

GlobeSurfer 3G

version 3.15.4 R2H

Reference Manual

Copyright © 2005, Option

All information about Option GlobeSurfer 3G may change without prior notice. Information published in this user guide is accurate at the time of publication. Although all security precautions were taken during the creation of this user guide Option is not liable toward persons or organizations for losses or damages caused either directly or indirectly due to instructions contained in this user guide.

All brands and registered brands are property of their respective owners. Services may be changed, added, or deleted. For the newest firmware version of your Globesurfer 3G, visit www.option.com

Questions and answers regarding the GlobeSurfer 3G can be found on our Support website:

<http://support.option.com/support/faq.php>

Technical questions can be posted after registering through our online Support Web Form:

<http://support.option.com/support/newticket.php>

For registering please go to:

<http://support.option.com/support/register.php>

DOC-UM--12-2005

December, 2005

Contents

Table of Contents	ii
1 Introduction to GlobeSurfer 3G	1
1.1 About This Manual	2
1.2 Basic Setup	3
1.3 Step 1 - Setting up LAN and WAN Connections	3
1.3.1 LAN Connection	3
1.3.2 WAN Connection	4
1.4 Step 2 - PC Network Configuration	4
1.4.1 Windows XP	5
1.4.2 Windows 2000/98/Me	5
1.5 Step 3 - GlobeSurfer 3G Quick Setup	6
1.5.1 UMTS Setup	7
1.5.2 Wireless Setup	8
1.5.2.1 Encryption	8
1.5.3 Firewall Setup	9
1.6 Additional Network Configuration	9
1.7 Adding Computers to Your Network	10
2 GlobeSurfer 3G Management Console	11
2.1 Accessing the GlobeSurfer 3G Management Console	11
2.2 Left Sidebar	12
2.3 UMTS Connection Status	13
2.4 Getting Help	14
2.5 Managing Tables	14
3 SMS Manager	15
3.1 Reading an SMS	15
3.2 Creating an SMS	16
3.2.1 Sent folder	17
3.3 Archiving an SMS	17
3.4 SMS Templates	17
3.5 SMS Settings	18
4 Network Connections	19
4.1 WAN UMTS Connection	21
4.1.1 General Network Connection Parameters	22
4.1.2 UMTS	22
4.1.3 PPP Authentication	23
4.1.4 Internet Protocol Settings	24

4.1.5	DNS Server	24
4.1.6	Routing	25
4.1.7	Additional Network Connection Settings	26
4.2	LAN Ethernet Connection	27
4.2.1	General Network Connection Parameters	27
4.2.2	Internet Protocol	28
4.2.3	DNS Server	29
4.2.4	DHCP	29
4.2.5	Routing	31
4.2.6	Additional Network Connection Settings	32
4.3	LAN Wireless Connection	33
4.3.1	Configuring Your Wireless Network	33
4.3.1.1	Configuring your GlobeSurfer 3G Wireless Connection	33
4.3.1.2	Configuring Your Wireless Windows XP Client	34
4.3.2	Securing Your Wireless Network	39
4.3.2.1	Securing Your Wireless Network with WPA	39
4.3.2.2	Connecting a Wireless Windows XP Client to the Secured Wireless Network	41
4.3.3	Advanced Wireless Connection Settings	47
4.3.3.1	General Network Connection Parameters	47
4.3.3.2	Wireless Access Point	47
4.3.3.3	MAC filtering settings	48
4.3.3.4	Advanced Wireless Options	48
4.3.3.5	Wireless Security	49
4.3.3.6	Internet Protocol	50
4.3.3.7	Additional Network Connection Settings	51
4.4	LAN Bridge Connection	52
4.4.1	General Network Connection Parameters	52
4.4.2	Internet Protocol	53
4.4.3	Bridge Settings	54
4.4.4	DNS Server	54
4.4.5	DHCP	55
4.4.6	Routing	57
4.4.7	Additional Network Connection Settings	57
4.5	VPN PPTP	59
4.5.1	Creating a PPTP Client Connection	59
4.5.2	Creating a PPTP Server Connection	61
4.5.3	Configuring a PPTP Connection	64
4.5.3.1	General	64
4.5.3.2	PPP Settings	65
4.5.3.3	PPP Authentication	65
4.5.3.4	PPP Encryption	66
4.5.3.5	Internet Protocol	66
4.5.3.6	DNS Server	67
4.5.3.7	Routing	68
4.5.3.8	Internet Connection Firewall	69
4.6	VPN L2TP	70
4.6.1	Creating an L2TP Connection	70
4.6.2	Configuring an L2TP Connection	72

4.6.2.1	General	72
4.6.2.2	PPP Settings	73
4.6.2.3	PPP Authentication	74
4.6.2.4	PPP Encryption	74
4.6.2.5	PPP Compression	75
4.6.2.6	Internet Protocol	75
4.6.2.7	DNS Server	76
4.6.2.8	Routing	77
4.6.2.9	Internet Connection Firewall	78
4.7	VPN IPsec	79
4.7.1	IPsec Network-to-Host Scenario Connection	79
4.7.1.1	Configuring IPsec on GlobeSurfer 3G	79
4.7.1.2	Configuring IPsec on the Windows Host	82
4.7.2	IPsec Network-to-Network Scenario Connection	95
4.7.2.1	Network Configuration	95
4.7.2.1.1	LAN Interface Settings	95
4.7.2.2	Network-to-Network with Pre-shared Secrets	97
5	Security	102
5.1	General Security Level Settings	104
5.2	Access Control	107
5.3	Local Servers (Port Forwarding)	110
5.4	DMZ Host	113
5.5	Port Triggering	114
5.6	Remote Administration	117
5.7	IP-Hostname Filtering	119
5.8	Advanced Filtering	122
5.8.1	Adding an Advanced Filtering Rule	123
5.9	Security Log	126
5.9.1	Security Log Settings	130
5.10	User-defined Services	132
5.11	Applying Corporate-Grade Security	134
6	Advanced	136
6.1	System Settings	139
6.1.1	System	139
6.1.2	GlobeSurfer 3G Management Console Settings	139
6.1.3	Management Application Ports Settings	139
6.1.4	System Logging Settings	140
6.1.5	Security Logging Settings	140
6.1.6	Outgoing Mail Server Settings	140
6.1.7	HTTP interception	140
6.2	DNS Server	141
6.2.1	Viewing and Modifying the DNS Table	141
6.3	Dynamic DNS	143
6.3.1	Using Dynamic DNS	143
6.4	Network Map	144
6.5	DHCP	146
6.5.1	DHCP Server Summary	146
6.5.2	DHCP Server Settings	147

6.5.3	DHCP Server Relay Settings	148
6.5.4	DHCP Connections	148
6.6	Network Objects	151
6.7	Routing	153
6.7.1	Managing Routing Table Rules	153
6.7.2	Multicasting	154
6.8	Managing Users	155
6.9	Certificates	157
6.9.1	Digital Certificates	157
6.9.2	X.509 Certificate Format	157
6.9.3	Obtaining an X.509 Certificate	158
6.9.4	Registering a CA's Certificate	162
6.10	Date and Time	163
6.11	Scheduler Rules	164
6.12	Firmware Upgrade	166
6.12.1	Upgrading From a Local Computer	166
6.13	Point-to-Point Tunneling Protocol (PPTP)	168
6.13.1	Managing Remote Users	168
6.13.2	Advanced PPTP Server Settings	170
6.13.3	Advanced PPTP Client Settings	170
6.14	IP Security (IPsec)	172
6.14.1	Technical Specifications	172
6.14.2	Basic IPsec Connection Settings	172
6.14.2.1	Key Management	173
6.14.2.2	Log Settings	174
6.14.3	Advanced IPsec Connection Settings	174
6.15	Universal Plug and Play (UPnP)	177
6.16	Simple Network Management Protocol (SNMP)	178
6.16.1	Configuring GlobeSurfer 3G's SNMP Agent	178
6.17	Diagnostics	179
6.17.1	Diagnosing Network Connectivity	179
6.18	Advanced Remote Administration	180
6.19	SIM Setup	182
6.20	Unlock Device	183
6.21	Restoring Default Settings	184
6.22	Restart	185
6.23	Technical Information	186
7	System Monitoring	187
7.1	Monitoring Connections	188
7.2	Traffic Statistics	189
7.3	System Log	190
7.4	System Up Time	191
A	Glossary	192

List of Acronyms

3G	Third Generation (mobile network)
ALG	Application-Level Gateway
API	Application Programming Interface
APN	Access Point Name
CA	Certificate Authority
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
HTTP	HyperText Transport Protocol
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
IPsec	IP Security
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
OAM	Operations and Maintenance
OEM	Original Equipment Manufacturer
PDA	Personal Digital Assistant
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PUK	Pin Unlocking Key
RG	Residential Gateway
RIP	Routing Information Protocol
SMS	Short Message Service
SMSC	Short Message Service Center
SIM	Security Identity Module
SNMP	Simple Network Management Protocol
SPI	Stateful Packet Inspection
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telephony System
UPnP	Universal Plug and Play

URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wireless Encryption Protocol
WLAN	Wireless Local Area Network
WPA	Wireless Protected Access

1

Introduction to GlobeSurfer 3G

Welcome to the third generation wireless network. By combining a wireless router following the 802.11 b/g WLAN standard with a 3G UMTS Gateway the GlobeSurfer 3G presents a new style of wireless freedom.

The GlobeSurfer 3G is a 802.11b/g wireless router and Internet gateway that provides Internet access for homes and small offices over the 3G UMTS network. By connecting laptops and stationary computers with either WLAN or Ethernet to the GlobeSurfer 3G you will get Internet access with a speed similar to a fixed DSL connection. And while sharing the wireless Internet connection you will also be able to share the resources of the local computers connected to the GlobeSurfer 3G.

GlobeSurfer 3G is easy to install and use. Yet it provides advanced networking functions and security functions that can be configured with a web-based management interface. Its small attractive design and powerful built-in functionality makes your Internet surfing easy and secure in any location with 3G access and a power outlet.

Some of the attractive features of the GlobeSurfer 3G:

- WAN - UMTS uplink and downlink
- Small attractive design with informative display
- Sends and receives SMS
- WLAN according to 802.11 b/g for maximum compatibility
- Ethernet connection for stationary computers
- Built-in firewall to protect against hacker attacks
- Wireless LAN Security: WEP, WPA, 802.1x
- VPN (Virtual Private Network): IPsec, PPTP, L2TP

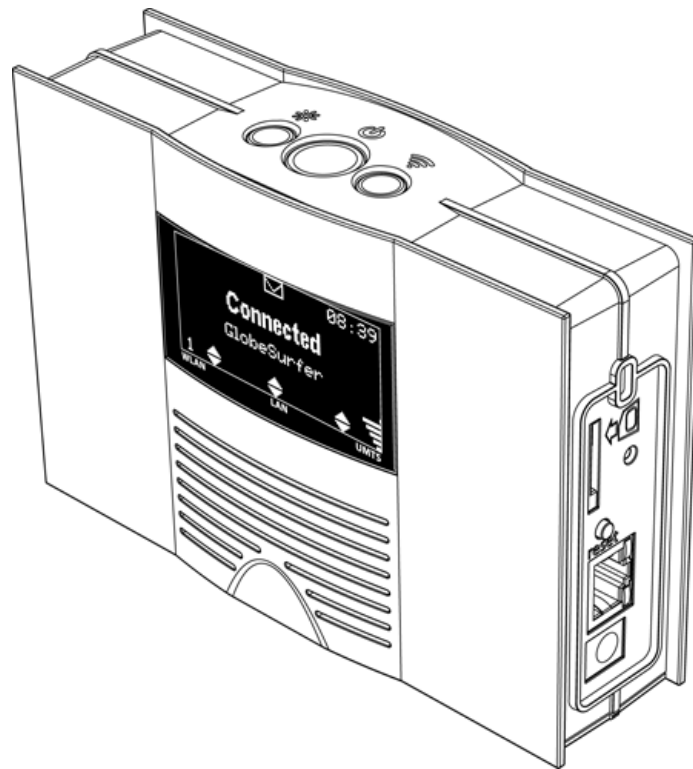


Figure 1.1: The GlobeSurfer 3G

- Web-based management console makes configuration intuitive
- System statistics and monitoring for the advanced users
- Remote upgrade to stay in touch with the future

1.1 About This Manual

This manual describes configuration and operation of the GlobeSurfer 3G. It is intended as a complement to the GlobeSurfer 3G User Guide to provide reference information for the advanced user of the GlobeSurfer 3G. It is assumed that the hardware installation of the GlobeSurfer 3G has been done when the Reference Manual is read.

This version of the manual is valid for GlobeSurfer 3G version 3.15.4 R2H. Other product versions with customer specific functions not described in this manual, may be available.

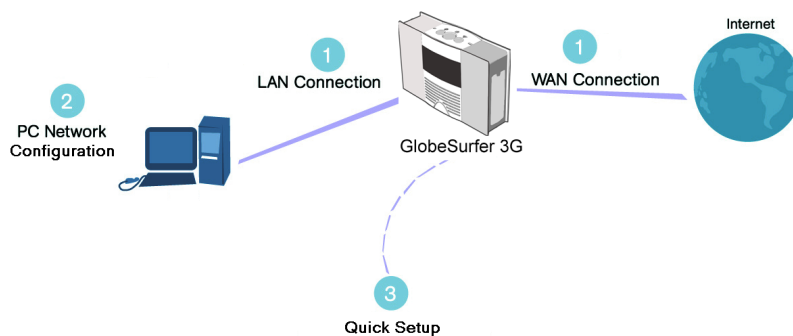


Figure 1.2: Hardware Configuration

1.2 Basic Setup

Connecting your computer or local network to the GlobeSurfer 3G is a simple procedure, varying slightly depending on your operating system. The setup is designed to seamlessly integrate GlobeSurfer 3G with your computer or local network.

The Windows default network settings will in most cases make the setup procedure described below unnecessary. For example, the default DHCP setting in Windows is *client*, requiring no further modification.

However, it is advised to follow the setup procedure described below to verify that all communication parameters are valid and that the physical cable connections are correct.

The basic setup procedure consists of three consecutive configuration steps (Please refer to figure 1.2):

1. Setting up LAN and WAN connections [1.3]
2. PC network configuration [1.4]
3. GlobeSurfer 3G Quick Setup [1.5]

1.3 Step 1 - Setting up LAN and WAN Connections

1.3.1 LAN Connection

Your computer can connect to the GlobeSurfer 3G either with a fixed cable connection or with a wireless connection.

If you want to use a fixed connection, connect a standard Ethernet RJ-45 cable (Category 5) between the LAN socket on the GlobeSurfer 3G and the corresponding Ethernet LAN port of your PC network card. Consult the GlobeSurfer 3G User Guide for more information about the LAN port.

