Settings |
| If the settings are correct, click on the Finish | IP Address 10.0.10.150 |
| button. | Subnet Mask 255.255.25.0 |
| | Local DNS |
| | |
| | wan settings |
| | Provider telekom |
| | Authentication PAP-CHAP |
| | Username mts |
| | Password 064 |
| | Dial String ATD*99***1# |
| | Initial String at+cgdcont=1,"IP","atest" |
| | PIN Enabled × |
| | PIN Value 1234 |
| | Group Setup |
| | Local Gateway Type IP Address |
| | Local Security Group Type IP |
| | Local IP Address |
| | Remote Gateway Type IP Address |
| | Remote Security Group Type IP |
| | Remote IP Address |
| | IPSec Setup |
| | DH Group Groupt |
| | Encryption DES |
| | Authentication MD5 |
| | Perfect Forward Secrecy x |
| | DH Group1 Group1 |
| | Encryption NULL |
| | Authentication NULL |
| | Preshared Key |
| | Advanced |
| | Aggressive Mode x |
| | Compress x |
| | Dead Peer Deection Enabled x |
| | Dead Peer Deection |
| | NAT Traversal x |
| | |
| | Cancel Back [Next] Finish |

Figure 45 - IPSec Tunnel Wizard - 6 of 6



Logout

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

Device configuration using console

Configuration may be performed via serial RS-232C port (DB-9 interface), using following credentials: user "*admin*" and initial password "*admin*". Console port allows partial administration, configuration and control options.

The GWR Router serial port configuration:

- 4. Read and follow the User Manual.
- 5. Connect a serial console cable to the RJ45 console port.
- 6. Serial port parameters:
 - Baud rate: 57600,
 - Data bits: 8,
 - Parity: None,
 - Stop bits: 1,
 - Flow control: None.

| Bits per second: 57600 | V |
|------------------------|---|
| Data bits: 8 | ~ |
| Parity: None | ~ |
| Stop bits: 1 | ~ |
| Elow control: None | ~ |

Figure 46 - Default serial port parameters

Configuration may be performed by following credentials the user "admin" with initial password "admin".

| ***** | ***** | ****** |
|-------|-----------------|-----------------|
| * | Log in | * |
| ***** | ****** | *************** |
| Enter | ·username>admin | |
| Enter | password> | |





USER MANUAL

After successfully finished process of authentication of username/password you can access *Custom Setup* menu – which is shown at *Figure 48*.

For navigation through menu please use following tips. The changes in settings will be applied after pressing "Q" button and process of saving configuration data. If you change network parameters router will reboot after pressing "Q" button and you will have to wait 1 min before it become available again. Press "*ESC*" button if you want to go back and return to previous menu. If you want to logout and quit console session pres button "L". When you logout you will have to retype username/password if you want to log in router again.

| ** | *************************************** | ****** |
|----|---|--------|
| × | Custom Setup | * |
| ** | *************************************** | ****** |
| × | 1. Network settings | * |
| × | 2. DHCP Server | * |
| × | 3. GPRS/EDGE settings | * |
| × | 4. Routing | * |
| × | 5. Administration | * |
| × | 6. Status | * |
| × | 7. Configuration wizard | * |
| ** | *************************************** | ****** |
| b | back – ESC; logout – l; exit – q | |
| > | | |

Figure 48 - Main configuration menu

Network Settings

To enter the network configuration, select the *Network settings* menu (*Figure 49*) item in *Custom Setup*. To define the network interface IP address (*IP address*), the network mask (*Netmask*), you can choose between static and dynamic IP configuration option.

| × | Network settings | * |
|-----------------|---|--------|
| ************ | *************************************** | ****** |
| * 1. Use statio | c IP address (Y) | * |
| * 2. Obtain an | IP address automatically (N) | * |
| ***** | ****** | ****** |
| back - ESC; log | gout - l; exit - q | |
| > | | |

Figure 49 - Network parameters

Static vs. Dynamic IP Addresses

The demand for public IP addresses continues to grow, yet there are a finite number of public IP addresses available. To solve this problem, wireless carriers have resorted to handing out dynamic IP addresses instead of static or fixed public addresses. With dynamic IP addresses, each device is given an IP address for a limited period of time (usually no more than a few hours), and then the IP address is changed. By using dynamic IP addresses to meet market demand. This creates a challenge for users with mobile terminated applications who need a fixed address to target. Fortunately, solutions to all of the challenges above are available using the GWR Router. For example, the network connection type between the carrier's network infrastructure and the customer's data center can provide some flexibility. Also, a frame relay or Virtual Private Network (VPN) connection between the carrier network and the customer's data center allows remote devices to use private IP address assignments for mobile terminated application connections. A static IP can also be maintained by creating a VPN connection to the end device.

If you want manually to configure TCP/IP parameters of the GWR Router choose option 1. You will get page like one on the *Figure 50*.



| ***** | *********** |
|---|--------------|
| * Static | * |
| *************************************** | ************ |
| * 1. IP (10.0.10.113) | * |
| * 2. Netmask (255,255,255,0) | × |
| *************************************** | *********** |
| back – ESC; logout – l; exit – q >∎ | |

Figure 50 - Network parameters configuration

DHCP Server Settings

Option 2 in *Custom setup* menu (*Figure 48*) is DHCP server. This menu (*Figure 51*) enables you to configure full DHCP server parameters. It is possible to define the beginning – option 2 (*IP Address From*) and end – option 3 (*IP Address To*) of the pool of IP addresses which will be assigned to DHCP clients as well as DNS and excluded IP addresses (currently under construction).

| ** | *************************************** | **** |
|----|---|------|
| × | DHCP Server | * |
| ×× | *************************************** | **** |
| × | 1. Enable DHCP (N) | * |
| × | 2. IP Address From (0.0.0.0) | * |
| × | 3. IP Address To (0.0.0.0) | * |
| × | 4. Address Exclusions | * |
| × | 5. Primary DNS (None) | * |
| × | 6. Secondary DNS (None) | * |
| × | 7. Lease Duration (days: 00 hrs: 08 mins: 20) | * |
| ** | *************************************** | **** |
| b | ack - ESC: logout - l: exit - q | |
| > | | |

Figure 51 - DHCP Server configuration

In the DNS submenu of DHCP Server menu you can configure *Primary* and *Secondary DNS* server.

| ***** | ************* |
|---|---------------|
| * Primary DNS | * |
| ***** | ************* |
| * 1. None | * |
| * 2. Used by ISP | * |
| * 3. User defined (0.0.0.0) | * |
| *************************************** | ****** |
| back - ESC; logout - l; exit - q | |
| > | |
| Figure 52 - Primary D | NS |
| ***** | ***** |
| * Secondary DNS | * |
| ****** | ****** |
| * 1. None | * |
| * 2. Used by ISP | * |
| * 3. User defined (0.0.0.0) | * |
| ****** | ****** |
| back - ESC; logout - l; exit - q | |
| > | |
| 0.0 | |

Figure 53 - Secondary DNS

GPRS/EDGE/HSDPA Settings

To enter the Wireless network GPRS/EDGE/HSDPA configuration, select the *GPRS/EDGE settings* menu item in *Custom Setup* (*Figure 54*). You can select for which SIM card you want to enter the parameters (*Figure 55*).

| ** | ******* |
|----|---|
| × | GPRS/EDGE settings * |
| ** | ****** |
| × | 1. SIM card 1 * |
| × | 2. SIM card 2 * |
| ** | *************************************** |
| b | ack - ESC; logout - l; exit - q |
| > | |

Figure 54 - SIM card selection

Once you choose which SIM card to configure, you can enter initial parameters for GPRS/EDGE/HSDPA access and you can choose authentication type. These parameters you will get from your Mobile provider. The changes in settings will apply after pressing "Q" button and saving configuration data.

| ****** | ** |
|---|----|
| * SIM card 1 | × |
| ****** | ** |
| * 1. Authentication (PAP-CHAP) | × |
| * 2. Username (mts) | × |
| * 3. Password (064) | × |
| * 4. Dial string (at+cgdcont=1.IP.APN1) | × |
| * 5. Initial string (ATD*99***1#) | × |
| * 6. Number of retries (6) | × |
| * 7. SIM enable (Y) | × |
| ***** | ** |
| back - ESC; logout - l; exit - q >∎ | |
| Figure 55 - SIM card GSM/UMTS configuration | |
| ***** | ** |
| * Authentication | * |
| ******** | ** |
| * 1. PAP-CHAP | * |
| * 2. PAP | × |
| * 3. CHAP | * |
| #************************************* | ** |
| back - ESC: logout - l: exit - g | |

Figure 56 - GSM/UMTS authentication

Routing

>

To enter the Routing configuration, select the *Routing* menu item in *Custom Setup*. In this version of router's software you are able only to see routing table and not to add/change routes. For add/edit/remove routes please use web configuration.







| * *********** | | KOUTING TADIE | ******* | ******* | ***** | | |
|------------------|--------------|-----------------|---------|---------|-------|-------|---------|
| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
| 10.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | eth0 |
| 127.0.0.0 | 0.0.0.0 | 255.0.0.0 | U | 0 | 0 | 0 | lo |
| ********* | ************ | *************** | ****** | ****** | ***** | ***** | ******* |

Figure 58 - Routing table (list of all routes)

Administration

Administration menu is available under option 5 (*Figure 48*). The changes in settings will apply after pressing "Q" button and saving configuration data.

| ** | ******* | ********* |
|----|----------------------------------|-----------|
| × | Administration | × |
| ** | ******* | ********* |
| × | 1. Administrator password | * |
| × | 2. Diagnostic | * |
| × | 3. Date/Time settings | * |
| × | 4. Reboot | * |
| × | 5. Factory default settings | * |
| ** | ******** | ********* |
| k | back - ESC; logout - l; exit - q | |
| > | | |

Figure 59 - Administration Menu

If you want to change default username/password please choose option 1 (Administrator password).

| ***** | ******** |
|---|----------|
| * Administrator password | × |
| ****** | ******** |
| * 1. Username (admin) | × |
| * 2. Password (admin) | × |
| * 3. Enable password authentication (N) | × |
| ******* | ******** |
| back - ESC: logout - l: exit - q | |
| > | |

Figure 60 - Administrator password

The GWR Router has basic diagnostic tool (Ping) for testing network connectivity. If you want to use *Ping utility* please use *Diagnostic* under *Administration* menu (*Figure 61*).

| ***** | ***** |
|---|-------|
| Ping utility | * |
| *************************************** | ***** |
| * 1. Ping IP Address of a device () | × |
| * 2. Number of retries (1) | × |
| * 3. Packet size (56) | × |
| * 4. Ping | × |
| ******** | ***** |
| back - ESC; logout - l; exit - q | |
| > | |

Figure 61 - Network diagnostic utility

If you want to setup/change time and date parameters choose Date/time settings (Figure 62).



| × | | Date/T: | me setting | (S | * |
|----|-----------|----------------|------------|-------------|---------|
| ** | ******* | ************* | ********** | | ****** |
| × | 1. Date | (01.01.1970.) | | | * |
| × | 2. Time | (02:05:27) | | | * |
| ** | ******* | ************ | ·********* | ********** | ******* |
| b | ack - ESI | C; refresh - r | : logout - | l; exit - q | |
| > | | N. 6 | 1 1 1 T 1 | 50 B | |

Figure 62 - Date/time parameters

If you want to restore factory default settings you have to possibilities. *Factory default settings* can be applied with default network parameters and without default network parameters. The default IP address of the router is 192.168.1.1. Option 1 (*Settings with default network params*) enable you to restore full factory default settings and option 2 (*Settings without default network params*) enable you to restore default settings without changing network parameters.

| ** | | ***** |
|----|--|-------|
| × | Factoy default settings | * |
| ** | *************************************** | ***** |
| × | 1. Settings with default network params | × |
| × | 2. Settings without default network params | × |
| ** | ************ | ***** |
| b | pack - ESC: logout - l: exit - q | |
| 1 | | |

Figure 63 - List of Restore option

Status

If you want to monitor system and check statuses please choose option *Status* in *Custom* menu. There are options for monitoring LAN and wireless parameters as well as global router parameters.

| ****** | ****** |
|----------------------------|---------------------------------|
| | |
| * 1. General | * |
| * 2. Network information | * |
| * 3. GPRS/EDGE information | * |
| ****** | ******************************* |



General System Information

The *General* page (*Figure 65*) displays the following information about the GWR Router, which can be useful in device monitoring and troubleshooting.

- Model The model of the GWR Router device.
- **Firmware Version** The current firmware version. This information may be used to help locate and download new firmware.
- **OS** The operating system.
- **OS Version -** The current OS version.
- CPU Utilization The amount of CPU resources being used by the GWR Router.
- **Up Time** The amount of time the GWR Router has been running since it was last powered on or rebooted.
- Total/Used/Free Memory The amount of memory (RAM) available, currently in use, and currently not being used.



 MAC Address - A unique network identifier. All network devices are required to have their own unique MAC address. The MAC address is on a sticker on you're the GWR Router. The number is displayed as 12 hexadecimal digits, usually starting with 00:1E:5C.

| ** | **************** | ****** | ** |
|----|--------------------|--------------------------------|----|
| * | | General | * |
| ** | ***** | ***** | ** |
| × | Model: | GWR251-S | * |
| × | Firmware version: | 1.1.7 | * |
| × | 0S: | Linux | * |
| × | OS version: | 2.6.8.1-crus2.0.8 | × |
| × | CPU utilization: | CirrusLogic ARM9 EP9302 200Mhz | * |
| × | Up time: | 02:07:31 | * |
| × | Total memory: | 29520 | * |
| × | Used memory: | 25784 | * |
| × | Free memory: | 3736 | * |
| × | MAC address: | 00:1E:5C:00:00:02 | * |
| ** | ****** | ***** | ** |
| b | ack - ESC; refresh | - r; logout - l; exit - q | |
| > | | | |

Figure 65 - List of basic system parameters

Network Information

The *Network information* (*Figure 66*) is used to view more detailed network statistics that may aid in troubleshooting network communication problems. The statistics displayed are those gathered since the tables containing the statistics were last cleared. Descriptions of the network statistics follow.

- **Protocol** The parameter of networks interface.
- Address Hardware (unique) address of networks interface.
- Netmask Mask of network.
- Broadcast Address Broadcast IP Address.
- Metric Number of routers, over which packet must pass.
- MAC Address A unique network identifier. All network devices are required to have their own unique MAC address. The MAC address is on a sticker on you're the GWR Router. The number is displayed as 12 hexadecimal digits, usually starting with 00:1E:5C.
- MTU Maximal size of packet, which is equipment able transmit.
- **Data received -** The total number of received bytes.
- Data transmitted The total number of transmitted bytes.
- **RX Packets/ RX Error Packets/ RX Dropped Packets -** The number of received packets, number of errors, dropped packets.
- **TX Packets/TX Error Packets/TX Dropped Packets -** The number of transmitted packets, number of errors, dropped packets.
- **DHCP Server -** Information about DHCP status.



| × | Netwo | , | |
|----|----------------------|-------------------------------|---------|
| ** | ******* | **************************** | ******* |
| × | Protocol: | Ethernet | ÷ |
| × | Address: | 10.0.0.139 | ÷ |
| × | Netmask: | 255,255,255,0 | • |
| * | Broadcast address: | 0.0.0 | ÷ |
| * | Metric: | 1 | ÷ |
| ÷ | MAC address: | 00:1E:5C:00:00:02 | ÷ |
| ÷ | MTU: | 1500 | • |
| ÷ | | | ÷ |
| • | Data receiced: | 0 | ÷ |
| • | Data transmitted: | 12374 | ÷ |
| • | RX packets: | 0 | ÷ |
| • | TX packets: | 400 | ÷ |
| ٠ | RX error packets: | 12374 | ÷ |
| ÷ | TX error packets: | 0 | ÷ |
| e | RX dropped packets: | 0 | • |
| ÷ | TX dropped packets: | 0 | ÷ |
| ÷ | | | ÷ |
| ÷ | DHCP server: | Stoped | ÷ |
| •* | ******* | ***************************** | ******* |
| b | ack - ESC; refresh - | r; logout - l; exit - q | |

Figure 66 - Status of LAN network connection

GPRS/EDGE Information

The *GPRS/EDGE information* page displays the mobile information, mobile connection and mobile statistics about the GWR Router, which can be useful in device monitoring and troubleshooting.

- Modem Manufacturer A character string, null-terminated describing the modem module.
- Modem Model A character string, null-terminated describing the modem module.
- **Modem Serial Number -** A character string, null-terminated used as a unique ID per modem module.
- **Modem Revision -** A character string, null-terminated describing the modem module's firmware version.
- **Operator -** The Mobile operator.
- **Cell ID** The modem reports this as a 4-hex-digit string. In the mobile statistics it is displayed both as hex and decimal representations. For example: "00C3 (195)"
- **Phone Number -** SIM card phone number.
- **Signal Strength** Returned as a signed integer value. 0 (zero) indicates no signal. Signal strength is indicated as a negative value in units of dBm. The following scale indicates the signal Strength LED ("bars" of signal strength):
 - -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)

Signal strength LED will blink when GPRS/EDGE 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.

- **Protocol** The parameter of networks interface. PPP interface (active connection to GPRS/EDGE).
- **PPP Address -** The IP address of the PPP connection
- WAN Address The IP address in GPRS/EDGE network provided by the mobile service.
- Primary DNS Address IP address of the primary DNS server provided by the mobile service.
- Secondary DNS Address IP address of the secondary DNS server provided by the mobile service.



- **Data received -** The total number of received bytes.
- Data transmitted The total number of transmitted bytes.
- **RX Packets/ RX Error Packets/ RX Dropped Packets -** The number of received packets, number of errors, dropped packets.
- **TX Packets/TX Error Packets/TX Dropped Packets -** The number of transmitted packets, number of errors, dropped packets.

| ** | *************************** | ********************** | ***** |
|----|-----------------------------|------------------------|-------|
| × | GPRS/EDGE in | formation | * |
| ** | ************************ | ****************** | ***** |
| × | Mobile information | | * |
| × | Modem manufacturer: | SIEMENS | + |
| × | Modem model: | SIEMENS MC75 | |
| × | Modem serial number: | 355634003480271 | * |
| × | Modem revision: | REVISION 03.010 | * |
| × | Operator: | YU MOBTEL | * |
| × | Cell ID: | 04C6 | * |
| × | Phone number: | - | * |
| × | Signal strength: | -59dB | * |
| × | | | * |
| × | Mobile connection | | |
| × | Protocol: | unknown | • |
| × | WAN address: | unknown | * |
| × | PPP address: | unknown | * |
| × | Primary DNS address: | unknown | • |
| × | Secondary DNS address: | unknown | • |
| × | | | • |
| × | Mobile statistics | | • |
| × | Data receiced: | 1 <u></u> | |
| × | Data transmitted: | - | |
| × | RX packets: | <u> </u> | , |
| × | TX packets: | 3 4 9) | * |
| × | RX error packets: | | * |
| × | TX error packets: | <u> </u> | + |
| × | RX dropped packets: | | * |
| × | TX dropped packets: | - | * |
| ** | ****** | ******* | ***** |

Figure 67 - GSM/UMTS status

Configuration Wizard

To enter the Configuration wizard, select the *Configuration wizard* menu item in *Custom Setup*. In this version of router's software you are able only to see routing table and not to add/change routes. For add/edit/remove routes please use web configuration.

| ** | ***** | ******** |
|----|---|----------|
| × | Configuration wizard | × |
| ** | *************************************** | ******** |
| × | 1. Internet configuration | × |
| × | 2. VPN/GRE tunneling | × |
| ** | ****** | ******** |
| b | ack - ESC; logout - l; exit - q | |
| > | | |

Figure 68 - Configuration wizard



Configuration Example

GWR Router as Internet Router

The GWR Routers can be used as *Internet router* for a single user or for a grooup 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 69 - 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 required from 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 add 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 tunnels, but it isn't a secure tunneling method. On the diagram below (*Figure 70*) is illustrated simple network with two GWR Routers. Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.



Figure 70 - 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.



USER MANUAL

| | GWR ROUTER - CO | NFIGURATION CONSOLE | |
|---|---|--|-------------|
| Status General | Network | | |
| General Network 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 Date/Time Settings Diagnostics Update Firmware | Obtain an IP address aut Obtain an IP address aut Obtain an IP address If address IP Address I92.16 Subnet Mask I255.25 Local DNS | pmatically using DHCP ess: (8:4.1 (5:255.0 | Reload Save |
| Reboot Default Settings Management Serial Port SNMP Logs Logout | Copy | yright © 2008 Geneka, All rights reserved. http://www.neneka.co.rs/ | |

Figure 71 - 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: 255.255.252 (Unchangeable, always 255.255.252)
 - Tunnel Source: 10.251.49.2
 - Tunnel Destination: 10.251.49.3
 - KeepAlive enable: no
 - Period:(none)
 - Retries:(none)
 - Press ADD to put GRE tunnel rule into GRE table.
 - Press *Save* to accept the changes.



USER MANUAL

| | GWR ROUTER - CONFIGURATION CONSOLE |
|---|--|
| Status General Network Information WAN Information | VPN Settings - GRE Generic Routing Encapsulation (GRE) Tunneling |
| Settings | Enable Local Tunnel Address Local Tunnel Netmask Tunnel Source Tunnel Destination Interface KeepAlive Enable Period Retries Action |
| DHCP Server | ☑ 10.10.10.1 255.255.255.252 10.251.49.2 10.251.49.3 gre1 □ Rem |
| WAN Settings Routing | |
| RIP VPN Settings GRE IP Filtering Maintenance Administrator Password Device Identity Settings Dataptrime Settings Diagnositos Update Firmware Settings Backup Reboot Default Settings Management Senai Port ShMP Logs | Loci Turnel Helmaski (Unchangelabe, Javaya 255 255,252) Turnel Source: Padress of Humel Source Turnel Destination: IP address of Humel destination Period: Yadi Values [3-00] Retens: Yadi Values [1-10] |
| Logout | Copyright © 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ |

Figure 72 - 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

| tue | Routina | | | | | | | | | |
|---|-------------------|--------------------------------|--|------------------------------------|---------------------|-------------|-----------|------------|--|--|
| General | | | | | | | | | | |
| Network Information | | | | | | | | | | |
| WAN Information | D au stime a | | . د است. ط | | | | | | | |
| tings | Rouung | Cable (Local ne | wurk): | | | | | 1 | | |
| Jetwork | Enable | Dest Network | k Netmask | Gate | eway | Metric | Interface | - | | |
| NAN Settings | × | 10.0.0.1 | 255.255.2 | \$55.255 | | 0 | ррр0 🚩 | | | |
| Routing | \checkmark | 10.0.10.0 | 255.255.2 | 55.0 * | | 0 | eth0 💌 | | | |
| Dynamic Routing Protocol | | | | | | | | 1 | | |
| RIP | Routing | table: | | | | | | | | |
| VPN Settings | Enable | Dest Network | k Netmasi | Gate | eway | Metric | Interface | Action | | |
| GRE | | 0.0.0.0 | 0.0.0.0 | | | 1 | ppp0 🚩 | <u>Rem</u> | | |
| IP Filtering | | 192.168.2.0 | 255.255.2 | 55.0 | | 1 | gre1 🔽 | Rem | | |
| Administrator Dassword | | | | | | [| ath0 at | 6 al al | | |
| Device Identity Settinas | | | | | | | eulo | Auu | | |
| Date/Time Settings | | | | | | | | | | |
| Diagnostics | | | | | | | | | | |
| Settings Backup | Forward | d protocol conne | ections from exte | rnal networks to t | the following inter | nal device | es: | | | |
| socarigs backap | Enable | Tunneling Pro | otocol Send to | | | | | | | |
| Reboot | | GRE | 10.0.0.1 | | | | | | | |
| Reboot Default Settings | | ESP | 10.0.0.2 | | | | | | | |
| Reboot Default Settings n agement | | 201 | 10.0.0.2 | | | | | | | |
| Reboot Default Settings nagement Berial Port | | | SNMP Forward TCP/UDP connections from external networks to the following internal devices: | | | | | | | |
| Reboot Default Settings nagement Serial Port SNMP ogg | Forward | d TCP/UDP conr | ections from ext | ernal networks to | the following inte | a nar uevic | | | | |
| Reboot Default Settings hagement Serial Port SNMP Logs | Forward Enable | d TCP/UDP conr Protocol Sou | nections from ext I rce Port | ernal networks to Dest IP Addre | ss Destinatio | n Port | Action | | | |

Figure 73 - 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 ROUTE | R - CONFIGURATION CONS | OLE | |
|--|--|---|-----------|-------------|
| Status General | Network | | | |
| Network Information WAN Information Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RIP | O Obtain an IP ac Ouse the followin IP Address Subnet Mask Local DNS | Idress automatically using DHCP ng IP address: 192.168.2.1 255.255.255.0 |] | |
| VPN Settings GRE IP Filtering Maintenance Administrator Password Device Identity Settings Date/Cime Settings | | | | Reload Save |
| Diagnostics Update Firmware Settings Backup Reboot Default Settings Management | | | | |
| Serial Port SNMP Logs Logout | | | | |
| | | Copyright © 2008 Geneko. All rights ru http://www.geneko.co.rs/ | reserved. | |

Figure 74 - 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: 255.255.252 (Unchangeable, always 255.255.255.252)
 - Tunnel Source: 10.251.49.3
 - Tunnel Destination: 10.251.49.2
 - KeepAlive enable: no
 - Period:(none)
 - Retries:(none)
 - Press ADD to put GRE tunnel rule into GRE table.
 - Press *Save* to accept the changes.


| | GWR ROUTER - CONFIGURATION CONSOLE |
|--|--|
| Status General Network Information WAN Information | VPN Settings - GRE Generic Routing Encapsulation (GRE) Tunneling |
| Settings | Enable Local Tunnel Address Local Tunnel Netmask Tunnel Source Tunnel Destination Interface KeepAlive Enable Period Retries Action |
| Network DHCP Server | ☑ 10.10.10.2 255.255.255.252 10.251.49.3 10.251.49.2 gre1 Rem |
| WAN Settings Routing | |
| RIP VPN Settings GRE IP Filtering Maintenance Administrator Password Device Identity Settings Data/Time Settings Diagnostics Update Firmware Settings Backup Reboot Default Settings Management Senal Port Senal Port Setting Sutt | Loci Turnel Nemaski, Unchangeske, Javay 252-253,252.03 Turnel Source: IP Address of Hurnel Source Turnel Destination: IP Address of Hurnel destination Period: Values [340] Retrie: Value Values [1-10] Source: Values (1-10) |
| Logout | Copyright © 2008 Geneka. All rights reserved. http://www.geneka.co.rs/ |

Figure 75 - 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

| | GWR RO | UTER - CONF | IGURATION CO | NSOLE | | | |
|--|--------------|---------------------|-----------------------|-----------------------|----------------------|-----------|------------|
| Status General | Routing | | | | | | |
| Network Information WAN Information Settings | Routing tab | ole (Local network) | : | | | | |
| Network | Enable De | est Network | Netmask | Gateway | Metric | Interface | |
| DHCP Server | 10 |).0.0.1 | 255.255.255.255 | * | 0 | ррр0 🔽 | |
| VVAN Settings Routing | ✓ 10 | 1.0.10.0 | 255.255.255.0 | * | 0 | eth0 🗸 | |
| Dynamic Routing Protocol | Routing tab | ole: | | | P | | |
| VPN Settings | Enable De | est Network | Netmask | Gateway | Metric | Interface | Action |
| GRE | I 0.0 | 0.0.0 | 0.0.0.0 | | 1 | ppp0 🔽 | Rem |
| IP Filtering | I 19 | 2.168.4.0 | 255.255.255.0 | | 1 | gre1 🔽 | Rem |
| Administrator Password Device Identity Settings | | | | | | eth0 💌 | Add |
| Date/Time Settings Diagnostics Update Firmware | Forward p | rotocol connections | from external netwo | rks to the follo | wing internal device | s: | |
| Reboot | Enable Tu | Inneling Protocol | Send to | | | | |
| Default Settings | 🗖 GI | RE | 10.0.0.1 | | | | |
| lanagement Corial Port | E | SP | 10.0.0.2 | | | | |
| SNMP | Forward T | CP/UDP connections | s from external netwo | ⊐ orks to the foll | owing internal devic | es: | |
| LUGS | Enable Pr | otocol Source Pa | ort Dest IP a | Address D | estination Port | Action | |
| .ogout | T | CP 🔽 | | | | Add | |
| | · | • | r | | | | |
| | | | | | | | Reload Sav |

Figure 76 - 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 77*) is illustrated simple network with two sites. Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.



Figure 77 - 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 195.178.54.1 255.255.255.0
description WAN interface
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 195.200.200.2
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.



| | GWR ROUTER | - CONFIGURATION CONSOLE |
|---|---|---|
| Status General | Network | |
| Network Information WAN Information Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol RIP VPN Settings GRE IP Filtering | Obtain an IP add Use the following IP Address Subnet Mask Local DNS | ess automatically using DHCP IP address: 10.1.1.1 255.255.255.0 195.178.6.36 Reload Save |
| Maintenance Administrator Password Device Identity Settings Diagnostics Update Firmware Settings Backup Reboot Default Settings Management Serial Port SIMP Logs | | |
| Logout | | |
| | | Copyright © 2008 Geneko. All rights reserved. http://www.geneko.co.rs/ |

Figure 78 - 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: 255.255.252 (Unchangeable, always 255.255.255.252)
 - Tunnel Source: 195.200.200.2
 - Tunnel Destination: 195.178.54.1
 - KeepAlive enable: no
 - Period:(none)
 - Retries:(none)
 - Press ADD to put GRE tunnel rule into VPN table.
 - Press *Save* to accept the changes.



| | VPN Setti | ngs - GRE | | | | | | | | |
|---|--|--|---|---------------|-----------------------|-----------|---------------------|--------|---------|-------|
| al | | | | | | | | | | |
| ork Information | Generic Ro | uting Encapsulat | tion (GRE) Tunneling | | | | | | | |
| nformation | | | | | - | | | | | - |
| ork | Enable | Local Tunnel Address | Local Tunnel Netmask | Tunnel Source | Tunnel Destination | Interface | KeepAlive Enable | Period | Retries | Actio |
| Settings | | 10.1.1.1 | 255.255.255.252 | 195.200.200.2 | 195.178.54.1 | gre1 | | | | Rem |
| | | | | | | | | | | |
| 19 | | | | | | | | | | Add |
| Ig hic Routing Protocol ettings Loc or ering Period histrator Password I Identity Settings Time Settings | al Tunnel Addri al Tunnel Netm inel Source: IP inel Destination iod: Valid value ies: Valid value | ess: IP Address of virtu; sk: (Unchangeable, alv address of trunnel sourc IP address of trunnel do [3-60] s [1-10] | al tunnel interface vays 255.255.255.252) e estination | | | | | Re | load (| Savi |
| Ig hic Routing Protocol ettings ettings loc loc loc loc loc loc loc loc | al Tunnel Addri al Tunnel Netm nel Source: IP nel Destination od: Valid value ies: Valid value | ssi IP Address of virtu sck: (Unchangeable, ak address of tunnel d IP address of tunnel d [2=40] [1=10] | al turnel interface wyr 255,255,252,352) e estination | | | | | Re | load | Save |

Figure 79 - GRE configuration page

- Configure GRE Route. Click *Routing* on *Settings* Tab. Parameters for this example are: ٠ -
 - Destination Network: 10.2.2.0
 - _ Netmask: 255.255.255.0

| | GWR ROUTER - CO | ONFIGURATION CC | NSOLE | | | |
|-----------------------------------|---------------------------|----------------------------|-----------------------|------------------|--------------|-------------|
| tatus | Routing | | | | | |
| General Network Information | | | | | | |
| WAN Information | | | | | | |
| ttings | Routing table (Local netv | work): | | | | |
| Network | Enable Dest Network | Netmask | Gateway | Metric | Interface | |
| DHCP Server | 10.0.0.1 | 255.255.255.255 | * | 0 | ррр0 🗸 | |
| wan secungs Routina | 10.0.10.0 | 255.255.255.0 | * | 0 | eth0 v | |
| Dynamic Routing Protocol | - | | | | | |
| RIP | Routing table: | | - | | | |
| VPN Settings | Enable Dest Network | Netmask | Gateway | Metric | Interface Ac | tion |
| GRE | 0.0.0.0 | 0.0.0 | | 1 | ppp0 💌 🛛 🥂 | em |
| IPSEC IP Eiltering | 10.2.2.0 | 255.255.255.0 | | 1 | gre1 💌 R | em |
| ntenance | | | | | oth0 🗸 A | dd |
| Administrator Password | | | | | | |
| Device Identity Settings | | | | | | |
| Date/Time Settings Diagnostics | | | | | | |
| Update Firmware | Forward protocol connec | tions from external netw | orks to the following | g internal devic | es: | |
| Settings Backup | Enable Tunneling Prot | tocol Send to | | | | |
| Reboot | GRE | 10.0.0.1 | | | | |
| Default Settings | ESP | 10.0.0.2 | | | | |
| Pagement Serial Port | | | | | | |
| SNMP | Forward TCP/UDP conne | ections from external netv | vorks to the followin | ng internal devi | ces: | |
| Logs | Enable Protocol Sour | ce Port Dest IP | Address Dest | ination Port | Action | |
| | TCP 💌 | | | | Add | |
| gout | | | 1 | | | |
| | | | | | | Reload Sava |
| | | | | | | |

Figure 80 - Routing configuration page

Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming ٠ 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. On the diagram below *Figure 81* is illustrated simple network with two GWR Routers. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.