If you want to use a wireless connection, according to the 802.11 b/g WLAN standard, follow the instructions from the supplier of your WLAN adapter card, or your PC if the WLAN adapter is built into the PC.

1.3.2 WAN Connection

Setting up the WAN connection requires that a SIM card is inserted correctly into the SIM slot of the GlobeSurfer 3G. See the User Guide for instructions on how to insert the SIM card. With the SIM card in place you configure the WAN connection through the Quick Setup of the GlobeSurfer 3G (see section 1.5). The first time you login to the GlobeSurfer 3G you will have to enter a PIN code. The PIN code is received from your ISP, but normally provided separately from the SIM card for security reasons.

1.4 Step 2 - PC Network Configuration

The GlobeSurfer 3G provides a DHCP server, which means that each computer connected to the LAN can obtain its network addresses – IP address and DNS server IP addresses – automatically from the GlobeSurfer 3G. This is the default setting in Windows and valid in most cases. Alternatively, each network interface on the LAN PCs can be configured with a statically defined IP address and DNS address. If this is the case you must receive valid addresses from your network operator and configure your PC and the GlobeSurfer 3G accordingly. Then refer to section 4.2.

Figure 1.3 displays the *TCP/IP Properties* dialog box as it appears in Windows XP. These properties are available on all operating systems but are accessed slightly differently on each operating system.

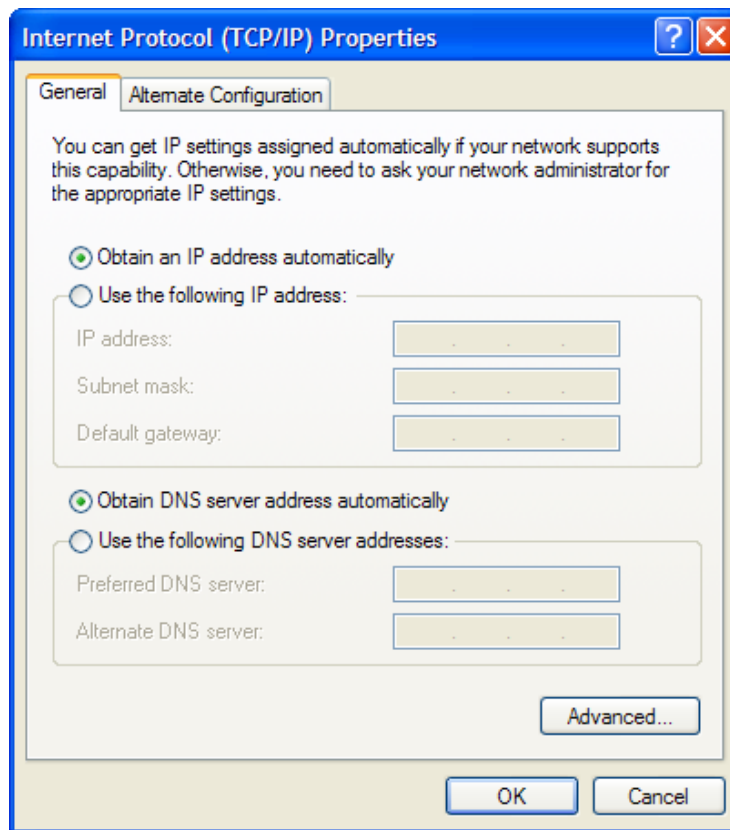


Figure 1.3: IP and DNS Configuration

1.4.1 Windows XP

1. Access *Network Connections* from the Control Panel.
2. Right-click on the Ethernet connection icon, and select *Properties*.
3. Under the *General* tab, select the *Internet Protocol (TCP/IP)* component, and click the *Properties* button.
4. The *Internet Protocol (TCP/IP)* properties window will be displayed (see figure 1.3).
 - (a) Select the *Obtain an IP address automatically* radio button.
 - (b) Select the *Obtain DNS server address automatically* radio button.
 - (c) Click *OK* to save the settings.

1.4.2 Windows 2000/98/Me

1. Access *Network and Dialing Connections* from the Control Panel.

-
2. Right-click on the Ethernet connection icon, and select *Properties* to display the connection's properties.
 3. Select the *Internet Protocol (TCP/IP)* component, and click the *Properties* button.
 4. The *Internet Protocol (TCP/IP)* properties will be displayed.
 - (a) Select the *Obtain an IP address automatically* radio button.
 - (b) Select the *Obtain DNS server address automatically* radio button.

1.5 Step 3 - GlobeSurfer 3G Quick Setup

The GlobeSurfer 3G management console allows you to control various GlobeSurfer 3G system parameters. The interface is accessed through a web browser:

1. Start a web browser on your PC.
2. Enter the address 192.168.1.1 to display the GlobeSurfer 3G management console. When first logging on to the management console, the welcome screen will appear (see figure 1.4), enabling you to place a shortcut to this screen in your *Favorites* folder. Click *OK* to continue. The *Login Setup* screen will appear (see figure 2.1).

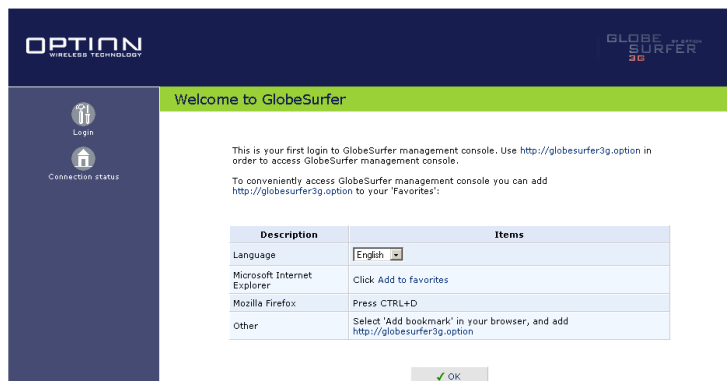


Figure 1.4: Welcome to GlobeSurfer 3G

3. To configure your login settings, enter a user name and password. To verify correctness retype the password, and click *OK* to login to the management console. For security reasons it is strongly recommended that you change the default user name and specify a password. However, make sure you remember your new user name and password, since this is the only way you will be able to login to the GlobeSurfer 3G from now on.

Figure 1.5: Login Settings

4. *Quick setup* helps you to quickly set the most important settings of your GlobeSurfer 3G. The *Quick setup* page is launched automatically when you log on to GlobeSurfer 3G for the first time (see figure 1.6). Alternatively, click the *Quick setup* icon on the left sidebar. The following sections describe the various configuration parameters of *Quick setup*. Once you have filled the *Quick setup* sections as described below, click the *OK* button to configure your GlobeSurfer 3G.

Figure 1.6: Quick Setup

1.5.1 UMTS Setup

Check or change the following settings on the *Quick setup* screen to configure the UMTS connection:

- **Access point name:** Enter the access point name as provided by your Internet Service Provider (ISP), or accept the name already set.

-
- **Connect automatically:** To automatically set up a UMTS connection when data is about to be sent or received, select *Automatically*. If *Manually* is selected, you must press the **Connect** button on the GlobeSurfer 3G each time a connection is required.
 - **Inactivity timeout:** There is normally no need to change the default value of 10 minutes. Set it to zero (0) if you don't want the UMTS connection to disconnect automatically at all. The maximum value is 1440 minutes (24 h). The inactivity timeout is not affected by incoming traffic.

1.5.2 Wireless Setup

The following settings are the most important to set up for the local Wireless LAN:

- **SSID:** The Service Set Identifier (SSID) is the name of the specific wireless network. Enter a name that you want to use as an identifier of your specific local wireless network (maximum 32 characters).
- **SSID broadcast:** When this checkbox is set to *Enabled* the GlobeSurfer 3G will broadcast the SSID on your wireless network. This will allow unauthorized devices from detecting your SSID and attempting to connect to your network. De-select the checkbox to disable broadcasting of the SSID. Disabling SSID broadcast will hide the name of the network from other wireless devices. This provides a very basic form of security. Other devices will still be able to connect, provided that they are supplied with the SSID. A recommendation is to install your wireless network with this feature enabled and then disable it once you have set up the GlobeSurfer 3G and any wireless clients.
- **Encryption:** With *No encryption* selected, anyone with a Wireless PC can eavesdrop on your network. *No encryption* should only be used during installation of your network to simplify the setup procedure. Select *WEP* encryption or *WPA* encryption once your local wireless network has been set up. See below for instructions on how to set the encryption type.

1.5.2.1 Encryption

The GlobeSurfer 3G supports two types of encryption:

- **WEP:** Wireless Equivalent Privacy (WEP) is a 64 bit or 128 bit encryption method with user configurable fixed keys. However, only 40/104 bits are effectively used.
- **WPA:** Wi-Fi Protected Access (WPA) is a 256 bit encryption method with keys that change over time.

Note: WPA provides a higher level of security, provided by its longer key and dynamic changes made to the key over time. Use WPA with any clients that support it. If you enable encryption on the GlobeSurfer 3G, you must configure your wireless PCs to use exactly the same encryption type and keys, otherwise the devices will not understand each other. The encryption secures the wireless communication between GlobeSurfer 3G and its wireless clients. Enabling

encryption has no security effect on data transmitted through wired (Ethernet) connections.

- Configuring WEP:

There are two levels of WEP encryption available, 64 bit and 128 bit. Select the desired level. Enter the pre-shared key in either hexadecimal (0-9, A-F) format, 10 or 26 characters, or plain text (ASCII) format, 5 or 13 characters.

- Configuring WPA:

With WPA there is only one level of encryption available. Enter the pre-shared key, either as a 256 bit series of hexadecimal digits (64 characters) or as a plain text (ASCII) pass-phrase (at least 8 characters).

Note: A plain text string is much easier to remember than hex keys, but it may be easier to crack. Also note that the ASCII-text format may not be supported by all wireless devices, since different manufacturers have developed different ways of converting plain text. If you are experiencing difficulty, the hex key format is supported by most vendors.

1.5.3 Firewall Setup

The GlobeSurfer 3G firewall has three pre-defined levels of security. As default the typical security is set, which blocks all traffic that has been initiated by an external (Internet) source, and allows all traffic that has been initiated from your local network.

Note: It is the *origin of the request*, not subsequent responses to this request, that determines whether the incoming or outgoing traffic is allowed or blocked.

To learn more about how to configure your firewall security parameters, please refer to Section 5. If you wish to apply corporate-grade security to your network refer to Section 5.11.

1.6 Additional Network Configuration

GlobeSurfer 3G does not require further configuration in order to start working. After the setup described in this chapter, you can immediately start using the GlobeSurfer 3G to:

- Build a local network by connecting additional PCs and network devices to the GlobeSurfer 3G.
- Share the Internet connection among multiple users and between all of the computers connected to your local network.
- Share resources like file servers, printers, etc. between computers in the local network.
- Control network parameters to, for example, set up Virtual Private Networks, LAN bridges and configure the security settings.
- View network status, traffic statistics, system log and more.

Advanced users can fully configure and control the GlobeSurfer 3G via the web-based management console. Chapter 2 serves as an introduction to the management console; in-depth module-specific information is available throughout chapters 4 – 7.

1.7 Adding Computers to Your Network

Any computers with a 802.11b/g wireless adapter will be able to connect to the WLAN created with the GlobeSurfer 3G. To connect additional computers without a wireless adapter to your GlobeSurfer 3G, connect a hub or switch to the LAN port, and then connect the computers to the hub or switch. Make sure to configure all computers to automatically obtain a network address as described above.

2

GlobeSurfer 3G Management Console

The GlobeSurfer 3G management console described here allows you to control various GlobeSurfer 3G system parameters, using a user-friendly graphical interface. The management console includes a quick setup screen, a graphical network map, network configuration, security configuration, authentication with multiple-user support, connection monitoring and more.

2.1 Accessing the GlobeSurfer 3G Management Console

To access the management console:

1. Launch a Web-browser on a PC in the LAN or WLAN.
2. Type the IP address of the GlobeSurfer 3G or a name as provided by the supplier in the address bar (Internet Explorer) or location bar (Netscape Navigator). The default IP address is 192.168.1.1, and default name is *http://umts-gateway.my-domain*.
3. Enter your username and password to log on to the web-based management console. **Note:** for security reasons, you should change these settings after the initial login as explained in Section 1.5. The default user name is *admin*, and the default password is none.

Login setup

Please configure GlobeSurfer's username and password:

Username:	<input type="text" value="admin"/>
New password:	<input type="password" value="*****"/>
Retype new password:	<input type="password" value="*****"/>







Figure 2.1: First Time Login

Your session will automatically time-out after a few minutes of inactivity. If you try to operate the management console after the session has expired the *Login* screen will appear and you will have to reenter your user name and password before proceeding. This feature helps to prevent unauthorized users from accessing the management console and changing the GlobeSurfer 3G settings.

2.2 Left Sidebar

The GlobeSurfer 3G management console screens have been grouped into several subject areas and may be accessed by clicking on the appropriate icon in the left sidebar.

The subject areas are:

-  **Connection status:** Display the status of the UMTS connection (see Section 2.2)
-  **SMS:** Send, receive and maintain SMS messages (see Chapter 3)
-  **Quick setup:** Quickly configure your GlobeSurfer 3G (see Section 1.5)
-  **Network connections:** Create and configure network connections (see Chapter 4)
-  **Security:** Configure the Firewall and regulate communication between the Internet and the local network (see Chapter 5)
-  **Advanced:** Control system parameters (DHCP server, DNS) and perform administrative functions, including changing password, setting date and time and upgrading the system (see Chapter 6)



System monitoring: View network status, traffic statistics and the system log (see Chapter 7)



Logout: Log out from GlobeSurfer 3G

2.3 UMTS Connection Status

The *Connection status* screen shows the status of the UMTS connection and provides a button to manually connect and disconnect. To connect automatically as required, for example when an Internet address is entered in the browser, select the radio button *Automatically*.

The following additional information is provided:

- Current connection time: the duration of the current connection.
- Total connection time: the cumulated duration of all connections.
- Bytes received: the amount of data received in bytes.
- Bytes sent: the amount of data sent in bytes.

The information in *Connection status* can be refreshed and updated manually by clicking *Refresh*. You can also set *Connection status* to update automatically by clicking *Automatic refresh on* once.



View UMTS connection status.