Figure 81 - IPSec 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: 10.0.10.1
 - Subnet Mask: 255.255.255.0
 - Press *Save* to accept the changes.



| | GWR ROUTER - | CONFIGURATION CONSOLE | | |
|--|----------------------|------------------------------------|-------------|-------------|
| Status | Network | | | |
| Network Information WAN Information Settings | O Obtain an IP addre | ss automatically using DHCP | | |
| Network DHCP Server | IP Address | 10.0.10.1 | | |
| WAN Settings | Cubert Mark | | | |
| Routing Dynamic Routing Protocol | Subriet Mask | 255.255.255.U | | |
| RIP | Local DNS | 195.78.6.36 | | |
| VPN Settings | | | | |
| GRE IPSec | | | | Reload Save |
| IP Filtering | | | | |
| Maintenance | | | | |
| Administrator Password | | | | |
| Date/Time Settings | | | | |
| Diagnostics | | | | |
| Update Firmware | | | | |
| Reboot | | | | |
| Default Settings | | | | |
| Management | | | | |
| Serial Port | | | | |
| Logs | | | | |
| Wizards | | | | |
| Internet Access | | | | |
| GRE Tunnel | | | | |
| IPSec Tunnel | | | | |
| Logout | | | | |
| | | Copyright © 2008 Geneko. All right | s reserved. | |
| | | http://www.geneko.rs/ | | |
| | | | | |

Figure 82 - 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: IP Only
 - IP Address: 172.29.8.4
 - Local Security Group Type: IP
 - IP Address: 10.0.10.1
 - 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 1
 - Phase 1 Encryption: DES
 - Phase 1 Authentication: MD5
 - Phase 1 SA Life Time: 28800
 - Perfect Forward Secrecy: true
 - Phase 2 DH group: Group 1
 - Phase 2 Encryption: DES
 - Phase 2 Authentication: MD5
 - Phase 2 SA Life Time: 3600
 - Preshared Key: 1234567890

- Advanced
 - Aggressive Mode: true
 - Compress(Support IP Payload Compression Protocol(IPComp)): false
 - Dead Peer Detection(DPD): false
 - NAT Traversal: true
 - Press *Save* to accept the changes.

| Device 2 Device Tunne | |
|---|-------------------------|
| Add New Tunnel | |
| Tunnel Number Tunnel Name Enable | 2 test |
| Local Group Setup | |
| Local Security Gateway Type IP Address | IP Only V 172.29.8.4 |
| Local Security Group Type IP Address | IP V 10.0.10.1 |
| Remote Group Setup | |
| Remote Security Gateway Type IP Address | IP Only V 172.29.8.5 |
| Remote Security Group Type IP Address | IP V 192.168.10.1 |

Figure 83 - IPSEC configuration page I for GWR Router 1

| IPSec Setup | | |
|---|--|------|
| Keying Mode Phase 1 DH Group Phase 1 Encryption Phase 1 Authentication | IKE with Preshared key v Group1 v DES v | |
| Phase 1 SA Life Time Perfect Forward Secrecy | 28800 seconds | |
| Phase 2 DH Group Phase 2 Encryption Phase 2 Authentication Phase 2 SA Life Time Preshared Key | Group1 DES MD5 Group3600 seconds 1234567890 | |
| Advanced | | |
| Aggressive Mode Compress (Support IP P Dead Peer Deection (DP) NAT Traversal | Payload Compression Protocol (IPComp)) 2D)sec | |
| | Back Reload | Save |

Figure 84 - IPSec configuration page II for GWR Router 1



- 🕞 сепеко GWR ROUTER - CONFIGURATION CONSO Summary Tunnels Used 1 Tunnels Avaible 5 Settings Add New Tunnel y ic Routing Protocol VPN Settings No. Name Enabled Status Enc/Auth/Grp Advanced Setup Local Group Remote Group Remote Gateway Action no stopped Ph1: DES/MD5/1 Ph2: DES/MD5/1 2 test A/N 10.0.10.1 192.168.10.1 172.29.8.5 Delete Edit IP Filtering ing the MTU size on the client side, can help eliminate mmended MTU size on client side 1300 ss Refresh button to re-check IPSec tunnels' status unnel status description: nectivity problems occurring at the protocol level Start Stop Refresh inistrator Password ce Identity Settings /Time Settings started - ipsec is running and tunne's waiting for other end to con established - tunnel is up nelated - tunnel is up establaneu - tonna - , deleted - tunnel is down -tonned - iosec is not running or tunnel is not enabled date Firmware ttings Backup boot fault Setting ial Port NMF GRE Tunnel (PSec Tunnel Logout
- Click Start button on Internet Protocol Security page to initiate IPSEC tunnel.

Figure 85 – IPSec start/stop page for GWR Router 1

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

• 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.



| Geneko | GWR ROUTER - | CONFIGURATION CONSOLE | | |
|--|-----------------------|---|--------------------------------------|-------------|
| Status | Network | | | |
| General Network Information WAN Information Settings | O Obtain an IP addres | as automatically using DHCP | | |
| Network | Ose the following IP | address: | | |
| WAN Settings | IP Address | 192.166.10.1 | | |
| Routing Dynamic Bouting Protocol | Subnet Mask | 255.255.255.0 | | |
| RIP | Local DNS | 195.78.6.36 | | |
| VPN Settings | | | | Delead Save |
| IPSec | | | | Reload Save |
| IP Filtering | | | | |
| Maintenance | | | | |
| Device Identity Settings | | | | |
| Date/Time Settings | | | | |
| Update Firmware | | | | |
| Settings Backup | | | | |
| Reboot | | | | |
| Default Settings | | | | |
| Serial Port | | | | |
| SNMP | | | | |
| Logs | | | | |
| Wizards | | | | |
| Internet Access | | | | |
| IPSec Tunnel | | | | |
| Logout | | | | |
| | | Capyright © 2008 Geneko. A http://www.qene | l rights reserved. :o.r <u>s/</u> | |

Figure 86 - 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: IP Only
 - IP Address: 172.29.8.5
 - 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: IP
 - IP Address: 10.0.10.1
- IPSec Setup
 - Keying Mode: IKE with Preshared key
 - Phase 1 DH group: Group 1
 - Phase 1 Encryption: DES
 - Phase 1 Authentication: MD5
 - Phase 1 SA Life Time: 28800
 - Perfect Forward Secrecy: true
 - Phase 2 DH group: Group 1
 - Phase 2 Encryption: DES
 - Phase 2 Authentication: MD5

- Phase 2 SA Life Time: 3600
- Preshared Key: 1234567890
- Advanced
 - Aggressive Mode: true
 - Compress(Support IP Payload Compression Protocol(IPComp)): false
 - Dead Peer Detection(DPD): false
 - NAT Traversal: true
 - Press *Save* to accept the changes.

| Device 2 Device Tunne | A |
|---|-------------------------|
| Add New Tunnel | |
| Tunnel Number Tunnel Name Enable | 2 test |
| Local Group Setup | |
| Local Security Gateway Type IP Address | IP Only V 172.29.8.5 |
| 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 | IP V 10.0.10.1 |

Figure 87 - IPSEC configuration page I for GWR Router 2

| IPSec Setup | |
|---|---|
| Keying Mode Phase 1 DH Group Phase 1 Encryption Phase 1 Authentication | IKE with Preshared key V Group1 V DES V |
| Phase 1 SA Life Time | 28800 seconds |
| Perfect Forward Secrecy | |
| Phase 2 DH Group Phase 2 Encryption Phase 2 Authentication Phase 2 SA Life Time Preshared Key | Group1 DES MD5 Group3600 seconds 1234567890 |
| Advanced | |
| Aggressive Mode Compress (Support IP P Dead Peer Deection (DP NAT Traversal | ayload Compression Protocol (IPComp)) D) sec |
| | Back Reload Save |

Figure 88 - IPSec configuration page II for GWR Router 2



-

🕞 сепеко GWR ROUTER - CONFIGURATION CONSOL twork Informa AN Information Summary Tunnels Used 1 nas rk Tunnels Avaible 5 Server Settings Add New Tunnel ng Iic Routing Protocol VPN Settings No. Name Enabled Status Enc/Auth/Grp Advanced Setup Local Group Remote Group Remote Gateway Action no stopped Ph1: DES/MD5/1 Ph2: DES/MD5/1 2 test A/N 10.0.10.1 192.168.10.1 172.29.8.5 Delete Edit IP Filtering Sucing the MTU size on the clent side, can help eliminate some connectiv commended MTU size on clent side 1300 pres Marthan block to pre-check. PDS-c turnels' status statted - panc in running and tunnel's waiting for other end to connect established - turnel is down dieted - turnel is down stopped - ipace in or turning or turnel is not enabled nectivity problems occurring at the protocol level Start Stop Refresh ninistrator Password ice Identity Settings e/Time Settings odate Firmware ettings Backup eboot fault Settings rial Port SNMF GRE Tunnel (PSec Tunnel Copyright © 2008 Geneko. All rights reserved. http://www.geneko.rs/

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

Figure 89 - 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 90* 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 90 - IPSec tunnel between GWR Router and Cisco Router

The GWR Routers requirements:

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

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

The GWR Router configuration:

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



| | GWR ROUTER - | CONFIGURATION CONSOLE | | |
|-------------------------|----------------------|-----------------------------------|---------------|-------------|
| | Network | | | |
| Conorol | Network | | | |
| Network Information | | | | |
| WAN Information | O Obtain an IB addre | on automatically using DUCR | | |
| tings | | as automatically using brick | | |
| Network | Use the following If | address: | | |
| OHCP Server | IP Address | 10.0.10.1 | | |
| WAN Settings | Subnet Mask | 255.255.255.0 | | |
| Noting | 1.010 | 105 70 0 20 | | |
| RIP | LOCAL DIVE | 195.78.6.36 | | |
| PN Settings | | | | |
| GRE | | | | Reload Save |
| IPSec | | | | |
| tenance | | | | |
| dministrator Password | | | | |
| evice Identity Settings | | | | |
| ate/Time Settings | | | | |
| agnostics | | | | |
| odate Firmware | | | | |
| ettings Backup | | | | |
| fault Settings | | | | |
| gement | | | | |
| erial Port | | | | |
| IMP | | | | |
| gs | | | | |
| rds | | | | |
| ternet Access | | | | |
| E Tunnel | | | | |
| Sec runner | | | | |
| but | | | | |
| | | Copyright © 2008 Geneko. All righ | its reserved. | |
| | | http://www.geneko.rs | 1 | |
| | | | | |

Figure 91 - Network configuration page for GWR Router

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

•

- Tunnel Name: test
- Enable: true
- Local Group Setup
 - Local Security Gateway Type: IP Only
 - IP Address: 172.30.147.96
 - Local Security Group Type: Subnet
 - IP Address: 192.168.10.0
 - Subnet Mask: 255.255.255.0
- Remote Group Setup
 - Remote Security Gateway Type: IP Only
 - IP Address: 150.160.170.1
 - Remote Security Group Type: IP
 - IP Address: 10.10.10.0
 - Subnet Mask: 255.255.255.0
- IPSec Setup
 - Keying Mode: IKE with Preshared key
 - Phase 1 DH group: Group 2
 - Phase 1 Encryption: 3DES
 - Phase 1 Authentication: SHA1
 - Phase 1 SA Life Time: 28800
 - Perfect Forward Secrecy: true
 - Phase 2 DH group: Group 2

- Phase 2 Encryption: 3DES
- Phase 2 Authentication: SHA1
- Phase 2 SA Life Time: 3600
 - Preshared Key: 1234567890
- Advanced
 - Aggressive Mode: true
 - Compress(Support IP Payload Compression Protocol(IPComp)): false
 - Dead Peer Detection(DPD): false
 - NAT Traversal: true
 - Press *Save* to accept the changes.
 - -

| Device 2 Device Tunne | 1 |
|--|------------------------------------|
| Add New Tunnel | |
| Tunnel Number Tunnel Name Enable | 2 test |
| Local Group Setup | |
| Local Security Gateway Type IP Address | IP Only V 172.30.147.96 |
| Local Security Group Type IP Address Subnet Mask | Subnet 192.168.10.0 255.255.255.0 |
| Remote Group Setup | |
| Remote Security Gateway Type IP Address | IP Only V 150.160.170.1 |
| Remote Security Group Type IP Address | Subnet |
| Subnet Mask | 255.255.255.0 |