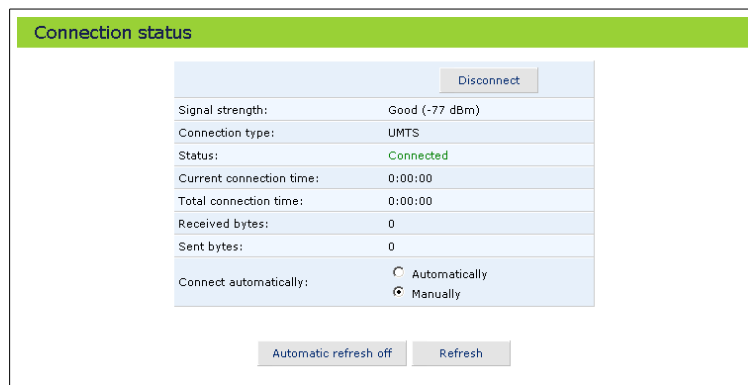


Figure 2.2: UMTS Connection Status

2.4 Getting Help

The help icon on the upper right side of the management console may be used to get on-line help about the settings you see on each particular screen.



View help information about each specific management console screen.

2.5 Managing Tables

Tables are used throughout the GlobeSurfer 3G management console. They handle user-defined entries relating to elements such as network connections, local servers, restrictions and configurable parameters. The principles outlined in this section apply to all tables in the management console.













Name	Status	Action
LAN Bridge	Connected	  
LAN Ethernet	Connected (no IP address assigned)	  
LAN Wireless	Connected (no IP address assigned)	  
WAN UMTS	Searching for network	  
New connection >>		

Figure 2.3: Typical Table Structure

Figure 2.3 illustrates a typical table. Each row defines an entry in the table. The following icons located in the *Action* column enable adding, editing and deleting table entries:



Click the **Add** icon to add an entry of the same type as on that row.



Click the **Edit** icon to edit the entry on that row.



Click the **Delete** icon to remove the entry on that row.

In many tables the last row includes a link that allows adding a new entry to the table.

3

SMS Manager

The SMS Manager is used for sending, receiving and managing your SMS messages. Using the SMS Manager is just like using the SMS functions on a mobile phone, but with the convenience of a full size PC screen and keyboard.



Access the SMS Manager by clicking *SMS* in the left sidebar.

The display of the GlobeSurfer 3G shows an envelope symbol when a new SMS message is received.

3.1 Reading an SMS

1. When starting the SMS Manager the *Inbox* tab of the SMS Manager is displayed (see figure 3.1). The inbox displays all received SMS messages in a table. Unread SMS messages are shown in bold.

The screenshot shows the 'SMS manager' interface with a green header bar. Below the header are several tabs: 'SMS CREATE', 'INBOX', 'OUTBOX', 'SENT', 'ARCHIVE', 'TEMPLATES', and 'SETTINGS'. The 'INBOX' tab is selected. Below the tabs is a table with three columns: 'Date', 'Number', and 'SMS'. The table contains one row of data.

Date	Number	SMS
2005-11-21 11:11:07	+46709989712	Welcome to GlobeSurfer 3G!

Figure 3.1: SMS Manager Inbox

2. Click the SMS in the table that you want to read. The complete message text is shown.

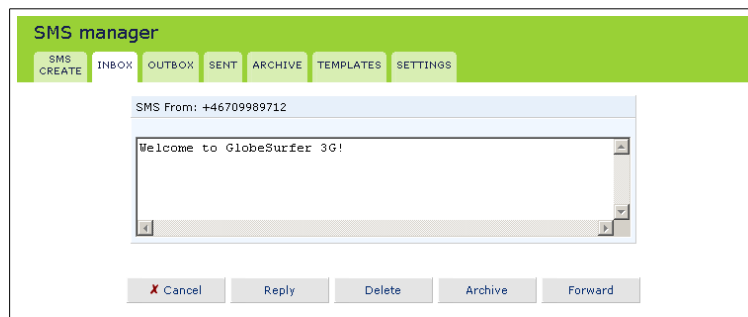


Figure 3.2: Reading an SMS

3. When you have read the SMS you can click any of the buttons underneath to:
 - **Reply** to the sender. You will then be moved to the *SMS create* screen with the received text displayed and the phone number of the sender already filled in (see Section 3.2).
 - **Delete** the SMS. **Note:** The SMS is deleted immediately without confirmation and is not possible to restore.
 - **Archive** the SMS (see Section 3.3).
 - **Forward** the SMS. You will be moved to **SMS Create** with the received text displayed (see Section 3.3).

3.2 Creating an SMS

1. Select the *SMS create* tab of the SMS Manager.
2. Type your message text in the *SMS message* field. The *Characters left* field shows how many characters you can type before the size limit is reached.
3. Enter the phone number of the receiver in the *Phone numbers* field. Additional numbers can be separated with a comma. Maximum 10 numbers are allowed. The phone number should be formatted like +49176123456789 for international and like 0176123456789 for national numbers.
4. Select the *Flash SMS* checkbox if you want the SMS to be shown in full on the receiver's display immediately when received (not supported by all mobile terminals).
5. Click the *Send* button when ready. Or click the *Save as template* button to save the message as a template for future use.

Figure 3.3: Creating an SMS

3.2.1 Sent folder

The SMS is put in the *Sent* folder whether it was successfully sent or not.

3.3 Archiving an SMS

The SMS archive is a storage area for SMS messages that you want to save. The total maximum number of SMS messages in the *Sent*, *Outbox*, *Archive* and *Templates* folders is 100.

1. Select the SMS that you want to store, either from the *Inbox* or from the *Sent* folder.
2. Click the *Archive* button below the open SMS. The message is moved to the archive.
3. Select the *Archive* tab and check that the message has been added to the archive table.

Date	Number	SMS
2005-11-21 11:11:07	+46709989712	Welcome to GlobeSurfer 3G!

Figure 3.4: The SMS archive

3.4 SMS Templates

Templates can be used when you write messages with similar contents. Then create an SMS with the standard text and save it as a template.

-
- To create a new template:
 1. Select the *SMS Create* tab to create a new message to use as a template (see Section 3.2).
 2. Click the *Save as template* button when ready.
 - To use an existing template:
 1. Select the *Templates* tab, and then click the message that you want to use.

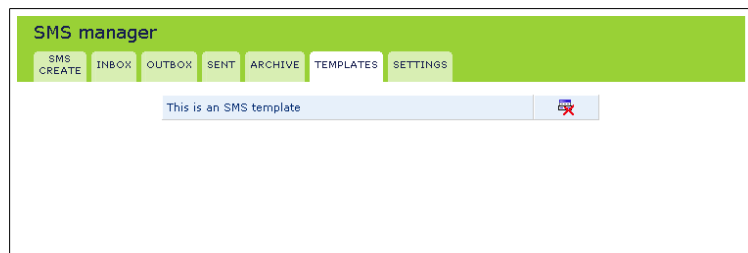


Figure 3.5: SMS Templates

You are then moved to the *SMS create* tab to change the text and to enter the phone number of the receiver, as required.

2. Click the *Send* button when ready.

3.5 SMS Settings

The only specific SMS Manager setting you can do is to set the number to the Short Message Service Center (SMSC number). This number is normally pre-configured by your ISP and stored in the SIM card.

Click the *Settings* tab to display the SMSC number. Enter the new number and click *OK*.

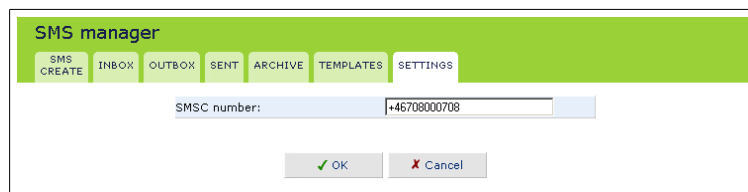


Figure 3.6: SMS Manager Settings

4

Network Connections

The *Network connections* screen enables you to configure the various parameters of each LAN, WAN and VPN connection. The following sections describe the network connection screens to configure:

- WAN - Connecting via UMTS to the Internet
 - UMTS connection (see Section 4.1).
- LAN - Creating a local network
 - Ethernet connection (see Section 4.2).
 - Wireless connection (see Section 4.3).
 - LAN bridge connection (see Section 4.4).
- VPN - Creating a secured connection
 - PPTP (see Section 4.5).
 - LT2P (see Section 4.6)
 - IPsec (see Section 4.7).

1. Click the *Network connections* icon on the sidebar. (see figure 4.1).

Name	Status	Action
LAN Bridge	Connected	
LAN Ethernet	Connected (no IP address assigned)	
LAN Wireless	Connected (no IP address assigned)	
WAN UMTS	Searching for network	
New connection >>		

[Quick setup](#) [Status](#) [Basic <<](#)

Figure 4.1: Network connections – Advanced

2. Click your connection entry in the network connections table to view the connection properties.
3. Click *New connection* to start a wizard to create a new connection type.

4.1 WAN UMTS Connection

The UMTS connection connects the GlobeSurfer 3G to the Internet and other networks through the 3G/UMTS mobile telecommunications standard. The *WAN UMTS properties* screen displays a summary of the connection properties.

The screenshot shows a window titled "WAN UMTS properties" with a green header bar. A "Disconnect" button is in the top right. The main area contains a table of connection details:

Name:	WAN UMTS
Status:	Connected
Network:	WAN
IP address:	10.145.10.76
Subnet mask:	255.0.0.0
Default gateway:	212.181.254.83
DNS server:	10.0.0.1 10.0.0.2
Username:	
Current connection time:	0:00:00
Total connection time:	0:10:10
Access point name:	online.telia.se
Operator:	Sweden 3G
Signal strength:	Good (-73 dBm)
Connection type:	UMTS
Connect automatically:	<input type="radio"/> Automatically <input checked="" type="radio"/> Manually

At the bottom, there are buttons for "OK", "Apply", "Cancel", and "Settings". Below these are "Automatic refresh off" and "Refresh" buttons.

Figure 4.2: WAN UMTS Properties

Clicking on the *Settings* button at the bottom-right of the connection's Properties window, will open its Configuration window.

Figure 4.3: WAN UMTS Configuration

4.1.1 General Network Connection Parameters

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The setting *Manual*, allows you to enter the largest packet size that will be transmitted. To have the GlobeSurfer 3G select the best MTU for your Internet connection, select *Automatic*.

4.1.2 UMTS

- **Access point name:** Enter the access point name as provided by your Internet Service Provider (ISP), or accept the name already set.
- **Connect automatically:** To automatically set up a UMTS connection when data is about to be sent or received, select *Automatically*. If *Manually* is selected, you must press the **Connect** button on the GlobeSurfer 3G to connect each time a connection is required.
- **Inactivity timeout:** There is normally no need to change the default value of 10 minutes. Set it to zero (0) if you don't want the UMTS connection to disconnect automatically at all. The inactivity timeout is not affected by incoming traffic.

- **Network type:** Select one of the following settings (not available in some product versions):
 - **Automatic:** The GlobeSurfer 3G automatically connects using the network type that gives the best connection, UMTS or GPRS.
 - **Automatic, UMTS preferred:** The GlobeSurfer 3G connects using UMTS. If UMTS fails, GPRS is used instead.
 - **Automatic, GPRS preferred:** The GlobeSurfer 3G connects using GPRS. If GPRS fails, UMTS is used instead.
 - **UMTS only:** The GlobeSurfer 3G connects using UMTS only.
 - **GPRS only:** The GlobeSurfer 3G connects using GPRS only.

4.1.3 PPP Authentication

Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2.

Please note that encryption is performed only if *Microsoft CHAP*, *Microsoft CHAP version 2*, or both are selected.

PPP	
PPP authentication	
Login username (case sensitive):	<input type="text" value="dina"/>
Login password:	<input type="password" value="*****"/>
<input type="checkbox"/>	Support unencrypted password (PAP)
<input type="checkbox"/>	Support Challenge Handshake Authentication (CHAP)
<input checked="" type="checkbox"/>	Support Microsoft CHAP (MS-CHAP)
<input checked="" type="checkbox"/>	Support Microsoft CHAP Version 2 (MS-CHAP v2)

Figure 4.4: PPP Authentication Settings

Login username As agreed with ISP.

Login password As agreed with ISP.

Support unencrypted password (PAP) Password Authentication Protocol (PAP) is a simple, plaintext authentication scheme. The user name and password are requested by your networking peer in plaintext. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

4.1.4 Internet Protocol Settings

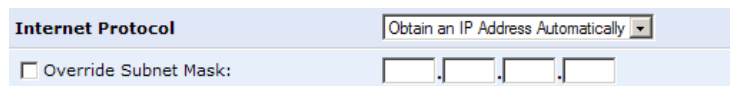
Select one of the following Internet protocol options from the *Internet protocol* drop down menu:

- Obtain an IP address automatically
- Use the following IP address

Please note that according to the selection you make in the *Internet protocol* drop down menu, the screen will refresh and display relevant configuration settings.

Obtain an IP address automatically Your PPP connection is configured by default to obtain an IP address automatically. You should change this configuration in case your service provider requires it.

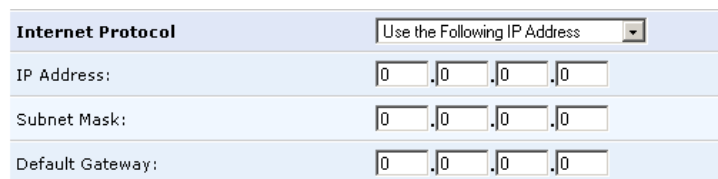
The server that assigns the GlobeSurfer 3G with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the *Override subnet mask* and specifying your own mask instead.



The screenshot shows the 'Internet Protocol' settings window. The dropdown menu is set to 'Obtain an IP Address Automatically'. Below this, there is a checkbox labeled 'Override Subnet Mask:' which is currently unchecked. To the right of the checkbox are four empty input boxes for entering a subnet mask in dotted decimal notation.

Figure 4.5: Internet Protocol Settings – Automatic IP

Use the following IP address Your WAN connection can be configured using a permanent (static) IP address. Your service provider should provide you with this IP address, subnet mask and the default gateway IP address.



The screenshot shows the 'Internet Protocol' settings window. The dropdown menu is set to 'Use the Following IP Address'. Below this, there are three rows of input fields. The first row is labeled 'IP Address:' and contains four input boxes with '0' in each. The second row is labeled 'Subnet Mask:' and also contains four input boxes with '0' in each. The third row is labeled 'Default Gateway:' and contains four input boxes with '0' in each.

Figure 4.6: Internet Protocol Settings – Static IP

4.1.5 DNS Server

Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP.

To configure the connection to automatically obtain a DNS server address, select *Obtain DNS Server Address Automatically* from the *DNS Server* drop down menu.



Figure 4.7: Automatic DNS Settings

To manually configure DNS server addresses, select *Use the following DNS server addresses* from the *DNS server* drop down menu (see figure 4.100). Specify up to two different DNS server addresses, one primary and one secondary.

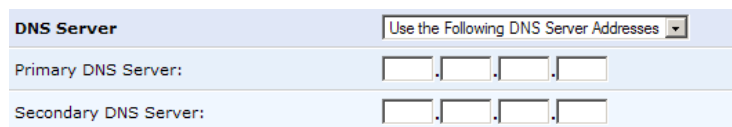


Figure 4.8: DNS Settings

To learn more about this feature, refer to Section 6.2.

4.1.6 Routing

You can choose to setup your GlobeSurfer 3G to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

Routing Select *Advanced* or *Basic* routing.

Routing Mode When *Advanced* routing is selected, select one of the following Routing modes:

Route Use route mode if you want your GlobeSurfer 3G to function as a router between two networks.

NAT Network Address Translation (NAT) translates an IP address to a valid, public address on the Internet. This adds security since internal LAN addresses are not transmitted over the Internet. In addition, NAT allows many addresses to exist behind a single valid address. Use the NAT routing mode if your LAN consists of a single device, otherwise collisions may occur if more than one device attempts to communicate using the same port.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device metric The device metric is a value used by the GlobeSurfer 3G to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default route Select this check box to define this device as the default route.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

- Listen to RIP messages - select *None*, *RIPv1*, *RIPv2* or *RIPv1/2*.
- Send RIP messages - select *None*, *RIPv1*, *RIPv2-broadcast* or *RIPv2-multicast*.

Multicast - IGMP proxy internal IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of LAN devices asking to join multicast groups. Select the *Multicast IGMP proxy internal* check-box to enable this feature.

Routing table Allows you to add or modify routes when this device is active. Click the link to an existing route to edit it, or click *New Route* to add a route.



Routing		Advanced ▾				
Routing mode:	Route					
Device metric:	4					
<input type="checkbox"/> Default route						
<input checked="" type="checkbox"/> Multicast - IGMP proxy internal						
<input type="checkbox"/> Routing Information Protocol (RIP)						
Routing table						
Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Wireless	192.168.22.3	192.168.2.1	255.255.255.255	0	Applied	 
New route >>						
Internet connection firewall		<input type="checkbox"/> Enabled				

Figure 4.9: Advanced Routing Properties

To learn more about this feature, refer to Section 6.7.

4.1.7 Additional Network Connection Settings

Internet connection firewall Select this check box to enable the GlobeSurfer 3G firewall on the connection. To learn more about configuring security settings, please refer to Chapter 5.

Internet connection firewall	<input checked="" type="checkbox"/> Enabled
-------------------------------------	---

Figure 4.10: Internet Connection Firewall

4.2 LAN Ethernet Connection

A LAN Ethernet connection connects local computers to GlobeSurfer 3G using Ethernet cables, either directly or via network hubs and switches. The *LAN Ethernet Properties* screen displays a summary of the connection properties.

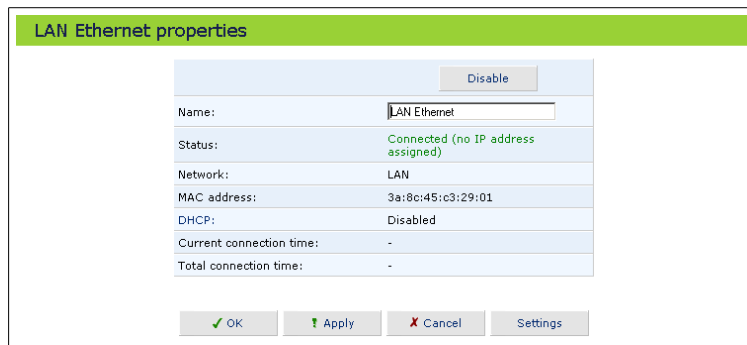


Figure 4.11: LAN Ethernet Properties

Clicking on the *Settings* button at the bottom-right of the connection's Properties window, will open its Configuration window.

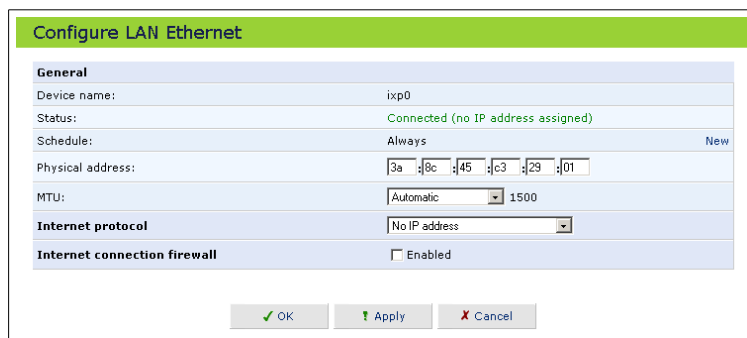


Figure 4.12: LAN Ethernet Configuration

4.2.1 General Network Connection Parameters

The top part of the configuration window displays general communication parameters. It is recommended not to change the default values in this screen unless you are familiar with the networking concepts they represent. Since your GlobeSurfer 3G is configured to operate with the default values, no parameter modification is necessary. You can configure the following general connection settings:

Schedule You can configure scheduler rules in order to define time segments during which the connection is active. To configure scheduler rules click the *New* link. To learn how to configure scheduler rules please refer to Section 6.11.

Physical Address The physical address of the network card used for your network. Some cards allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The setting *Manual*, allows you to enter the largest packet size that will be transmitted. To have the GlobeSurfer 3G select the best MTU for your Internet connection, select *Automatic*.

4.2.2 Internet Protocol

Select one of the following Internet protocol options from the *Internet protocol* drop down menu:

- No IP address
- Obtain an IP address automatically
- Use the following IP address

Please note that according to the selection you make in the *Internet protocol* drop down menu, the screen will refresh and display relevant configuration settings.

No IP address Select *No IP address* if you require that this connection will have no IP address. This can be useful if this connection is under a bridge.



Figure 4.13: Internet Protocol Settings – No IP address

Obtain an IP address automatically A LAN connection can be configured to obtain an IP address automatically. You should only change this configuration in case your service provider requires it.

The server that assigns the GlobeSurfer 3G with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the *Override subnet mask* and specifying your own mask instead.

Use the following IP address The LAN connection is usually configured using a permanent (static) IP address. Your service provider should provide you with this address and subnet mask.

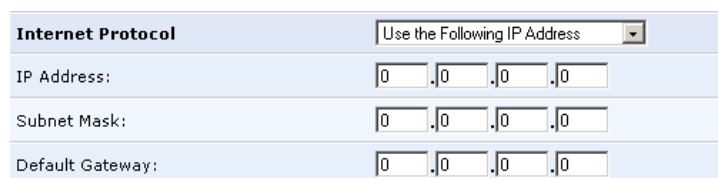
A screenshot of a configuration window titled "Internet Protocol". The dropdown menu is set to "Use the Following IP Address". Below the dropdown, there are three rows of input fields: "IP Address:" with four boxes containing "0", ".0", ".0", ".0"; "Subnet Mask:" with four boxes containing "0", ".0", ".0", ".0"; and "Default Gateway:" with four boxes containing "0", ".0", ".0", ".0".

Figure 4.14: Internet Protocol Settings – Static IP

4.2.3 DNS Server

Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP.

To configure the connection to automatically obtain a DNS server address, select *Obtain DNS Server Address Automatically* from the *DNS Server* drop down menu.

DNS Server	Obtain DNS Server Address Automatically ▾
-------------------	---

Figure 4.15: Automatic DNS Settings

To manually configure DNS server addresses, select *Use the following DNS server addresses* from the *DNS server* drop down menu (see figure 4.100). Specify up to two different DNS server addresses, one primary and one secondary.

DNS Server	Use the Following DNS Server Addresses ▾
Primary DNS Server:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS Server:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Figure 4.16: DNS Settings

To learn more about this feature, refer to Section 6.2.

4.2.4 DHCP

The *DHCP* section allows you to configure the Dynamic Host Configuration Protocol (DHCP) server parameters of the GlobeSurfer 3G. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure every network PC as *DHCP Client*.

IP Address Distribution	DHCP Server ▾
Start IP Address:	<input type="text"/> 192. <input type="text"/> 168. <input type="text"/> 3. <input type="text"/> 1
End IP Address:	<input type="text"/> 192. <input type="text"/> 168. <input type="text"/> 3. <input type="text"/> 244
Subnet Mask:	<input type="text"/> 255. <input type="text"/> 255. <input type="text"/> 255. <input type="text"/> 0
WINS Server IP Address:	<input type="text"/> 0. <input type="text"/> 0. <input type="text"/> 0. <input type="text"/> 0
Lease Time In Minutes:	<input type="text"/> 60
<input checked="" type="checkbox"/> Provide Host Name If Not Specified by Client	

Figure 4.17: IP Address Distribution

Select one of the following options from the *DHCP* drop down menu:

- DHCP server

Start IP address Specify the IP address from which the gateway starts issuing addresses. Since the gateway's default IP address is 192.168.1.1, the *Start IP address* must be 192.168.1.2 or greater.

End IP address Specify the end of the IP address range that can be used to automatically issue IP addresses.

Subnet mask The subnet mask determines which portion of a destination LAN IP address is the network portion, and which portion is the host portion.

WINS server IP address If you use a Windows Internet Naming Service (WINS), specify the WINS server address in this field.

Lease time in minutes This is duration of time a network user will be allowed connection to the gateway with its currently issued dynamic IP address. Just before the time is up, the user will automatically request to extend the lease or get a new IP address.

Provide host name if not specified by client Mark this check box if you want the gateway to automatically assign network PCs with a host name, in case a host name is not provided by the user.

IP Address Distribution	DHCP Server
Start IP Address:	192 .168 .1 .1
End IP Address:	192 .168 .1 .254
Subnet Mask:	255 .255 .255 .0
WINS Server IP Address:	0 .0 .0 .0
Lease Time In Minutes:	60
<input checked="" type="checkbox"/> Provide Host Name If Not Specified by Client	

Figure 4.18: IP Address Distribution - DHCP Server

- DHCP relay

Your gateway can act as a DHCP relay, if you require receiving a dynamically assigned IP address from a DHCP server other than your gateway's DHCP server.

1. After selecting *DHCP relay* from the drop down menu, a *New IP address* link will appear.

IP Address Distribution	DHCP Relay	New IP Address
--------------------------------	------------	--------------------------------

Figure 4.19: IP Address Distribution - DHCP Relay

Click the *New IP address* link. The *DHCP Relay server address* screen will appear:

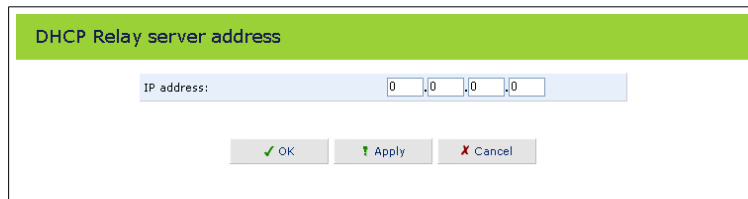


Figure 4.20: IP Address Distribution - DHCP Server Definition

2. Specify the IP address of the DHCP server.
3. Click *OK* to save the setting.

- **Disabled**
Select *Disabled* from the drop down menu if you want to statically assign IP addresses to your network computers.



Figure 4.21: IP Address Distribution - Disable DHCP

Click *OK* to save the setting.

4.2.5 Routing

You can choose to setup your GlobeSurfer 3G to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

Routing Select *Advanced* or *Basic* routing.

Device Metric The device metric is a value used by the GlobeSurfer 3G to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

- Listen to RIP messages - select *None*, *RIPv1*, *RIPv2* or *RIPv1/2*.
- Send RIP messages - select *None*, *RIPv1*, *RIPv2-broadcast* or *RIPv2-multicast*.




Routing Advanced ▾						
Routing mode:	Route					
Device metric:	<input type="text" value="4"/>					
<input type="checkbox"/> Default route						
<input checked="" type="checkbox"/> Multicast - IGMP proxy internal						
<input type="checkbox"/> Routing Information Protocol (RIP)						
Routing table						
Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Wireless	192.168.22.3	192.168.2.1	255.255.255.255	0	Applied	 
New route >>						
Internet connection firewall		<input type="checkbox"/> Enabled				

Figure 4.22: Advanced Routing Properties

To learn more about this feature, refer to Section 6.7.

4.2.6 Additional Network Connection Settings

The bottom part of the configuration screen displays the following options:

Internet connection firewall Select this check box to enable the GlobeSurfer 3G firewall on the connection. To learn more about configuring security settings, please refer to Chapter 5.




Internet Connection Firewall	<input type="checkbox"/> Enabled	
Allow Unrestricted Administration	<input type="checkbox"/> Enabled	
Additional IP Addresses	New IP Address	
IPv6		
Link Local Address:	fe80::16f8:52ff:fe0b:7514 / 10	
6to4 Address:	2002:c0a8:416f:3:16f8:52ff:fe0b:7514 / 64	
Unicast Addresses		
Address	Use MAC Address for Interface ID	Action
fec0::2:16f8:52ff:fe0b:7514 / 64	Yes	 
New Unicast Address >>		

Figure 4.23: Additional Network Connection Parameters

4.3 LAN Wireless Connection

This section begins with basic instructions to quickly and easily configure your wireless network, and continues with advanced settings options.

4.3.1 Configuring Your Wireless Network

As soon as GlobeSurfer 3G is active, your wireless network is available. This section will familiarize you with GlobeSurfer 3G's wireless configuration, and demonstrate how to connect a wireless PC to the network.

4.3.1.1 Configuring your GlobeSurfer 3G Wireless Connection

GlobeSurfer 3G will automatically set up a wireless connection as a bridged LAN network device.

1. Click the *Network Connections* icon on the sidebar, the *Network Connections* screen will appear (see figure 4.33).



Figure 4.24: Network Connections

2. Click the LAN wireless connection link (or its *Edit* icon) to view its properties. The *LAN Wireless Properties* screen will appear (see figure 4.34).

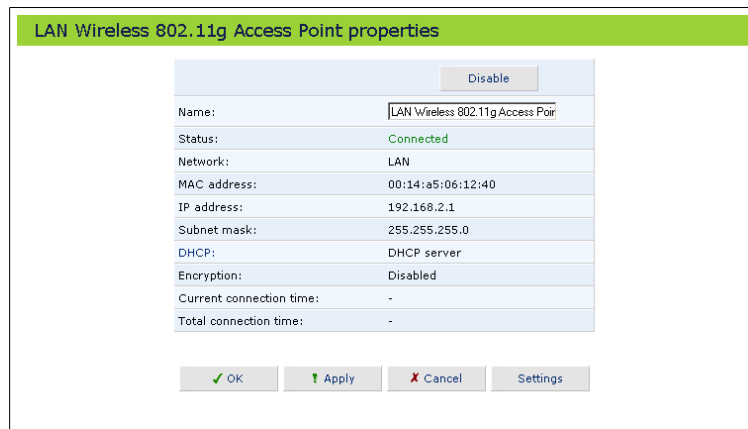


Figure 4.25: LAN Wireless Properties

3. Click the *Settings* button to display the various wireless connection settings. The *Configure LAN Wireless* screen will appear (see figure 4.35).