Figure 92 - IPSEC configuration page I for GWR Router



| IPSec Setup | |
|--|---|
| Keying Mode Phase 1 DH Group Phase 1 Encryption Phase 1 Authentication Phase 1 SA Life Time Perfect Forward Secrecy | IKE with Preshared key Group2 3DES SHA1 28800 seconds |
| Phase 2 DH Group Phase 2 Encryption Phase 2 Authentication Phase 2 SA Life Time Preshared Key | Group2 V 3DES V SHA1 V 3600 seconds 1234567890 |
| Advanced | |
| Aggressive Mode Compress (Support IP F Dead Peer Deection (DP NAT Traversal | ayload Compression Protocol (IPComp)) D)sec |
| | Back Reload Save |

Figure 93 - IPSec configuration page II for GWR Router

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

| | GWR ROUT | | | IFIGUR) | | CONSOLE | | | | | | |
|--|---|--|---|--|---------------------------------------|--|---------------------------|--|---|----------------|-----------------------|---------|
| Status General Network Information | Internet Proto | ocol | Secu | rity | | | | | | | | |
| WAN Information Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol | Tunnels Used Tunnels Avaible | el | | | 1 5 | | | | | | | |
| RIP VPN Settings GRE IPSec | | No. 2 | Name test | Enabled yes | Status started | Enc/Auth/Grp Ph1: 3DES/SHA1/2 Ph2: 3DES/SHA1/2 | Advanced Setup | Local Group 192.168.10.0 255.255.255.0 | Remote Group 10.10.10.0 255.255.255.0 | Remote Gateway | Action Delete Edit | |
| IP Filtering Maintenance Administrator Password Device Identity Settings Data/Time Settings Diagnostics Update Firmware Settings Backup Reboot Default Settings Management Serial Port SIMP Logs Wizards | * Reducing the MTU size ** Recommonded MTU * *** Press Refract button **** Trans Refract button established - turnel id detted - pace is in stopped - pace is n | on the ize on iption: ining a is up lown ot runn | client sid check IP and tunn- ning or tr | Je, can help e e 1300 Sec tunnels' sec waiting fo | liminate sor status r other end | ne connectivity problems (| securring at the protocol | level | <u>.</u> | Start | Stop | Refresh |
| Internet Access GRE Tunnel IPSec Tunnel Logout | | | | | C | opyright © 2008 Geneko | . All rights reserved. | | | | | |

Figure 94 - IPSec start/stop page for GWR Router

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



The Cisco Router configuration:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Cisco-Router
boot-start-marker
boot-end-marker
1
no aaa new-model
no ip domain lookup
!--- Keyring that defines wildcard pre-shared key.
crypto keyring remote pre-shared-key address 0.0.0.0 0.0.0.0 key 1234567890
!--- ISAKMP policy
crypto isakmp policy 10
 encr 3des
  authentication pre-share
  group 2
  Íifetime 28800
!
.
!--- Profile for LAN-to-LAN connection, that references
!--- the wildcard pre-shared key and a wildcard identity
crypto isakmp profile L2L
   description LAN to LAN vpn connection
   keyring remote
  match identity address 0.0.0.0
crypto ipsec transform-set testGWR esp-3des esp-sha-hmac
!--- Instances of the dynamic crypto map
!--- reference previous IPsec profile.
crypto dynamic-map dynGWR 5
 set transform-set testGWR
 set isakmp-profile L2L
!--- Crypto-map only references instances of the previous dynamic crypto map.
crypto map GWR 10 ipsec-isakmp dynamic dynGWR
interface FastEthernet0/0
description WAN INTERFACE
 ip address 150.160.170.1 255.255.255.252
 ip nat outside
no ip route-cache
no ip mroute-cache
duplex auto
speed auto
 crypto map GWR
interface FastEthernet0/1
description LAN INTERFACE
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
ip route 0.0.0.0 0.0.0.0 150.160.170.2
```