Configure LAN Wireless	
General	
Device name:	ra0
Status:	Connected (no IP address assigned)
Schedule:	Always New
Physical address:	00 14 55 06 10 15
MTU:	Automatic 1500
Wireless access point	
Name of WLAN network (SSID):	GlobeSurfer
<input checked="" type="checkbox"/> SSID broadcast	
802.11 mode:	802.11b/g mixed
Channel:	11 - 2.462 GHz
Network authentication:	Open System authentication
MAC filtering mode:	Disable
MAC filtering settings	New MAC address >>
Advanced wireless options	
Transmission rate:	Auto
CTS protection mode:	None
Beacon interval:	100 ms
DTIM interval:	1 ms
Fragmentation threshold:	2346
RTS threshold:	2346
Wireless security	
<input type="checkbox"/> Enabled	
Internet protocol	
<input type="checkbox"/> No IP address	
Internet connection firewall	
<input type="checkbox"/> Enabled	
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 4.26: Configure LAN Wireless

4. In the *SSID* field, change the broadcasted name of your wireless network from the default to a more unique name. Click *OK*, then click *OK* again on the properties screen to save your changes.

A comprehensive description of all the wireless connection settings in the configuration screen is available in section 4.3.3.

4.3.1.2 Configuring Your Wireless Windows XP Client

If your PC has wireless capabilities, Windows XP will automatically recognize this and create a wireless connection for you. You can view this connection under Window's Network Connections.

Note: The following descriptions and images are in accordance with Microsoft Windows XP, Version 2002, running Service Pack 2.

1. Open your Network Connections window from Windows Control Panel (see figure 4.38).



Figure 4.27: Network Connections

2. Double-click the wireless connection icon. The *Wireless Network Connection* screen will appear, displaying all available wireless networks in your vicinity. If your gateway is connected and active, you will see GlobeSurfer 3G's wireless connection (see figure 4.28). Note that the connection's status is *Not connected* and defined as "Unsecured wireless network".

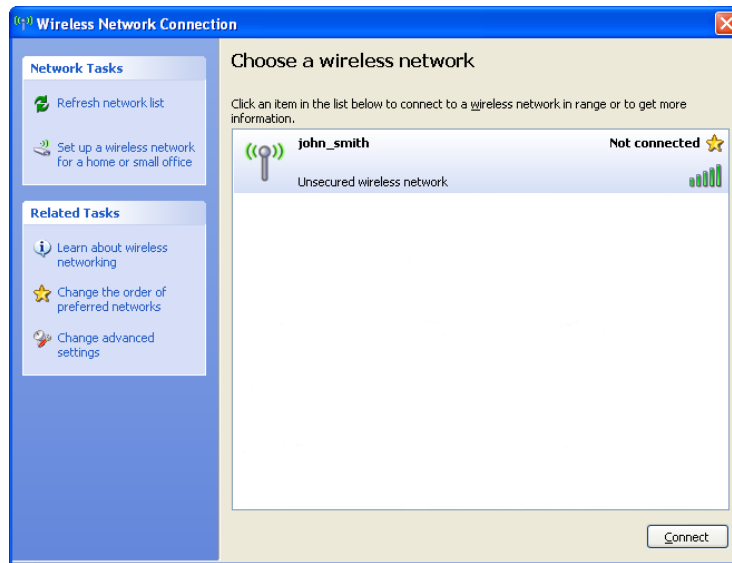


Figure 4.28: Available Wireless Connections

3. Select the wireless network name (SSID) that you configured in the *Configure LAN Wireless* screen (see figure 4.35) as your wireless network. Select the *Enable IEEE 802.1x authentication for this network* check box to enable authenticated communication between the PC and the GlobeSurfer 3G. If you choose to enable 802.1x, you must also configure the GlobeSurfer 3G accordingly.
4. Click the *Advanced* button, the *Wireless network properties* screen will appear (see figure 4.29).

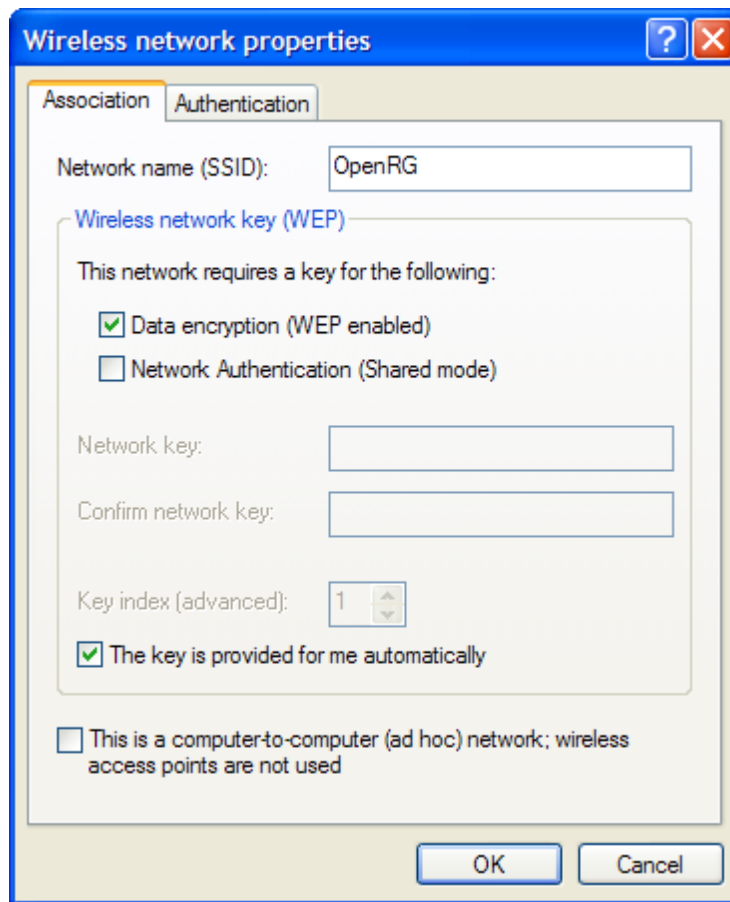


Figure 4.29: Wireless Connection Association

5. Select the *Data Encryption (WEP)* check box to encrypt the Wireless data transmitted between GlobeSurfer 3G and your Wireless device.
6. Select the *Authentication* tab to configure wireless authentication protocols (see figure 4.30). When selecting an *EAP Type* authentication method, make sure that your GlobeSurfer 3G is configured accordingly.

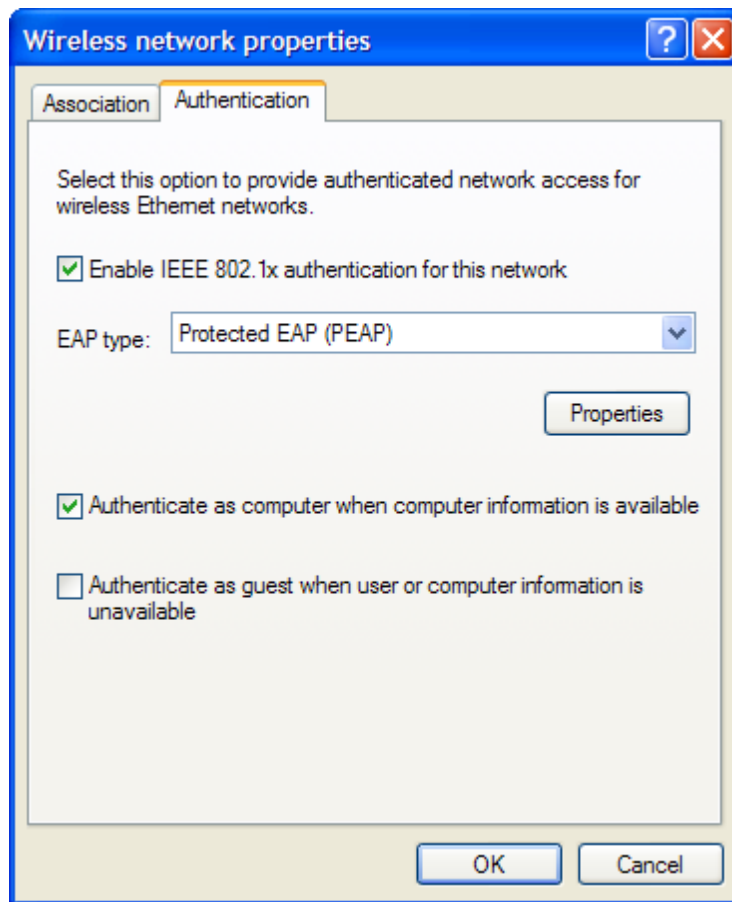


Figure 4.30: Wireless Connection Authentication

7. Click the connection once to mark it and then click the *Connect* button at the bottom of the screen. After the connection is established, its status will change to *Connected*:

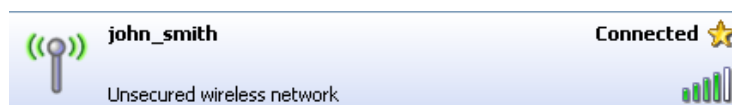


Figure 4.31: Connected Wireless Network

An icon will appear in the notification area, announcing the successful initiation of the wireless connection (see figure 4.42).

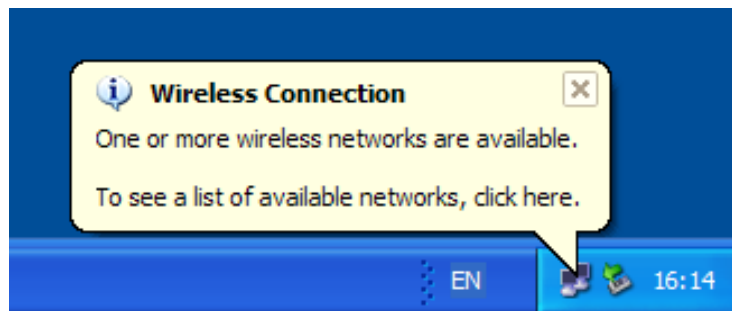


Figure 4.32: Wireless Connection Information

8. Test the connection by disabling all other connections in the Network Connections window (see figure 4.38) and browsing the Internet.

You can now use GlobeSurfer 3G's wireless network from the configured PC. However, so can any other user with a wireless PC, which happens to be in your network's radio range. To prevent this scenario, the next step is to secure your wireless network, allowing only specific users to connect.

4.3.2 Securing Your Wireless Network

The GlobeSurfer 3G wireless network is ready for operation with its default values. However, as soon as your wireless connection is established, any computer with a wireless capability can connect to your LAN. The following section describes how to secure your wireless connection using the **Wi-Fi Protected Access** (WPA) security protocol.

The Wi-Fi Alliance created the WPA security protocol as a data encryption method for 802.11 wireless local area networks (WLANs). WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of Wired Equivalent Privacy (WEP), including the use of dynamic keys.

4.3.2.1 Securing Your Wireless Network with WPA

1. Click the *Network Connections* icon on the sidebar, the *Network Connections* screen will appear (see figure 4.33).

□

Figure 4.33: Network Connections

2. Click the LAN wireless connection link (or its *Edit* icon) to view its properties. The *LAN Wireless Properties* screen will appear (see figure 4.34).

LAN Wireless 802.11g Access Point properties	
<input type="button" value="Disable"/>	
Name:	LAN Wireless 802.11g Access Point
Status:	Connected
Network:	LAN
MAC address:	00:14:a5:06:12:40
IP address:	192.168.2.1
Subnet mask:	255.255.255.0
DHCP:	DHCP server
Encryption:	Disabled
Current connection time:	-
Total connection time:	-
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Settings"/>	

Figure 4.34: LAN Wireless Properties

3. Click the *Settings* button to display the various wireless connection settings. The *Configure LAN Wireless* screen will appear (see figure 4.35).

Configure LAN Wireless	
General	
Device name:	ra0
Status:	Connected (no IP address assigned)
Schedule:	Always New
Physical address:	00 14 a5 06 12 40
MTU:	Automatic 1500
Wireless access point	
Name of WLAN network (SSID):	GlobeSurfer
<input checked="" type="checkbox"/> SSID broadcast	
802.11 mode:	802.11b/g mixed
Channel:	11 - 2.462 GHz
Network authentication:	Open System authentication
MAC filtering mode:	Disable
MAC filtering settings	New MAC address >>
Advanced wireless options	
Transmission rate:	Auto
CTS protection mode:	None
Beacon interval:	100 ms
DTIM interval:	1 ms
Fragmentation threshold:	2346
RTS threshold:	2346
Wireless security	<input type="checkbox"/> Enabled
Internet protocol	No IP address
Internet connection firewall	<input type="checkbox"/> Enabled
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 4.35: Configure LAN Wireless

4. Enable the *Wireless security* feature by checking its *Enabled* check box.

The screen will refresh, displaying the wireless security options (see figure 4.50).

5. Verify that the *Stations security type* is set to *Accept WPA stations*.
6. Verify that the *Authentication method* selected is *Pre-Shared key*.
7. Enter a phrase of at least 8 characters in the *Pre-Shared key* text field. Verify that *ASCII* is selected in the associated combo box

Wireless Security	<input checked="" type="checkbox"/> Enabled
<input checked="" type="checkbox"/> Accept WPA Stations	
Authentication Method:	Pre-Shared Key ▾
Pre-Shared Key:	garfield ASCII ▾
Encryption Algorithm:	TKIP
<input type="checkbox"/> Accept 802.1X WEP Stations	
<input checked="" type="checkbox"/> Group Key Update Interval:	900 Seconds
<input type="checkbox"/> Accept Non-802.1X WEP Stations	

Figure 4.36: LAN Wireless Security Parameters

8. Click *OK*. An *Attention* screen will appear warning you that the browser page might require reloading.

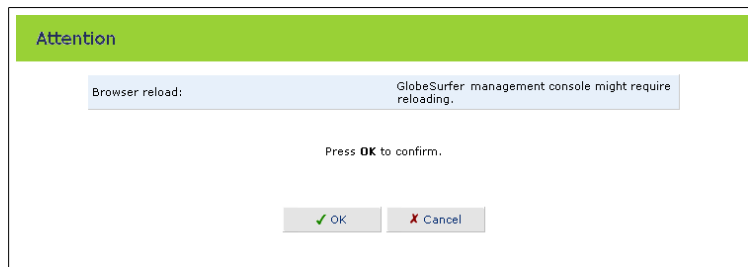


Figure 4.37: Browser Reload Warning

9. Click *OK* to save the changes.

Make the corresponding settings on your Windows PC Client as described below.

4.3.2.2 Connecting a Wireless Windows XP Client to the Secured Wireless Network

1. Open your Network Connections window from Window's Control Panel (see figure 4.38).



Figure 4.38: Network Connections

2. Double-click the wireless connection icon. The *Wireless Network Connection* screen will appear, displaying GlobeSurfer 3G's wireless connection (see figure 4.39). Note that the connection is defined as "Security-enabled wireless network (WPA)".

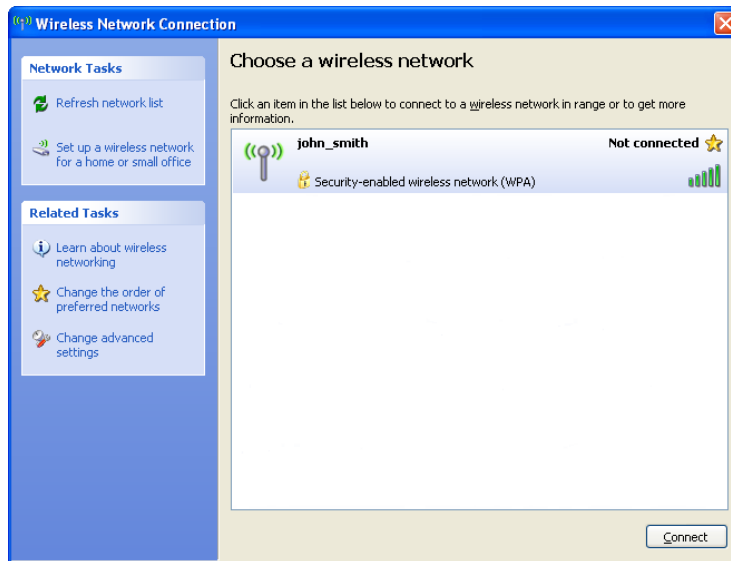


Figure 4.39: Available Wireless Connections

3. Click the connection once to mark it and then click the *Connect* button at the bottom of the screen. The following login window will appear, asking for a *Network Key*, which is the pre-shared key you have configured above.



Figure 4.40: Wireless Network Connection Login

4. Enter the pre-shared key in both fields and click the *Connect* button. After the connection is established, its status will change to *Connected*:

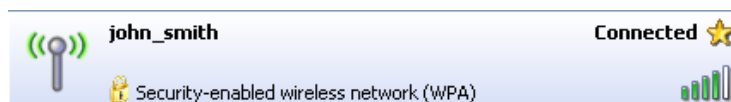


Figure 4.41: Connected Wireless Network

An icon will appear in the notification area, announcing the successful initiation of the wireless connection (see figure 4.42).

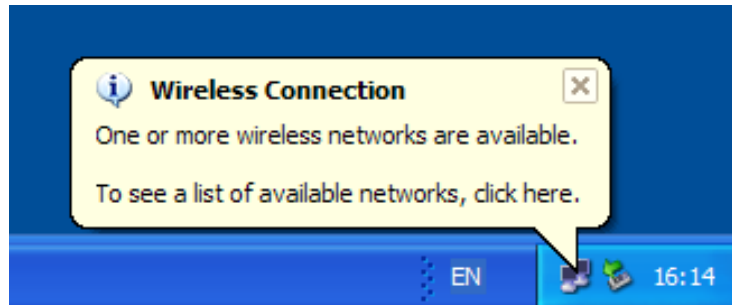


Figure 4.42: Wireless Connection Information

5. Test the connection by disabling all other connections in the Network Connections window (see figure 4.38) and browsing the Internet.

Should the login window above not appear and the connection attempt fail, please configure Window's connection manually:

1. Click the connection once to mark it and then click the *Change advanced settings* link in the *Related Tasks* box on the left part of the window (see figure 4.43).

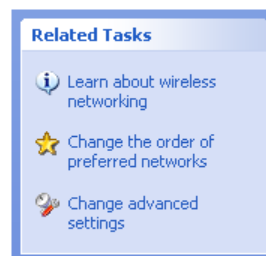


Figure 4.43: Related Tasks

2. The *Wireless Network Connection Properties* window will appear. Select the *Wireless Networks* tab (see figure 4.44).

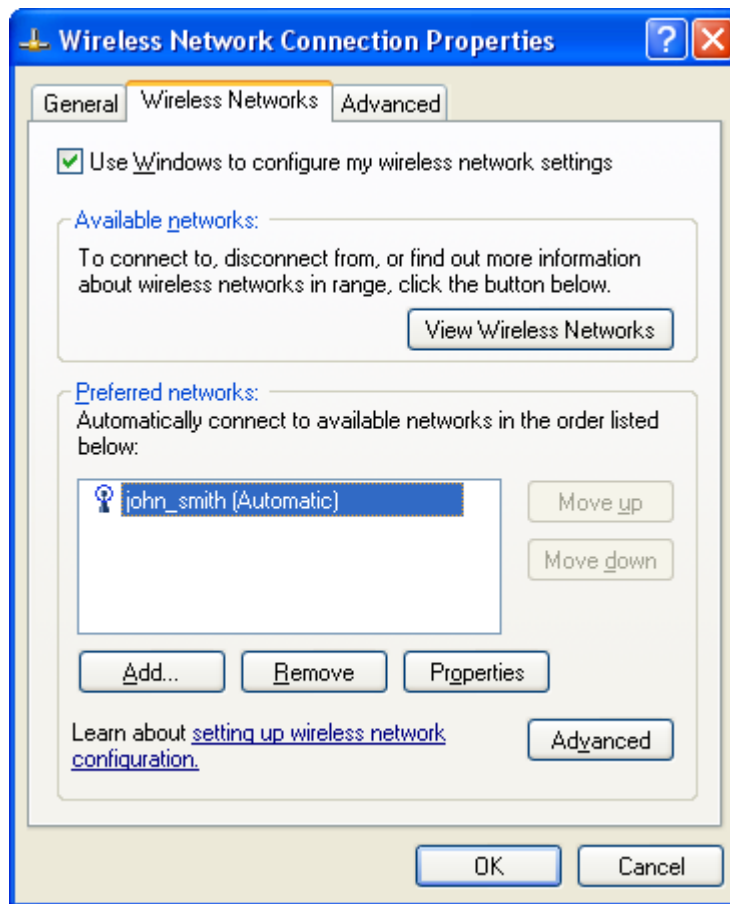


Figure 4.44: Wireless Network Connection Properties

3. Click your connection to highlight it and then click the *Properties* button. Your connection's properties window will appear (see figure 4.45).

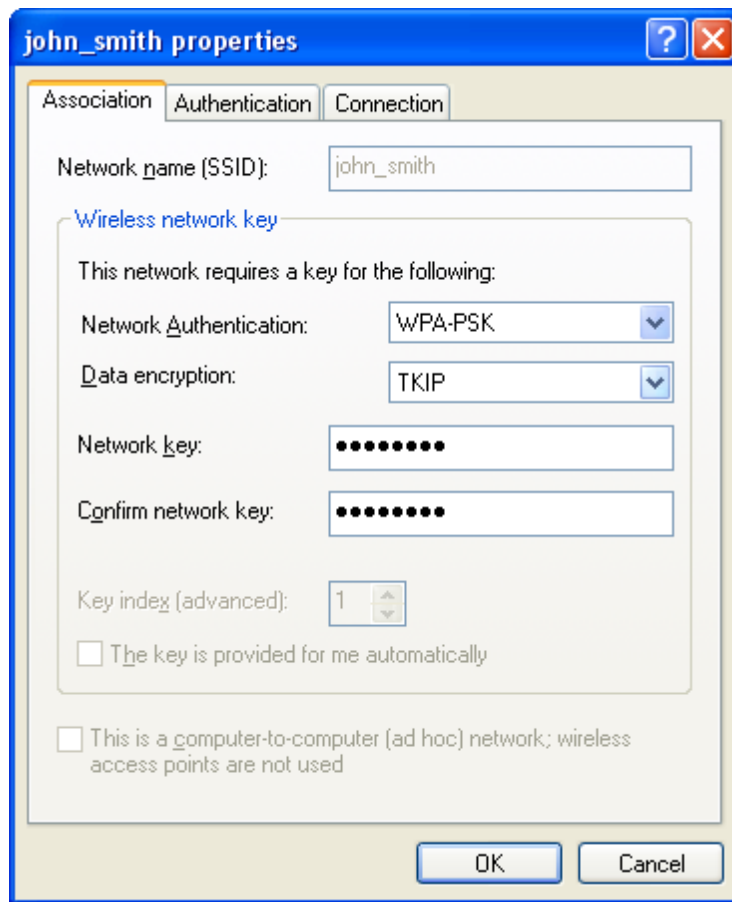


Figure 4.45

Connection Properties Configuration

- In the *Network Authentication* combo box, select "WPA-PSK".
 - In the *Data Encryption* combo box, select "TKIP".
 - Enter your pre-shared key in both the *Network key* and the *Confirm network key* fields.
4. Click OK on both windows to save the settings.
 5. When attempting to connect to the wireless network, the login window will now appear, pre-filled with the pre-shared key. Click the *Connect* button to connect.

Since your network is now secured, only users that know the pre-shared key will be able to connect. The WPA security protocol is similar to securing network access using a password.

4.3.3 Advanced Wireless Connection Settings

The following sections describe how to configure the advanced settings of your wireless connection, which is only recommended for advanced users. These settings are accessible from the *Configure LAN Wireless* screen (see figure 4.35).

4.3.3.1 General Network Connection Parameters

The top part of the configuration window displays general communication parameters. It is recommended not to change the default values in this screen unless you are familiar with the networking concepts they represent. Since your GlobeSurfer 3G is configured to operate with the default values, no parameter modification is necessary. You can configure the following general connection settings:

Schedule You can configure scheduler rules in order to define time segments during which the connection is active. To configure scheduler rules click the *New* link. To learn how to configure scheduler rules please refer to Section 6.11.

Physical Address The physical address of the network card used for your network. Some cards allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The setting *Manual*, allows you to enter the largest packet size that will be transmitted. To have the GlobeSurfer 3G select the best MTU for your Internet connection, select *Automatic*.

General	
Device name:	ra0
Status:	Connected (no IP address assigned)
Schedule:	Always New
Connection type:	Wireless
Physical address:	00 :14 :a5 :06 :12 :40
MTU:	Automatic 1500

Figure 4.46: LAN Wireless General Connection Parameters

4.3.3.2 Wireless Access Point

SSID The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (*my-wlan*) to a unique name.

SSID broadcast Select this checkbox to enable broadcasting of the SSID. Disabling SSID broadcast is used in order to hide the name of the wireless device from clients that should not be aware of its existence.

802.11 Mode Select the wireless communication standard that is compatible with your PC's wireless card. You can work in either 802.11g, 802.11b or in mixed mode.

Channel Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly.

Network authentication Select *Open System Authentication* or *Shared Key Authentication*.

Wireless access point	
Name of WLAN network (SSID):	surfhome
<input checked="" type="checkbox"/> SSID broadcast	
802.11 mode:	802.11b/g mixed
Channel:	11 - 2.462 GHz
Network authentication:	Open System authentication

Figure 4.47: LAN Wireless Access Point Parameters

4.3.3.3 MAC filtering settings

MAC filtering mode A common method of restricting WLAN network access is to specify the Media Access Control (MAC) address of computers that are allowed or denied access to your network. Every WLAN network adapter is identified by a unique MAC address. The GlobeSurfer 3G supports MAC filtering based on either a list of denied or allowed computers. MAC filtering mode *Allow* specifies that the list of MAC addresses is granted access to GlobeSurfer 3G. MAC filtering mode *Deny* specifies that all computers except those in the list of MAC addresses are granted access to GlobeSurfer 3G. Select *Disable* if you want to disable MAC filtering.

MAC filtering settings Click the *New MAC address* link to define MAC addresses to filter. The selected MAC filtering mode will be performed on the corresponding network adapters.

MAC filtering mode:	Allow
MAC filtering settings	New MAC address

Figure 4.48: LAN Wireless MAC Filtering Settings

4.3.3.4 Advanced Wireless Options

Transmission rate The transmission rate is set according to the speed of your wireless connection. Select the transmission rate from the drop down list, or select *Auto* to have GlobeSurfer 3G automatically use the fastest possible data transmission rate.

CTS protection mode CTS protection mode boosts your gateway's ability to intercept Wireless-G and 802.11b transmissions. Conversely, CTS protection mode decreases performance. Leave this feature disabled unless you

encounter severe communication difficulties between the GlobeSurfer 3G and Wireless-G products.

Beacon interval A beacon is a packet broadcast by GlobeSurfer 3G to synchronize the wireless network. The beacon interval value indicates how often the beacon is sent.

DTIM interval The Delivery Traffic Indication Message (DTIM) is a count-down value that informs wireless clients of the next opportunity to receive multicast and broadcast messages. This value ranges between 1 and 16384.

Fragmentation threshold Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.

RTS threshold GlobeSurfer 3G sends Request to Send (RTS) packets to the wireless client in order to negotiate the dispatching of data. The wireless client responds with a Clear to Send (CTS) packet, signaling that transmission can commence. In case packets are smaller than the pre-set threshold, the RTS/CTS mechanism is not active. If you encounter inconsistent data flow, try a minor reduction of the RTS threshold size.

Advanced wireless options	
Transmission rate:	Auto
CTS protection mode:	None
Beacon interval:	100 ms
DTIM interval:	1 ms
Fragmentation threshold:	2346
RTS threshold:	2346

Figure 4.49: LAN Wireless Access Point Advanced Parameters

4.3.3.5 Wireless Security

To configure your wireless security, select the *Enabled* check-box on the *Configure LAN Wireless* screen (see figure 4.35). The screen will refresh, displaying the wireless security options (see figure 4.50). Click *Apply* to save this change.

Stations security type Select *Accept WPA stations* to allow wireless clients that use WPA to communicate with the gateway. Select *Accept 802.1X WEP stations* to allow wireless clients that use standard WEP to communicate with the gateway. Select *Accept Non-802.1X WEP stations* to allow wireless clients that use non-standard WEP to communicate with the gateway.

Authentication method Select the authentication method you would like to use from the *Authentication method* combo box. Choose between *Pre-Shared key* and *802.1x*.

Pre-Shared key This entry appears only if you had selected this authentication method. Enter your encryption key in the *Pre-Shared key* field. You can use either an ASCII or a Hex value by selecting the value type in the combo box provided.

Encryption algorithm Select whether to use *TKIP* or *AES* for encryption.

Group key update interval Define the time interval in seconds for updating a group key.

The screenshot shows a configuration window for Wireless Security. At the top, there is a header 'Wireless Security' with a status indicator 'Enabled' and a checkmark. Below this, there are several rows of settings: 'Accept WPA Stations' is checked; 'Authentication Method' is set to 'Pre-Shared Key'; 'Pre-Shared Key' is 'garfield' with an 'ASCII' dropdown; 'Encryption Algorithm' is 'TKIP'; 'Accept 802.1X WEP Stations' is unchecked; 'Group Key Update Interval' is '900' seconds and is checked; and 'Accept Non-802.1X WEP Stations' is unchecked.