```
ip http server
no ip http secure-server
ip nat inside source list nat_list interface FastEthernet0/0 overload
ip access-list extended nat_list
                                  192.168.10.0 0.0.0.255
deny
      ip 10.10.10.0 0.0.0.255
permit ip 10.10.10.0 0.0.0.255
                                  any
access-list 23 permit any
line con 0
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
 login local
transport input telnet ssh
line vty 5 15
access-class 23 in
privilege level 15
 login local
transport input telnet ssh
I
end
```

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

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



IPSec Tunnel configuration between GWR Router and Juniper SSG firewall

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. On the diagram below *Figure 95* 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 95 - IPSec tunnel between GWR Router and Cisco Router

The GWR Routers requirements:

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

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

The GWR Router configuration:

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



| <u> </u> | | | | |
|--------------------------|------------------------|------------------------------------|-------------|-------------|
| 🕞 сепеко | GWR ROUTER - | CONFIGURATION CONSOLE | | |
| HARDWARE | | | | |
| | | | | |
| Status | Network | | | |
| General | | | | |
| Network Information | | | | |
| WAN Information | O Obtain an IP addre | ss automatically using DHCP | | |
| Settings | I use the following TP | address: | | |
| Network | | 10.0.10.1 | | |
| WAN Settings | IP Address | 10.0.10.1 | | |
| Routing | Subnet Mask | 255.255.255.0 | | |
| Dynamic Routing Protocol | Local DNS | 195,78.6.36 | | |
| RIP | | | | |
| VPN Settings | | | | Delead Save |
| IPSec | | | | Reidad Save |
| IP Filtering | | | | |
| Maintenance | | | | |
| Administrator Password | | | | |
| Device Identity Settings | | | | |
| Date/Time Settings | | | | |
| Update Firmware | | | | |
| Settings Backup | | | | |
| Reboot | | | | |
| Default Settings | | | | |
| Management | | | | |
| Senal Port | | | | |
| Logs | | | | |
| Wizards | | | | |
| Internet Access | | | | |
| GRE Tunnel | | | | |
| IPSec Tunnel | | | | |
| Logout | | | | |
| | | Capyright © 2008 Geneko, All right | s reserved. | |
| | | http://www.geneko.rs/ | | |
| | | | | |

Figure 96 - Network configuration page for GWR Router

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

•

- Tunnel Name: test
- Enable: true
- Local Group Setup
 - Local Security Gateway Type: IP Only
 - IP Address: 172.30.147.96
 - Local Security Group Type: Subnet
 - IP Address: 192.168.10.0
 - Subnet Mask: 255.255.255.0
- Remote Group Setup
 - Remote Security Gateway Type: IP Only
 - IP Address: 150.160.170.1
 - Remote Security Group Type: IP
 - IP Address: 10.10.10.0
 - Subnet Mask: 255.255.255.0
- IPSec Setup
 - Keying Mode: IKE with Preshared key
 - Phase 1 DH group: Group 2
 - Phase 1 Encryption: 3DES
 - Phase 1 Authentication: SHA1
 - Phase 1 SA Life Time: 28800
 - Perfect Forward Secrecy: true
 - Phase 2 DH group: Group 2

- Phase 2 Encryption: 3DES
- Phase 2 Authentication: SHA1
- Phase 2 SA Life Time: 3600
- Preshared Key: 1234567890
- Advanced
 - Aggressive Mode: true
 - Compress(Support IP Payload Compression Protocol(IPComp)): false
 - Dead Peer Detection(DPD): false
 - NAT Traversal: true
 - Press *Save* to accept the changes.

| Device 2 Device Tunne | el |
|--|---------------|
| Add New Tunnel | |
| Tunnel Number Tunnel Name Enable | 2 test |
| Local Group Setup | |
| Local Security Gateway Type | IP Only 💌 |
| IP Address | 172.30.147.96 |
| | |
| Local Security Group Type | Subnet 🚩 |
| IP Address | 192.168.10.0 |
| Subnet Mask | 255.255.255.0 |
| Remote Group Setup | |
| Remote Security Gateway Type | IP Only 💌 |
| IP Address | 150.160.170.1 |
| | |
| Remote Security Group Type | Subnet 💌 |
| IP Address | 10.10.10.0 |
| Subnet Mask | 255.255.255.0 |

Figure 97 - IPSEC configuration page I for GWR Router



| IPSec Setup | |
|--|---|
| Keying Mode Phase 1 DH Group Phase 1 Encryption Phase 1 Authentication Phase 1 SA Life Time Perfect Forward Secrecy | IKE with Preshared key Group2 3DES SHA1 28800 seconds |
| Phase 2 DH Group Phase 2 Encryption Phase 2 Authentication Phase 2 SA Life Time Preshared Key | Group2 V 3DES V SHA1 V 3600 seconds 1234567890 |
| Advanced | |
| Aggressive Mode Compress (Support IP P Dead Peer Deection (DP NAT Traversal | ayload Compression Protocol (IPComp)) D)sec |
| | Back Reload Save |

Figure 98 - IPSec configuration page II for GWR Router

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

| | GWR ROUTE | | CON | IFIGUR | | CONSOLE | | | | | | |
|---|--|---|---|---|---|--|-------------------------------------|-------------------------------|-----------------------------|----------------|-------------|---------|
| Status General | Internet Proto | ocol | Secu | rity | | | | | | | | |
| WAN Information | Summary | | | | | | | | | | | |
| Settings Network DHCP Server WAN Settings Routing Dynamic Routing Protocol | Tunnels Used Tunnels Avaible Add New Tunne | el | | | 1 5 | | | | | | | |
| RIP VDN Cattings | 1 | No | Name | Enabled | Ctatus | Enclauth/Con | Advanced Cetur | Local Crown | Domoto Crown | Domoto Catoway | Action | |
| GRE IPSec | | 2 | test | yes | started | Ph1: 3DES/SHA1/2 Ph2: 3DES/SHA1/2 | A/N | 192.168.10.0 255.255.255.0 | 10.10.10.0 255.255.255.0 | 150.160.170.1 | Delete Edit | |
| Maintenance Administrator Password Device Identity Settings Data/Time Settings Diagnostics Update Firmware Settings Backup Reboot Default Settings Management Serial Port SIMIP Logs Weards Internet Access GRE Tunnel | Reducing the MTU law ** Recommended MTU is *** Press Refrach button **** Tunnel situu descri tatted - ipsei tun un establiched - tunnel is d nopped - ipsei tin no | on the ze on ito re- ption: ning a is up own own ot runn | client sid check IP and tunn ning or t | de, can help + 1300 Sec tunnels' set waiting fo | eliminate sor status or other end mabled | ne connectivity problems (| courring at the protocol | level | | Start | Stop | Refresh |
| Logout | | | | | | | | | | | | |
| | | | | | C | opyright © 2008 Geneka <u>http://www.qe</u> | . All rights reserved. eneko.rs/ | | | | | |

Figure 99 - IPSec start/stop page for GWR Router

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



Help Logout

The Juniper SSG firewall configuration:

Step1 - Create New Tunnel Interface

• Click Interfaces on Network Tab.

| Juniper * | List ALL(14) Interfaces | | | | | | New Tunnel IF |
|---|-------------------------|----------------|---------|--------|-------|----------|---------------|
| SSG-140 | Name | IP/Netmask | Zone | Туре | Link | PPPoE | Configure |
| | ethernet0/0 | 10.0.250/24 | Trust | Layer3 | Up | - | Edit |
| | ethernet0/1 | | DMZ | Layer3 | Up | - | Edit |
| uration | ethernet0/2 | | Untrust | Layer3 | Up | 2 | Edit |
| <u>k</u> | ethernet0/3 | 10.0.10.254/24 | Trust | Layer3 | Up | - | Edit |
| ding | ethernet0/4 | 0.0.0/0 | Null | Unused | Down | 82 | Edit |
| IS | ethernet0/5 | 0.0.0/0 | Null | Unused | Down | - | Edit |
| ies | ethernet0/6 | 0.0.0/0 | Null | Unused | Down | 12 | Edit |
| rfaces | ethernet0/7 | 0.0.0/0 | Null | Unused | Down | - | Edit |
| <u>CP</u> | ethernet0/8 | 0.0.0/0 | Null | Unused | Down | 12 | Edit |
| ating | ethernet0/9 | 0.0.0/0 | Null | Unused | Down | - | Edit |
| RP | tunnel.1 | unnumbered | Untrust | Tunnel | Ready | | Edit |
| p | tunnel.2 | unnumbered | Untrust | Tunnel | Ready | 2 | Edit |
| ing | tunnel.3 | unnumbered | Untrust | Tunnel | Ready | <u>_</u> | Edit |
| 5 | vian1 | 0.0.0/0 | VLAN | Layer3 | Down | - | Edit |
| and the second se | <u>.</u> | | | | | | |

Figure 100 - Network Interfaces (list)

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

| | Network > Interfaces > Edit | SSG140RBGE | ? |
|---|--|------------------|--------|
| | Interface: tunnel.3 (IP/Netmask: 0.0.0.0/0) | Back To Interfac | e List |
| | Properties: Basic MIP DIP IGMP NHTB Tunnel | | |
| | Tunnel Interface Name tunnel.3 Zone (VR) Untrust (trust-vr) | | |
| Home <u>Configuration</u> <u>Network</u> <u>Binding</u> UNS | O Fixed IP IP Address / Netmask | | _ |
| Zones Interfaces | Unnumbered Interface etherne@/2 (trust-vr) v | | |
| <u>DHCP</u> <u>802.1X</u> | Maximum Transfer Unit(MTU) Admin MTU 1500 Bytes (Operating MTU: 1500; Default MTU: 1500) | | |
| <u>Kouting</u> <u>NSRP</u> PPP | DNS Proxy | | _ |
| * <u>Screening</u> Policies | Traffic Bandwidth Egress Maximum Bandwidth G Kbps | | |
| MCast Policies | Ingress Maximum Bandwidth 0 Kbps | | |
| * Reports * Wizards | OK Apply Cascal | | |
| Logout | | | |
| Toggle Menu | | | |

Figure 101 - Network Interfaces (edit)



Step 2 - Create New VPN IPSEC tunnel

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

| | VPNs > AutoKey Advanced > Gat | teway | | | | SSG140R | BGE | ? |
|---|-------------------------------|-----------|-----------------------|---------------|----------------|---------|----------|-----|
| | List 20 v per page | | | | | | .(| New |
| | Name | Peer Type | Address/ID/User Group | Local ID | Security Level | c | onfigure | |
| | Dialup GW | Dialup | Dialup Group | | Custom | Edit | Xauth | - |
| Home | GW-VPNtoUSSD | Static | | | Custom | Edit | Xauth | - |
| + Configuration | TestGWR | Dynamic | 172.27.76.80 | 212.62.38.106 | Custom | Edit | Xauth | - |
| Network | VPNtoTehnika | Static | | 5 <u>2</u> 8 | Custom | Edit | Xauth | 1 |
| DNS Zones Interfaces DHCP 802.1X Routing NSRP 9PD Policies MCast Policies VPNs AutoKey IKE AutoKey IKE AutoKey Advanced Gateway P1 Proposal P2 Proposal Xath Settings VPN Groups Manual Key L2TP Monitor Status Objects Reports Wizards Jagest | | | | | | | | |

Figure 102 - AutoKey Advanced Gateway

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



| VPNs > AutoKey Advanced > O | Gateway > Edit | SSG140RBGE | ? |
|--|---|------------|---|
| M Juniper [®] | | | |
| SSG-140 Bone. Configuration. Network. Screening. Policies. MCast Policies. MCast Policies. AutoKey IKE. AutoKey KE. AutoKey Advanced P2 Proposal P2 Proposal VPN Groups Manual Key Manual Key Manual Key | Gateway Name TexOWR Security Level Standard Compatible Basic Custom IP Address/Hostname Peer ID 17:20:147:56 User None V Group None V Preshared Key | | |
| Monitor Status Objects Directs Reports Mizards Logout | | | |

Figure 103 - Gateway parameters

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



| | VPNs > AutoKey Advanced > Gateway > Edit | SSG140RBGE | ? |
|--|--|------------|---|
| | | | |
| SSG-140 | Security Level Predefined O Standard O Compatible O Basic User Defined O Custom Phase I Proposal pre-g2-3des-sha V None V None V | | |
| DNS | Mode (Initiator) 🔿 Main (ID Protection) 📀 Aggressive | | |
| <u>Zones</u> <u>Interfaces</u> <u>DHCP</u> | Enable NAT-Traversal UDP Checksum Keepalive Frequency Seconds (0~300 Sec) | | |
| * <u>Routing</u> * <u>NSRP</u> | Peer Status Detection Hello Generation Heartbeat Hello Seconds (1~3600, 0: disable) Reconnect Seconds (60+999 Sec) | | |
| <u>PPP</u> <u>Screening</u> <u>Policies</u> MCast Policies | Threshold 5 OppO Interval 0 Seconds (3~28800, 0; disable) Retry 5 (1~128) Alvars Send | | |
| AutoKey IKE AutoKey Advanced Gateway Di Procent | Preferred Certificate(optional) Local Cert None v Peer CA None v Peer Type X509-SIG v | | |
| P1 Proposal P2 Proposal XAuth Settings VPN Groups Manual Key ELTP | Use Distinguished Name for Peer ID CN OU Organization Location State | | |
| <u>Objects</u> <u>Reports</u> | Country E-mail Container | | |
| Toggle Menu | Return Cancel | | |

Figure 104 - Gateway advanced parameters

Step 3 - Create AutoKey IKE

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



| | VPNs > AutoKey IKE | | | | SS | G140RBGE | ? |
|--------------------|--------------------|--------------|----------|---------|------|-----------|-----|
| | List 20 yer page | | | | | | |
| (A) luniner | | | | | | (| New |
| A ZNETWORKS | | | | | | | |
| | Name | Gateway | Security | Monitor | | Configure | |
| | DialupVPN | Dialup GW | Custom | Off | Edit | - | |
| Home | LinkToTehnika | VPNtoTehnika | Custom | On | Edit | Remove | |
| + Configuration | TestGWR | TestGWR | Custom | Off | Edit | Remove | |
| Network | VPNtoUSSD | GW-VPNtoUSSD | Custom | Off | Edit | Remove | |
| Binding | | | | | | | |
| ± <u>DNS</u> | | | | | | | |
| Interfaces | | | | | | | |
| DHCP | | | | | | | |
| = 802.1X | | | | | | | |
| Routing | | | | | | | |
| • <u>NSRP</u> | | | | | | | |
| <u> </u> | | | | | | | |
| * <u>Screening</u> | | | | | | | |