Figure 4.50: LAN Wireless Security Parameters

4.3.3.6 Internet Protocol

Select one of the following Internet protocol options from the *Internet protocol* drop down menu:

- No IP address
- Obtain an IP address automatically
- Use the following IP address

Please note that according to the selection you make in the *Internet protocol* drop down menu, the screen will refresh and display relevant configuration settings.

No IP address Select *No IP address* if you require that this connection will have no IP address. This can be useful if this connection is under a bridge.

The screenshot shows a dropdown menu for 'Internet Protocol' with 'No IP Address' selected.

Figure 4.51: Internet Protocol Settings – No IP address

Obtain an IP address automatically A LAN connection can be configured to obtain an IP address automatically. You should only change this configuration in case your service provider requires it.

The server that assigns the GlobeSurfer 3G with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the *Override subnet mask* and specifying your own mask instead.

Use the following IP address The LAN connection is usually configured using a permanent (static) IP address. Your service provider should provide you with this address and subnet mask.

Internet Protocol	Use the Following IP Address
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0

Figure 4.52: Internet Protocol Settings – Static IP

4.3.3.7 Additional Network Connection Settings

The bottom part of the configuration screen displays the following options:

Internet connection firewall Select this check box to enable the GlobeSurfer 3G firewall on the connection. To learn more about configuring security settings, please refer to Chapter 5.




Internet Connection Firewall	<input type="checkbox"/> Enabled	
Allow Unrestricted Administration	<input type="checkbox"/> Enabled	
Additional IP Addresses	New IP Address	
IPv6		
Link Local Address:	fe80::16f8:52ff:fe0b:7514 / 10	
6to4 Address:	2002:c0a8:416f:3:16f8:52ff:fe0b:7514 / 64	
Unicast Addresses		
Address	Use MAC Address for Interface ID	Action
fec0::2:16f8:52ff:fe0b:7514 / 64	Yes	 
New Unicast Address >>		

Figure 4.53: Additional Network Connection Parameters

4.4 LAN Bridge Connection

The LAN bridge connection is used to combine several LAN devices under one virtual network. For example, creating one network for LAN Ethernet and LAN wireless devices.

Please note, that when a bridge is removed, its formerly underlying devices inherit the bridge's DHCP settings. For example, the removal of a bridge that is configured as DHCP client, automatically configures the LAN devices formerly constituting the bridge as DHCP clients, with the exact DHCP client configuration.

LAN Bridge Properties	
<input type="button" value="Disable"/>	
Name:	LAN Bridge
Device name:	br0
Status:	Connected
Network:	LAN
Underlying device:	LAN Ethernet LAN Wireless 802.11g Access Point
Connection type:	Bridge
MAC address:	00:09:8c:00:40:4c
IP address:	192.168.1.1
Subnet mask:	255.255.255.0
DHCP:	DHCP server
Current connection time:	-
Total connection time:	-

Figure 4.54: General Bridge Settings

4.4.1 General Network Connection Parameters

The top part of the configuration window displays general communication parameters. It is recommended not to change the default values in this screen unless you are familiar with the networking concepts they represent. Since your GlobeSurfer 3G is configured to operate with the default values, no parameter modification is necessary. You can configure the following general connection settings:

Physical Address The physical address of the network card used for your network. Some cards allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The setting *Manual*, allows you to enter the largest packet size that will be transmitted. To have the GlobeSurfer 3G select the best MTU for your Internet connection, select *Automatic*.

General	
Device Name:	br0
Status:	Connected
Schedule:	Always New
Network:	LAN
Connection Type:	Bridge
Physical Address:	16 :a9 :a2 :57 :b3 :41
MTU:	Automatic 1500

Figure 4.55: General Bridge Settings

4.4.2 Internet Protocol

Select one of the following Internet protocol options from the *Internet protocol* drop down menu:

- No IP address
- Obtain an IP address automatically
- Use the following IP address

Please note that according to the selection you make in the *Internet protocol* drop down menu, the screen will refresh and display relevant configuration settings.

No IP address Select *No IP address* if you require that this connection will have no IP address. This can be useful if this connection is under a bridge.

Internet Protocol
No IP Address

Figure 4.56: Internet Protocol Settings – No IP address

Obtain an IP address automatically A LAN connection can be configured to obtain an IP address automatically. You should only change this configuration in case your service provider requires it.

The server that assigns the GlobeSurfer 3G with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the *Override subnet mask* and specifying your own mask instead.

Use the following IP address The LAN connection is usually configured using a permanent (static) IP address. Your service provider should provide you with this address and subnet mask.

Internet Protocol	
Use the Following IP Address	
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0

Figure 4.57: Internet Protocol Settings – Static IP

4.4.3 Bridge Settings

The bridge section allows you to specify the LAN devices that you would like to join under the network bridge. Click the *Edit* icon on the VLAN column to assign the network connections to specific Virtual LANs.

Select the *STP* check box to enable the Spanning Tree Protocol on the device. You should use this to ensure that there are no loops in your network configuration, and apply these settings in case your network consists of multiple switches, or other bridges apart from those created by the GlobeSurfer 3G.

Bridge					
Name	VLANs	Status	STP	Action	
LAN Bridge	Disabled	Connected	<input type="checkbox"/>		
<input checked="" type="checkbox"/> LAN Ethernet	Disabled	Connected (No IP Address Assigned)	<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> LAN USB	Disabled	Disconnected	<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/> LAN Wireless 802.11g Access Point	Disabled	Device missing	<input checked="" type="checkbox"/>		

Figure 4.58: LAN Bridge Settings

4.4.4 DNS Server

Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP.

To configure the connection to automatically obtain a DNS server address, select *Obtain DNS Server Address Automatically* from the *DNS Server* drop down menu.

DNS Server: Obtain DNS Server Address Automatically

Figure 4.59: Automatic DNS Settings

To manually configure DNS server addresses, select *Use the following DNS server addresses* from the *DNS server* drop down menu (see figure 4.100). Specify up to two different DNS server addresses, one primary and one secondary.

DNS Server: Use the Following DNS Server Addresses

Primary DNS Server: [] . [] . [] . []

Secondary DNS Server: [] . [] . [] . []

Figure 4.60: DNS Settings

To learn more about this feature, refer to Section 6.2.

4.4.5 DHCP

The *DHCP* section allows you to configure the Dynamic Host Configuration Protocol (DHCP) server parameters of the GlobeSurfer 3G. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure every network PC as *DHCP Client*.

IP Address Distribution	DHCP Server
Start IP Address:	192 .168 .3 .1
End IP Address:	192 .168 .3 .244
Subnet Mask:	255 .255 .255 .0
WINS Server IP Address:	0 .0 .0 .0
Lease Time In Minutes:	60
<input checked="" type="checkbox"/> Provide Host Name If Not Specified by Client	

Figure 4.61: IP Address Distribution

Select one of the following options from the *DHCP* drop down menu:

- DHCP server

Start IP address Specify the IP address from which the gateway starts issuing addresses. Since the gateway's default IP address is 192.168.1.1, the *Start IP address* must be 192.168.1.2 or greater.

End IP address Specify the end of the IP address range that can be used to automatically issue IP addresses.

Subnet mask The subnet mask determines which portion of a destination LAN IP address is the network portion, and which portion is the host portion.

WINS server IP address If you use a Windows Internet Naming Service (WINS), specify the WINS server address in this field.

Lease time in minutes This is duration of time a network user will be allowed connection to the gateway with its currently issued dynamic IP address. Just before the time is up, the user will automatically request to extend the lease or get a new IP address.

Provide host name if not specified by client Mark this check box if you want the gateway to automatically assign network PCs with a host name, in case a host name is not provided by the user.

IP Address Distribution	DHCP Server
Start IP Address:	192 . 168 . 1 . 1
End IP Address:	192 . 168 . 1 . 254
Subnet Mask:	255 . 255 . 255 . 0
WINS Server IP Address:	0 . 0 . 0 . 0
Lease Time In Minutes:	60
<input checked="" type="checkbox"/> Provide Host Name If Not Specified by Client	

Figure 4.62: IP Address Distribution - DHCP Server

- DHCP relay
Your gateway can act as a DHCP relay, if you require receiving a dynamically assigned IP address from a DHCP server other than your gateway's DHCP server.
 1. After selecting *DHCP relay* from the drop down menu, a *New IP address* link will appear.

IP Address Distribution	DHCP Relay	New IP Address
--------------------------------	------------	--------------------------------

Figure 4.63: IP Address Distribution - DHCP Relay

Click the *New IP address* link. The *DHCP Relay server address* screen will appear:

DHCP Relay server address

IP address: 0 . 0 . 0 . 0

Figure 4.64: IP Address Distribution - DHCP Server Definition

2. Specify the IP address of the DHCP server.
 3. Click *OK* to save the setting.
- Disabled
Select *Disabled* from the drop down menu if you want to statically assign IP addresses to your network computers.

IP Address Distribution	Disabled
--------------------------------	----------

Figure 4.65: IP Address Distribution - Disable DHCP

Click *OK* to save the setting.

4.4.6 Routing

You can choose to setup your GlobeSurfer 3G to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

Routing Select *Advanced* or *Basic* routing.

Device metric The device metric is a value used by the GlobeSurfer 3G to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default route Select this check box to define this device as the default route.

Multicast - IGMP proxy internal IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of LAN devices asking to join multicast groups. Select the *Multicast IGMP proxy internal* check-box to enable this feature.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

- Listen to RIP messages - select *None*, *RIPv1*, *RIPv2* or *RIPv1/2*.
- Send RIP messages - select *None*, *RIPv1*, *RIPv2-broadcast* or *RIPv2-multicast*.

Routing table Allows you to add or modify routes when this device is active. Click the link to an existing route to edit it, or click *New route* to add a route.




Routing	Advanced					
Routing mode:	Route					
Device metric:	4					
<input type="checkbox"/> Default route						
<input checked="" type="checkbox"/> Multicast - IGMP proxy internal						
<input type="checkbox"/> Routing Information Protocol (RIP)						
Routing table						
Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Wireless	192.168.22.3	192.168.2.1	255.255.255.255	0	Applied	 
New route >>						
Internet connection firewall	<input type="checkbox"/> Enabled					

Figure 4.66: Advanced Routing Properties

To learn more about this feature, refer to Section 6.7.

4.4.7 Additional Network Connection Settings

The bottom part of the configuration screen displays the following options:

Internet connection firewall Select this check box to enable the GlobeSurfer 3G firewall on the connection. To learn more about configuring security settings, please refer to Chapter 5.




Internet Connection Firewall	<input type="checkbox"/> Enabled	
Allow Unrestricted Administration	<input type="checkbox"/> Enabled	
Additional IP Addresses	New IP Address	
IPv6		
Link Local Address:	fe80::16f8:52ff:fe0b:7514 / 10	
6to4 Address:	2002:c0a8:416f:3:16f8:52ff:fe0b:7514 / 64	
Unicast Addresses		
Address	Use MAC Address for Interface ID	Action
fec0::2:16f8:52ff:fe0b:7514 / 64	Yes	 
New Unicast Address >>		

Figure 4.67: Additional Network Connection Parameters

4.5 VPN PPTP

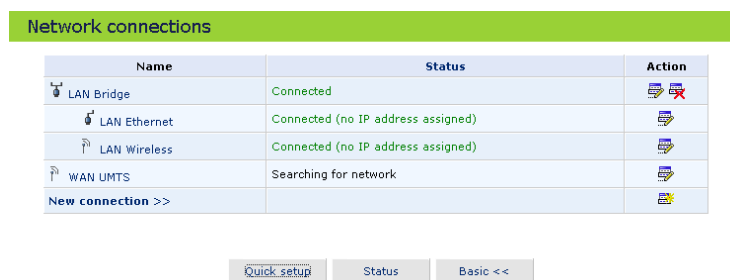
Point-to-Point Tunneling Protocol (PPTP) is a protocol developed by Microsoft targeted at creating VPN connections over the Internet. This enables remote users to access the gateway via any ISP that supports PPTP on its servers. PPTP encapsulates network traffic, encrypts content using Microsoft's Point-to-Point Encryption (MPPE) protocol that is based on RC4, and routes using the generic routing encapsulation (GRE) protocol.

For more information on PPTP connections, refer to Section 6.13.2 for PPTP server settings and Section 6.13.3 for PPTP client settings.

4.5.1 Creating a PPTP Client Connection

To create a PPTP client connection, perform the following steps:

1. Click *Network connections* on the sidebar – the *Network connections* screen will appear (see figure 4.68).



The screenshot shows a window titled "Network connections" with a table of network connections. Below the table are three buttons: "Quick setup", "Status", and "Basic <<".







Name	Status	Action
LAN Bridge	Connected	 
LAN Ethernet	Connected (no IP address assigned)	
LAN Wireless	Connected (no IP address assigned)	
WAN UMTS	Searching for network	
New connection >>		

Figure 4.68: Network Connections

2. Click the *New connection* link to list the connection alternatives.

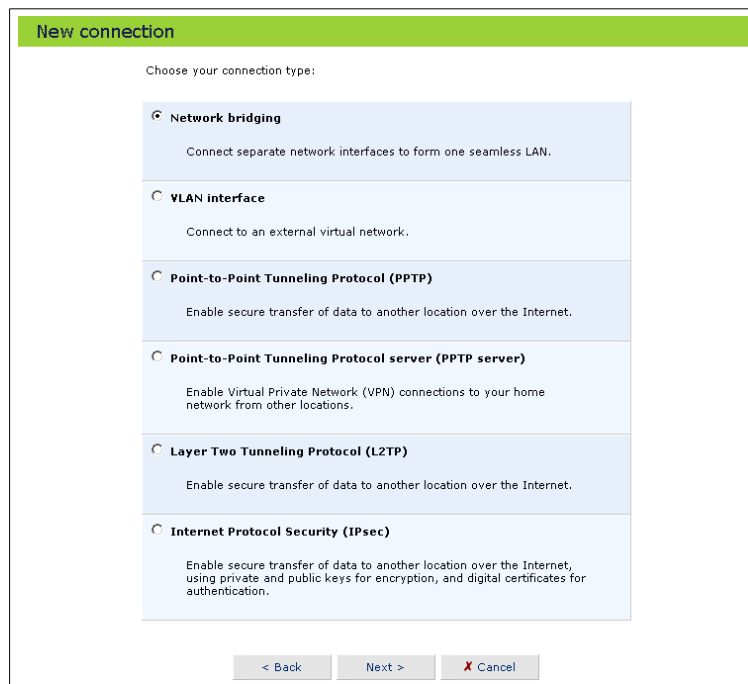


Figure 4.69: New Connection Alternatives

3. Select the *Point-to-Point Tunneling Protocol (PPTP)* radio button and click *Next*. The *Point-to-Point Tunneling Protocol (PPTP)* configuration screen will appear (see figure 4.70).