| Policies | | | | | | | |
| NCast Policies | | | | | | | |
| AutoKey IKE | | | | | | | |
| - AutoKey Advanced | | | | | | | |
| Gateway | | | | | | | |
| P1 Proposal | | | | | | | |
| P2 Proposal | | | | | | | |
| XAuth Settings | | | | | | | |
| VPN Groups | | | | | | | |
| + L 2TD | | | | | | | |
| Monitor Status | | | | | | | |
| + Objects | | | | | | | |
| * Reports | | | | | | | |
| <u>Wizards</u> | | | | | | | |
| + Help | | | | | | | |
| Logout | | | | | | | |
| Toggle Monn | | | | | | | |
| Toggle Menu | | | | | | | |

Figure 105 - AutoKey IKE

AutoKey IKE parameters are:

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



| VPNs > AutoKey IKE > Edit | SSG140RBGE |
|---|------------------|
| | |
| Juniper | |
| | |
| SSG-140 Security Level O Standard O Compatible O Basic O Custom | |
| Home Remote Gateway () Predefined TestGWR | v |
| Configuration | |
| <u>Network</u> Gateway Name | |
| Binding Type Static IP | Address/Hostname |
| Zones Opjamic IP | User None Y |
| Interfaces O Dialup Group | Group None |
| DHCP • 802 1X Local ID (optional) | |
| Routing Preshared Key Use | s Seed |
| NSRP Security Level Standard Cor | atible O Basic |
| Outgoing Interface ethernetU/U Screening | |
| Policies OK Cancel Advanced | |
| <u>MCast Policies</u> | |
| AutoKey IKE | |
| AutoKey Advanced | |
| Gateway D1 Decement | |
| - P2 Proposal | |
| XAuth Settings | |
| - <u>VPN Groups</u> | |
| | |
| <u>Monitor Status</u> | |
| Delects | |
| Wizards | |
| • Help | |
| Logant | |
| | |

Figure 106 - AutoKey IKE parameters

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



GWR Series Router

| | VPNs > AutoKey IKE > Edit | SSG140RBGE | ? |
|--|--|------------|---|
| | | | |
| | Security Level Predefined O Standard O Compatible O Basic User Defined O Custom Predefined O Custom Predef | | |
| <u></u> | g2-esp-3des-sha v None v | | |
| * Screening | None None | | |
| <u>Policies</u> <u>MCast Policies</u> | Replay Protection Transport Mode (For L2TP-over-IPSec only) | | |
| AutoKey IKE AutoKey Advanced | Bind to O None O Tunnel Interface Untrust-Tunnel Zone Untrust-Tun V | | |
| P1 Proposal P2 Proposal XAuth Settings | Proxy-ID Image: Constraint of the second secon | | |
| Manual Key L2TP | VPN Group None Veight 0 | | |
| Monitor Status | VPN Monitor Source Interface default | | |
| * <u>Reports</u> | Destination IP debut | | |
| <u>Wizards</u> <u>Help</u> | Rekey | | |
| Logout | Return Cancel | | |
| Toggle Menu | | | |

Figure 107 - AutoKey IKE advanced parameters

Step 4 - Routing

•

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



| Network | x > Routing > Routing Entries > Configurati | on | | SSG140RBGE | ? |
|----------------------------|---|----------------|-------------------|------------|---|
| | | | | | |
| (A) luniper | | | | | |
| NETWORKS | | | | | |
| | Virtual Router Name t | rust-vr | | | |
| | IP Address/Netmask | 192.168.10.0 | / 0 | | |
| Home | | | | | - |
| Configuration_ | Next Hop | Virtual Router | untrust-vr 😒 | | |
| <u>Network</u> | | Gateway | | | |
| DNS |] | T | nterface tunnel 3 | | |
| Zones | | Gateway IP | Address 0.0.0 | | |
| Interfaces | | Per | rmanent | | |
| DHCP | | | Tag 0 | | |
| Bouting | Mataia | . 1 | | | _ |
| Destination | metric | | | | |
| Source | Preference | 20 | | | |
| Source Interface | | | OK Crust | | |
| MCast Routing | | L | OK Care | | |
| Virtual Routers | | | | | |
| U NSRP | | | | | |
| • ppp | | | | | |
| * Screening | | | | | |
| Policies MCast Policies | | | | | |
| - VPNs | | | | | |
| AutoKey IKE | | | | | |
| AutoKey Advanced | | | | | |
| <u>Gateway</u> | | | | | |
| P2 Proposal | | | | | |
| XAuth Settings | | | | | |
| <u>VPN Groups</u> | | | | | |
| Manual Key | | | | | |
| Monitor Status | | | | | |
| + Objects | | | | | |
| Reports | | | | | |
| < > | | | | | |

Figure 108 - Routing parameters

Step 4 - Policies

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



| | Policies (From Untrust To Trust) | SSG140RBGE | ? |
|-----------------------|----------------------------------|---|---|
| | | | |
| (No luniner* | | | |
| A ANETWORKS | | | |
| SSG-140 | Name (optional) | | |
| <u> </u> | | O New Address | |
| Home | Source Address | ⊙ Address Book Entry 192.168.10.0/24 V Multiple | |
| <u>Configuration</u> | | O New Address / | |
| Binding | Destination Address | O Address Book Entry 10.0.0.0/24 V Multiple | |
| DNS | Service | ANY V Multiple | |
| Zones | Application | None | |
| Interfaces | | | |
| + 802.1X | | WEB Filtering | |
| Routing | Action | | |
| Destination | Autoine De Cla | Name and A | |
| Source Source | Antivirus Profile | | |
| MCast Routing | Antispam enable | | |
| . <u>₽BR</u> | Tunnel | VPN None 💌 | |
| Virtual Routers | | Modify matching bidirectional VPN policy | |
| + NSRP | | L2TP None Y | |
| * Screening | Logging | ✓ at Session Beginning ✓ | |
| Policies | Position at Top | | |
| <u>MCast Policies</u> | | | |
| AutoKey IKE | | OK Cancel Advanced | |
| AutoKey Advanced | | | |
| Gateway | | | |
| P1 Proposal | | | |
| XAuth Settings | | | |
| VPN Groups | | | |
| Manual Key | | | |
| Monitor Status | | | |
| Objects | | | |
| ± Reports ⊻ | | | |

Figure 109 - Policies from untrust to trust zone

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



| | Policies (From Trust To Untrust) | | SSG140RBGE | ? |
|------------------------|----------------------------------|--|------------|---|
| (| | | | |
| (A) luninor | | | | |
| NETWORKS | | | | |
| | Name (optional) | | | |
| | | | | |
| Home | Source Address | ⊙ Address Book Entry 10.0.0/24 ✓ Multiple | | |
| * <u>Configuration</u> | | | | |
| Network | Destination Address | Address Book Entry 192 168 10 0/24 Multiple | | |
| Binding + DNS | | | | |
| Zones | Service | Aivi | | |
| Interfaces | Application | None Y | | |
| DHCP | | | | _ |
| E Routing | | WEB Filtering | | |
| Destination | Action | Permit V Deep Inspection | | |
| Source | Antivirus Profile | None v | | |
| Source Interface | Antispam enable | | | |
| MCast Routing | Tunnel | VPN None | | |
| Virtual Routers | | Modify matching bidirectional VPN policy | | |
| • NSRP | | | | |
| <u>□</u> <u>PPP</u> | Longing | | | |
| Screening | Logging | | | |
| MCast Policies | Position at Top | | | |
| - VPNs | | OK Crevel Advanced | | |
| AutoKey IKE | | | | |
| AutoKey Advanced | | | | |
| P1 Proposal | | | | |
| P2 Proposal | | | | |
| XAuth Settings | | | | |
| VPN Groups | | | | |
| ± L2TP | | | | |
| Monitor Status | | | | |
| Objects | | | | |
| * Reports | | | | |

Figure 110 - Policies from trust to untrust zone



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.



B. Mobile operator GPRS settings

| Australia | | | | |
|----------------------------------|-----------------------|-----------------|-----------------|--|
| Operator | GPRS APN | Username | Password | Optional Settings |
| Optus | internet | [blank] | [blank] | DNS: 202.139.83.3, 192.65.91.129 |
| Telstra | telstra.internet | [blank] | [blank] | DNS: 139.130.4.4, 203.50.170.2 |
| Three | 3netaccess | а | а | DNS: 202.124.68.130, 202.124.76.66 |
| Vodafone | vfinternet.au | [blank] | [blank] | DNS: 192.189.54.33, 210.80.58.3 |
| Austria | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Connect Austria ONE OneNet | web.one.at | [user specific] | [user specific] | DNS: 194.24.128.100, 194.24.128.102 |
| Max Online | gprsinternet | GPRS | [blank] | DNS: 213.162.64.1, 213.162.64.2 |
| Max Online Business | business.gprsinternet | GPRS | [blank] | DNS: 213.162.64.1, 213.162.64.2 |
| Max Online Metro | gprsmetro | GPRS | [blank] | DNS: 213.162.64.1, 213.162.64.2 |
| Mobilkom A1 | A1.net | gprs@a1plus.at | [blank] | DNS: 194.48.124.200, 194.48.139.254 |
| tele.ring | web | web@telering.at | web | DNS: 212.95.31.11, 212.95.31.35 |
| Belgium | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Mobistar | web.pro.be | mobistar | mobistar | DNS: 212.65.63.10, 212.65.63.145 |
| Proximus | internet.proximus.be | [blank] | [blank] | DNS: 195.238.2.21, 195.238.2.22 |
| Orange / BASE | orangeinternet | [blank] | [blank] | - |
| Brasil | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Claro | claro.com.br | claro | claro | - |
| TIM | tim.br | tim | tim | - |
| Canada | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Rogers AT&T (Internet) | internet.com | wapuser1 | wap | - |
| Rogers AT&T (VPN) | vpn.com | wapuser1 | wap | - |



| Fido Microcell | internet.fido.ca | fido | fido | DNS: 204.92.15.211 |
|---------------------------|-----------------------|----------|----------|--|
| China | | | • | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| China Mobile | cmnet | [blank] | [blank] | - |
| China Unicom | [none] | [blank] | [blank] | DNS: 10.0.2.100 |
| Croatia | | | • | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| VIPNET Start | gprs0.vipnet.hr | 38591 | 38591 | - |
| VIPNET Pro | gprs5.vipnet.hr | 38591 | 38591 | - |
| Czech Republic | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Cesky Mobil (contract) | internet | [blank] | [blank] | DNS: 212.67.64.2 |
| Cesky Mobil (prepaid) | cinternet | [blank] | [blank] | DNS: 212.67.64.2 |
| Eurotel (contract) | internet | [blank] | [blank] | DNS: 160.218.10.200, 160.218.43.200 |
| Eurotel Go | gointernet | [blank] | [blank] | DNS: 160.218.10.201, 194.228.2.1 |
| Oscar (contract) | internet | [blank] | [blank] | DNS: 217.77.161.130, 217.77.161.131 |
| Oscar (Oskarta) | ointernet | [blank] | [blank] | DNS: 217.77.161.130, 217.77.161.131 |
| T-Mobile | internet.t-mobile.cz | [blank] | [blank] | DNS: 62.141.0.1, 62.141.0.2 |
| Denmark | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| TDC | internet | [blank] | [blank] | DNS: 193.162.146.9, 193.162.153.31 |
| Sonofon | [blank] | [blank] | [blank] | DNS: 212.88.64.14, 212.88.64.15 |
| Orange DK | web.orange.dk | [blank] | [blank] | DNS: 212.97.206.131, 212.97.206.161 |
| Egypt | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Click Vodafone | internet.vodafone.net | internet | internet | - |
| MobiNil | mobinilweb | [blank] | [blank] | - |
| Estonia | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| EMT | internet.emt.ee | [blank] | [blank] | DNS: 217.71.33.200, 217.71.32.20 |
| RLE | internet | [blank] | [blank] | - |
| Finland | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |



| Dna | internet | [blank] | [blank] | DNS: 217.78.192.78, 217.78.192.22 |
|---|---|--|--|--|
| Radiolinja | internet | [blank] | [blank] | DNS: 213.161.33.200, 193.185.210.10 |
| Sonera | internet | [blank] | [blank] | DNS: 192.89.123.230, 192.89.123.231 |
| France | • | | • | • |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Bouygues | ebouygtel.com | [blank] | [blank] | DNS: 62.201.119.99, 62.201.159.99 |
| Bouygues (B2Bouygtel) | b2bouygtel.com | [blank] | [blank] | DNS: 62.201.119.99 |
| SFR | websfr | [blank] | [blank] | DNS: 172.20.2.10, 194.6.128.4 |
| Orange Pro | orange.fr | orange | orange | DNS: 194.051.003.056, 194.051.003.076 |
| Orange Perso | orange | orange | orange | DNS: 194.051.003.056, 194.051.003.076 |
| Orange MIB | orange-mib | mportail | mib | Proxy: 172.16.2.8:8000 |
| | | | | |
| Germany | | | | |
| <mark>Germany</mark> Operator | GPRS APN | Username | Password | Optional Settings |
| Germany Operator D2 Vodafone | GPRS APN web.vodafone.de | Username [any] | Password [any] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 |
| Germany Operator D2 Vodafone E-Plus | GPRS APN web.vodafone.de internet.eplus.de | Username [any] eplus | Password [any] gprs | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de | Username [any] eplus td1 | Password [any] gprs gprs | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de | Username [any] eplus td1 quam | Password [any] gprs gprs quam | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet | Username [any] eplus td1 quam [blank] | Password [any] gprs gprs quam [blank] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet | Username [any] eplus td1 quam [blank] | Password [any] gprs gprs quam [blank] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece Operator | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet | Username [any] eplus td1 quam [blank] Username | Password [any] gprs gprs quam [blank] Password | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 Optional Settings |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece Operator Telestet | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet GPRS APN gnet.b-online.gr | Username [any] eplus td1 quam [blank] Username your phone number | Password [any] gprs gprs quam [blank] Password 24680 | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 Optional Settings DNS: 212.152.79.19, 212.152.79.20 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece Operator Telestet Vodafone GR | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet GPRS APN gnet.b-online.gr internet.vodafone.gr | Username [any] eplus td1 quam [blank] Username your phone number [blank] | Password [any] gprs gprs quam [blank] Password 24680 [blank] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 Optional Settings DNS: 212.152.79.19, 212.152.79.20 DNS: 213.249.17.10, 213.249.17.11 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece Operator Telestet Vodafone GR Cosmote | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet GPRS APN gnet.b-online.gr internet.vodafone.gr | Username [any] eplus td1 quam [blank] Username your phone number [blank] | Password [any] gprs gprs quam [blank] Password 24680 [blank] [blank] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 Optional Settings DNS: 212.152.79.19, 212.152.79.20 DNS: 213.249.17.10, 213.249.17.11 DNS: 195.167.065.194 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece Operator Telestet Vodafone GR Cosmote Hongkong | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet GPRS APN gnet.b-online.gr internet.vodafone.gr | Username [any] eplus td1 quam [blank] Username your phone number [blank] [blank] | Password [any] gprs gprs quam [blank] Password 24680 [blank] [blank] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 DNS: 212.152.79.19, 212.152.79.20 DNS: 213.249.17.10, 213.249.17.11 DNS: 195.167.065.194 |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece Operator Telestet Vodafone GR Cosmote Hongkong Operator | GPRS APN Web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet GPRS APN gnet.b-online.gr internet.vodafone.gr internet GPRS APN | Username [any] eplus td1 quam [blank] Username your phone number [blank] [blank] | Password [any] [any] gprs gprs quam [blank] Password 24680 [blank] [blank] [blank] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 Optional Settings DNS: 212.152.79.19, 212.152.79.20 DNS: 213.249.17.10, 213.249.17.11 DNS: 195.167.065.194 Optional Settings |
| Germany Operator D2 Vodafone E-Plus D1 T-Mobile Quam O2 (Viag Interkom) Greece Operator Telestet Vodafone GR Cosmote Hongkong Operator CSL | GPRS APN web.vodafone.de internet.eplus.de internet.t-d1.de quam.de internet GPRS APN gnet.b-online.gr internet.vodafone.gr internet GPRS APN hkcsl or internet | Username [any] eplus td1 quam [blank] Username your phone number [blank] [blank] Username | Password [any] [any] gprs gprs quam [blank] Password 24680 [blank] [blank] [blank] [blank] [blank] | Optional Settings DNS: 139.7.30.125, 139.7.30.126 DNS: 212.023.97.2, 212.23.97.3 DNS: 193.254.160.1 - DNS: 193.254.160.1 - DNS: 195.182.096.28, 195.182.96.61 DNS: 212.152.79.19, 212.152.79.20 DNS: 213.249.17.10, 213.249.17.11 DNS: 195.167.065.194 Optional Settings DNS: 10005.194 |


USER MANUAL

| Orange | web.orangehk.com | [blank] | [blank] | - |
|------------------------|--|----------------------------|----------------------------|---|
| People | internet | [blank] | [blank] | - |
| SmarTone | internet | [blank] | [blank] | DNS: 202.140.96.51, 202.140.96.52 |
| Sunday | internet | [blank] | [blank] | - |
| Hungary | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Pannon (contract) | net | [blank] | [blank] | DNS: 193.225.155.254, 194.149.0.157 |
| Pannon (flat rate) | netx | [blank] | [blank] | DNS: 193.225.155.254, 194.149.0.157 |
| Vodafone (prepaid) | vitamax.snet.internet.n et or internet.vodafone.net | [blank] | [blank] | DNS: 80.244.97.30, 80.244.96.1 |
| Vodafone (contract) | standardnet.vodafone. hu or internet.vodafone.net | [blank] | [blank] | DNS: 80.244.97.30, 80.244.96.1 |
| Westel (contract) | internet | wap or user specific | wap or user specific | DNS: 194.176.224.3, 194.176.224.1 |
| India | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| AirTel | airtelgprs.com | [blank] | [blank] | - |
| BPL | bplgprs.com | bplmobile | [blank] | DNS: 202.169.145.34, 202.169.129.40 |
| Orange | portalnmms | [blank] | [blank] | DNS: 10.11.206.51, 10.11.206.50 |
| Indonesia | | | • | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| IM3 | www.indosat-m3.net | gprs | im3 | - |
| Indosat | satelindogprs.com | [blank] | [blank] | DNS: 202.152.162.66, 202.152.162.67 |
| Ireland | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| O2 (contract) | open.internet | gprs | gprs | DNS: 62.40.32.33, 62.40.32.34 |
| O2 (prepaid) | pp.internet | gprs | gprs | DNS: 62.40.32.33, 62.40.32.34 |
| Vodafone | isp.vodafone.ie | vodafone | vodafone | - |
| Israel | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |



| Cellcom | internetg | [blank] | [blank] | - |
|-----------------------|---------------------|----------|----------|---|
| MTC-Vodafone | apn01 | [blank] | [blank] | DNS: 10.10.10.30 |
| Orange | internet | [blank] | [blank] | - |
| Italy | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| BLU Contratto | INTERNET | [blank] | [blank] | DNS: 212.17.192.49, 212.17.192.49 |
| BLU Prepagata | PINTERNET | [blank] | [blank] | DNS: 212.17.192.49, 212.17.192.49 |
| Vodafone Omnitel | web.omnitel.it | [blank] | [blank] | DNS: 194.185.97.134 |
| TIM | uni.tim.it | [blank] | [blank] | DNS: 213.230.155.94, 213.230.130.222 |
| Wind | internet.wind | [blank] | [blank] | DNS: 212.245.255.2 |
| Japan | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| J-Phone (Vodafone) | phone | j@phone | jphone | - |
| Lithuania | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Bite GSM | banga | [blank] | [blank] | DNS: 213.226.131.131, 193.219.32.13 |
| Omnitel Lithuania | gprs.omnitel.net | [blank] | [blank] | DNS: 194.176.32.129, 195.22.175.1 |
| Luxembourg | | | | <u>.</u> |
| Operator | GPRS APN | Username | Password | Optional Settings |
| LUXGSM | web.pt.lu | [blank] | [blank] | DNS: 194.154.192.101, 194.154.192.102 |
| VOXmobile | vox.lu | - | - | - |
| Tango | internet | tango | tango | - |
| Macedonian | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Mobimak | internet | internet | mobimak | - |
| Malaysia | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| DIGI | diginet | [blank] | [blank] | DNS: 203.92.128.131, 203.92.128.132 |
| Maxis | internet.gprs.maxis | [blank] | [blank] | DNS: 202.75.129.101, 10.216.4.21 |
| Timecel | timenet.com.my | [blank] | [blank] | DNS: 203.121.16.85, 203.121.16.120 |
| TM Touch | internet | [blank] | [blank] | DNS: 202.188.0.133 |



| Mexico | | | | |
|-------------------------|--------------------------------|---------------------------|---------------------------|--|
| Operator | GPRS APN | Username | Password | Optional Settings |
| Telcel | internet.itelcel.com | webgprs | webgprs2002 | - |
| Netherlands | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| KPN Mobile | internet | KPN or [blank] | gprs or [blank] | DNS: 62.133.126.28, 62.133.126.29 |
| O2 | internet | [blank] | [blank] | - |
| Telfort | internet | [blank] | [blank] | - |
| T-Mobile | internet or internet-act | t-mobile or [blank] | t-mobile or [blank] | DNS: 193.79.237.39, 193.79.242.39 |
| Vodafone (normal) | web.vodafone.nl | vodafone | vodafone | - |
| Vodafone (business) | office.vodafone.nl | vodafone | vodafone | - |
| New Zeleand | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Vodafone | www.vodafone.net.nz | - | - | - |
| Norway | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Telenor Mobil | internet | [blank] | [blank] | - |
| Netcom | internet.netcom.no | [blank] | [blank] | DNS: 212.45.118.43, 212.45.118.44 |
| Poland | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| ERA | erainternet | erainternet | erainternet | DNS: 213.158.194.1 |
| Idea | www.idea.pl | idea | idea | DNS: 194.9.223.79, 194.204.159.1 |
| Plus GSM / Polkomtel | www.plusgsm.pl | [blank] | [blank] | DNS: 212.2.96.51, 212.2.96.52 |
| Phillipines | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Globe | www.globe.com.ph | globe | globe | DNS: 203.127.225.10, 203.127.225.11 |
| Smart | internet | [blank] | [blank] | DNS: 202.57.96.3, 202.57.96.4 |
| Sun Cellular | minternet | [blank] | [blank] | [blank] |
| Portugal | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Optimus | internet | [blank] | [blank] | DNS: 194.79.69.129 |
| TMN | internet | [blank] | [blank] | DNS: 194.65.3.20, 194.65.3.21 |
| Vodafone | internet.vodafone.pt | [blank] | [blank] | DNS: 212.18.160.133, |



| (Telcel) | | | | 212.18.160.134 |
|----------------------|----------------------------|-----------|-----------|--|
| Russia | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| BeeLine | internet.beeline.ru | beeline | beeline | DNS: 194.190.195.66, 194.190.192.34 |
| Megafon (NWGSM) | internet.nw | [blank] | [blank] | - |
| MTS | internet.mts.ru | mts | mts | DNS: 213.87.0.1, 213.87.1.1 |
| PrimTel | internet.primtel.ru | [blank] | [blank] | - |
| Serbia | | • • | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Mobtel Srbija | internet | mobtel | gprs | DNS: 217.65.192.1 |
| Telekom Srbija | gprsinternet | mts | 064 | DNS: 195.178.38.3 |
| VIP Mobile Srbija | vipmobile | vipmobile | vipmobile | - |
| Singapore | | • | | - - |
| Operator | GPRS APN | Username | Password | Optional Settings |
| M1 | mobilenet or sunsurf | [blank] | [blank] | DNS: 202.79.64.21, 202.79.64.26 |
| SingTel | internet | [blank] | [blank] | DNS: 165.21.100.88, 165.21.83.88 |
| Starhub | shwapint | [blank] | [blank] | DNS: 203.116.1.78, 203.116.254.150 |
| Slovakia | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Eurotel | internet | [blank] | [blank] | - |
| Orange | internet | jusernejm | pasvord | - |
| Slovenia | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Mobitel | internet | [blank] | [blank] | DNS: 193.189.160.11, 193.189.160.12 |
| Si.mobil | internet.si.mobil | [blank] | [blank] | DNS: 80.95.225.230, 80.95.225.231 |
| South Africa | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| MTN | myMTN | | | - |
| Cell-c | internet | Cellcis | Cellcis | - |
| Spain | | | | |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Amena | internet | CLIENTE | AMENA | DNS: 213.143.33.8, 213.143.32.20 |
| Telefonica | movistar.es | movistar | movistar | DNS: 94.179.001.100, |



| 2.67 ettings |
|--|
| 2.67 ettings |
| ettings |
| ettings |
| ettings |
| |
| |
| |
| |
| |
| ettings |
| .128.1, 8.2 |
| .35.35, 5.5 |
| 8.36.34, 6.39 |
| |
| ettings |
| 1.1 |
| 9.199 |
| |
| |
| |
| ettings |
| .255.20, 5.21 |
| 5.33.1 <i>,</i> 4.33 |
| |
| ettings |
| 56.4.1, 4.4 |
| |
| |
| 3.240, 19.4 |
| |
| ettings |
| |
| |
| ett: 1 9.1 9.1 2 5 5 2 5 2 5 2 5 2 5 2 5 2 5 2 53 2 19 19 19 19 19 19 19 19 19 10 10 10 10 10 10 10 10 10 10 10 10 10 |



| (contract) | | | | 193.113.200.200, 193.113.200.201 |
|------------------------------------|---------------------|----------------------------------|-----------|--|
| O2 UK (prepaid) | payandgo.o2.co.uk | payandgo | payandgo | - |
| Orange UK | orangeinternet | [blank] | [blank] | DNS: 158.43.192.1, 158.143.128.1 |
| T-Mobile | general.t-mobile.uk | user | mms | - |
| T-Mobile (One2One) | general.t-mobile.uk | Username | one2one | - |
| Jersey Telecom | pepper | [blank] | [blank] | DNS: 212.9.0.135, 212.9.0.135 |
| Ukraine | | - | | • |
| Operator | GPRS APN | Username | Password | Optional Settings |
| Jeans | www.jeans.ua | - | - | - |
| UMC | www.umc.ua | - | - | - |
| USA | | | | - |
| Operator | GPRS APN | Username | Password | Optional Settings |
| AT&T (VPN) | public | - | - | - |
| AT&T | proxy | - | - | Gateway IP: 10.250.250.250 or blank Port: 9201 or blank |
| Bell Mobility | - | - | - | Gateway IP: 207.236.197.199 Port: 9203 |
| Cellular One | cellular1wap | - | - | Gateway IP: 207.236.197.199 Port: 9203 |
| Cincinnati Bell | wap.gocbw.com | cbw | - | Gateway IP: 216.68.79.199 Port: 9201 |
| Cingular (former AT&T users) | proxy | - | - | Gateway IP: 10.250.250.250 or blank Port: 9201 or blank |
| Cingular (MediaWorks) | WAP.CINGULAR | WAP@ CINGULARGPR S .COM | CINGULAR1 | - |
| Cingular | isp.cingular | ISPDA@CINGU LARGPRS.COM | CINGULAR1 | DNS: 66.209.10.201, 66.209.10.202 |
| Nextel/Telus | - | - | - | - |
| Rogers | internet.com | - | - | - |
| Sprint - CDMA | - | - | - | CDMA and not GPRS settings |



| T-Mobile (T- Zone) | wap.voicestream.com | [blank] or Your T-MOBILE Username | [blank] or Your T-MOBILE Password | - |
|------------------------|-------------------------------|---|---|---|
| T-Mobile (Internet) | internet2.voicestream.c om | [blank] | [blank] | DNS: 216.155.175.105, 216.155.175.106 |
| T-Mobile (VPN) | internet3.voicestream.c om | [blank] | [blank] | DNS: 216.155.175.105, 216.155.175.106 |