Enter the following parameters, supplied by your VPN server.

Hostname or IP address of destination Hostname or IP address of the VPN host server.

Login username Your username.

Login password Your password.

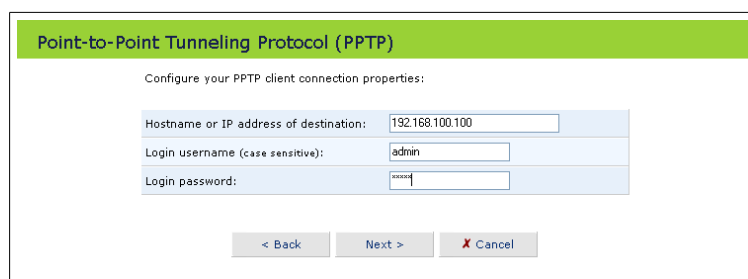


Figure 4.70: PPTP Connection Properties

Click *Next* when ready. The wizard will display a connection summary (see figure 4.77).

Click *Finish* to create your VPN PPTP client connection.

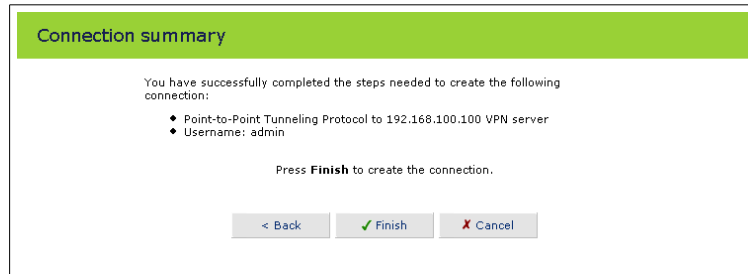


Figure 4.71: PPTP Client Connection Summary

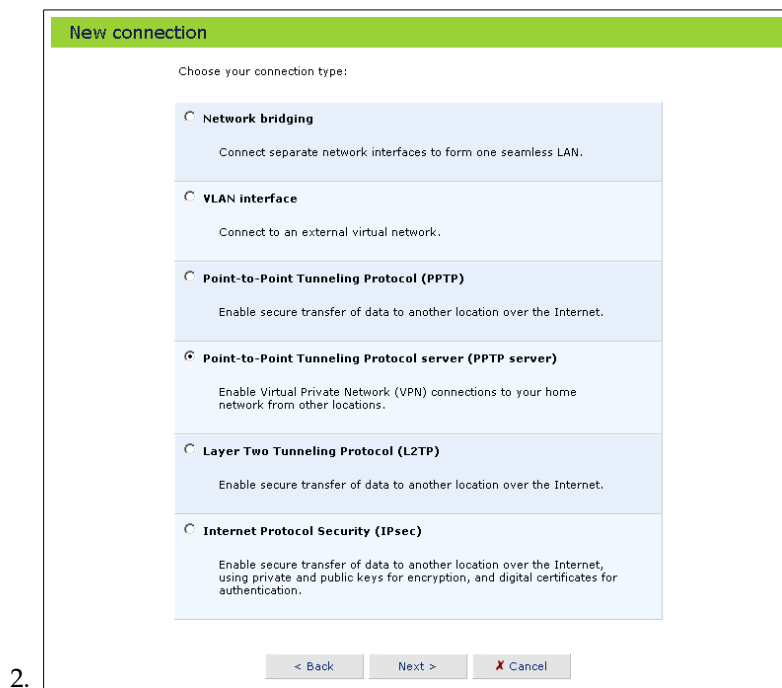
4.5.2 Creating a PPTP Server Connection

To create a PPTP server connection, perform the following steps:

1. Click *Network connections* on the sidebar – the *Network connections* screen will appear (see figure 4.72).

Figure 4.72: Network Connections

Click the *New connection* link to list the connection alternatives.

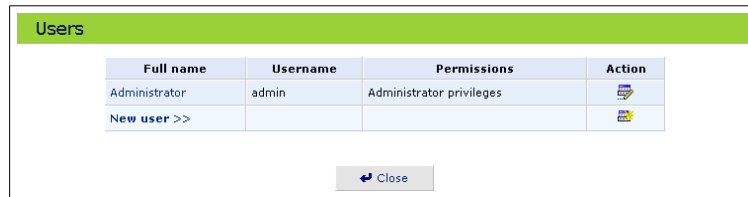




2.

Figure 4.73: New Connection Alternatives

-
3. Select the *Point-to-Point Tunneling Protocol Server (PPTP Server)* radio button and click *Next*.

Specify the users that will be authorized to access your VPN server (see figure 6.39).



Full name	Username	Permissions	Action
Administrator	admin	Administrator privileges	
New user >>			




Figure 4.74: User table

You can add, edit and delete users allowed to access the GlobeSurfer 3G and your local network by managing the user table as described in Section 2.5. To add a new user click *New user* in the table and specify the following parameters:

- **Full name:** The remote user's full name.
- **Username:** The name the remote user will use to access your local network.
- **New password:** Type a new password for the remote user. If you do not want to assign a password to the remote user leave this field empty.
- **Retype new password:** If a new password was assigned, type it again to verify correctness.
- **Permissions:** Select the remote user's privileges on your local network.
 - **Administrator privileges:** Grants remote system setting modification via the web-based management console or telnet.
 - **Remote access by PPTP:** Grants access with no system modification privileges.
 - **SMS access only:** Grants access to the SMS manager only, for example to send and read SMS messages. Other parts of the management console will be hidden and can not be accessed.

Figure 4.75: Managing Users

Please note, that changing any of the user parameters will prompt the connection associated with the user to terminate. For changes to take effect you should activate the connection manually after modifying user parameters.

You can use email notification to receive indications of system events for a predefined severity classification. The available types of events are *System* or *Security* events. The available severity of events are *Error*, *Warning* and *Information*. If the *Information* level is selected the user will receive notification of *Information*, *Warning* and *Error* events. If the *Warning* level is selected the user will receive notification of *Warning* and *Error* events etc.

To configure email notification for a specific user:

- First make sure you have configured an outgoing mail server in *System settings*. A click on the *Configure mail server* link will display the *System settings* screen where you can configure the outgoing mail server.
- Enter the user's email address in the *Address* field in the *Email* section.
- Select the *System* and *Security* notification levels in the *System notify level* and *Security notify level* combo boxes respectively.

Click *Ok* to save the settings. The *Point-to-Point Tunneling Protocol (PPTP)* remote address range screen will appear.

Figure 4.76: Remote Address Range

Define the IP address range that an authorized user can assume when accessing your local network (see figure 4.76), and click *Next*.

The wizard will display a connection summary (see figure 4.77). Click *Finish* to create your VPN PPTP server connection.

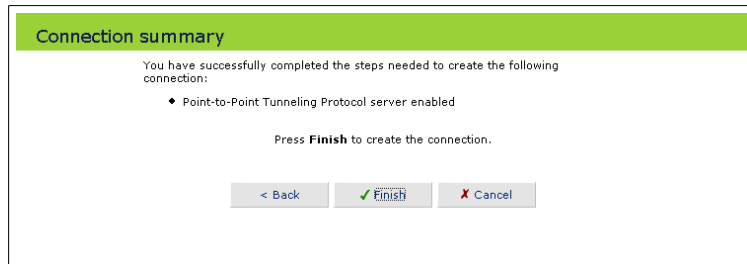


Figure 4.77: VPN PPTP Server Connection Summary

4.5.3 Configuring a PPTP Connection

Clicking on the *Settings* button at the bottom-right of the connection's Properties window, will open its Configuration window.

4.5.3.1 General

Schedule You can configure scheduler rules in order to define time segments during which the connection is active. To configure scheduler rules click the *New* link. To learn how to configure scheduler rules please refer to Section 6.11.

Network Select whether the parameters you are configuring relate to a LAN/WAN connection, by selecting LAN/WAN from the drop down list.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The setting *Manual*, allows you to enter the largest packet size that will be transmitted. To have the GlobeSurfer 3G select the best MTU for your Internet connection, select *Automatic*.

General	
Device Name:	ppp200
Status:	Disconnected
Schedule:	Always New
Network:	WAN
Connection Type:	VPN PPTP
MTU:	Automatic 1460

Figure 4.78: General PPTP Settings

4.5.3.2 PPP Settings

Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

PPTP Server Host name or IP address should be configured according to your ISP information.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time between reconnect attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

PPP	
Host Name or IP Address of Destination:	<input type="text" value="192.168.71.39"/>
<input type="checkbox"/> On Demand (will attempt to connect only when packets are sent)	
Time Between Reconnect Attempts:	<input type="text" value="30"/> Seconds

Figure 4.79: PPP Configuration

4.5.3.3 PPP Authentication

Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2.

Please note that encryption is performed only if *Microsoft CHAP, Microsoft CHAP version 2*, or both are selected.

PPP	
PPP authentication	
Login username (case sensitive):	<input type="text" value="dina"/>
Login password:	<input type="password" value="*****"/>
<input type="checkbox"/> Support unencrypted password (PAP)	
<input type="checkbox"/> Support Challenge Handshake Authentication (CHAP)	
<input checked="" type="checkbox"/> Support Microsoft CHAP (MS-CHAP)	
<input checked="" type="checkbox"/> Support Microsoft CHAP Version 2 (MS-CHAP v2)	

Figure 4.80: PPP Authentication Settings

Login username As agreed with ISP.

Login password As agreed with ISP.

Support unencrypted password (PAP) Password Authentication Protocol (PAP) is a simple, plaintext authentication scheme. The user name and password are requested by your networking peer in plaintext. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks

can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

4.5.3.4 PPP Encryption

PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link.

Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication algorithms.



PPP Encryption
<input type="checkbox"/> Require Encryption (Disconnect If Server Declines)
<input type="checkbox"/> Support Encryption (40 Bit Keys)
<input type="checkbox"/> Support Maximum Strength Encryption (128 Bit Keys)

Figure 4.81: PPP Encryption

Require encryption Select this check box to ensure that the PPP connection is encrypted.

Support encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support maximum strength encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

4.5.3.5 Internet Protocol

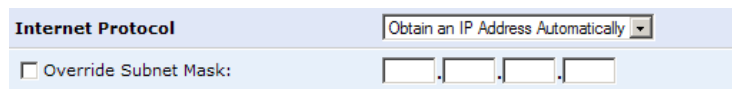
Select one of the following Internet protocol options from the *Internet protocol* drop down menu:

- Obtain an IP address automatically
- Use the following IP address

Please note that according to the selection you make in the *Internet protocol* drop down menu, the screen will refresh and display relevant configuration settings.

Obtain an IP address automatically Your PPP connection is configured by default to obtain an IP address automatically. You should change this configuration in case your service provider requires it.

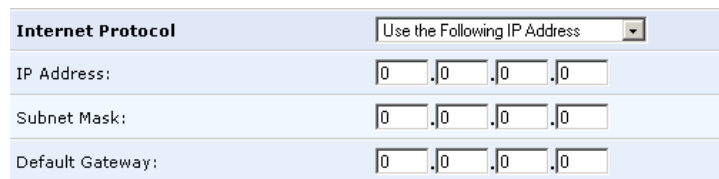
The server that assigns the GlobeSurfer 3G with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the *Override subnet mask* and specifying your own mask instead.



The screenshot shows a configuration window titled "Internet Protocol". On the right, a dropdown menu is set to "Obtain an IP Address Automatically". Below this, there is a checkbox labeled "Override Subnet Mask:" which is unchecked. To the right of the checkbox is a text input field for a subnet mask, currently showing "0.0.0.0".

Figure 4.82: Internet Protocol Settings – Automatic IP

Use the following IP address Your WAN connection can be configured using a permanent (static) IP address. Your service provider should provide you with this IP address, subnet mask and the default gateway IP address.



The screenshot shows a configuration window titled "Internet Protocol". On the right, a dropdown menu is set to "Use the Following IP Address". Below this, there are three rows of input fields. The first row is labeled "IP Address:" and contains four boxes with "0". The second row is labeled "Subnet Mask:" and contains four boxes with "0". The third row is labeled "Default Gateway:" and contains four boxes with "0".

Figure 4.83: Internet Protocol Settings – Static IP

4.5.3.6 DNS Server

Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP.

To configure the connection to automatically obtain a DNS server address, select *Obtain DNS Server Address Automatically* from the *DNS Server* drop down menu.



The screenshot shows a configuration window titled "DNS Server". On the right, a dropdown menu is set to "Obtain DNS Server Address Automatically".

Figure 4.84: Automatic DNS Settings

To manually configure DNS server addresses, select *Use the following DNS server addresses* from the *DNS server* drop down menu (see figure 4.100). Specify up to two different DNS server addresses, one primary and one secondary.

DNS Server	
	Use the Following DNS Server Addresses ▾
Primary DNS Server:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS Server:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Figure 4.85: DNS Settings

To learn more about this feature, refer to Section 6.2.

4.5.3.7 Routing

You can choose to setup your GlobeSurfer 3G to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

Routing Select *Advanced* or *Basic* routing.

Device metric The device metric is a value used by the GlobeSurfer 3G to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default route Select this check box to define this device as the default route.

Multicast - IGMP proxy internal IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of LAN devices asking to join multicast groups. Select the *Multicast IGMP proxy internal* check-box to enable this feature.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

- Listen to RIP messages - select *None*, *RIPv1*, *RIPv2* or *RIPv1/2*.
- Send RIP messages - select *None*, *RIPv1*, *RIPv2-broadcast* or *RIPv2-multicast*.

Routing table Allows you to add or modify routes when this device is active. Click the link to an existing route to edit it, or click *New route* to add a route.

Routing Advanced ▾						
Routing mode:	Route					
Device metric:	<input type="text" value="4"/>					
<input type="checkbox"/> Default route						
<input checked="" type="checkbox"/> Multicast - IGMP proxy internal						
<input type="checkbox"/> Routing Information Protocol (RIP)						
Routing table						
Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Wireless	192.168.22.3	192.168.2.1	255.255.255.255	0	Applied	
New route >>						
Internet connection firewall		<input type="checkbox"/> Enabled				

Figure 4.86: Advanced Routing Properties

To learn more about this feature, refer to Section 6.7.

4.5.3.8 Internet Connection Firewall

The GlobeSurfer 3G firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network or the Internet. The firewall applies security per network connection, for example the firewall can be applied on the UMTS WAN and the Wireless LAN, but not on the Ethernet LAN.

To enable the firewall on this network connection, select the *Enabled* check box.

Internet Connection Firewall	<input type="checkbox"/> Enabled
-------------------------------------	----------------------------------

Figure 4.87: Enable Firewall Connection

To learn more about the security features of the GlobeSurfer 3G, please refer to Chapter 5.

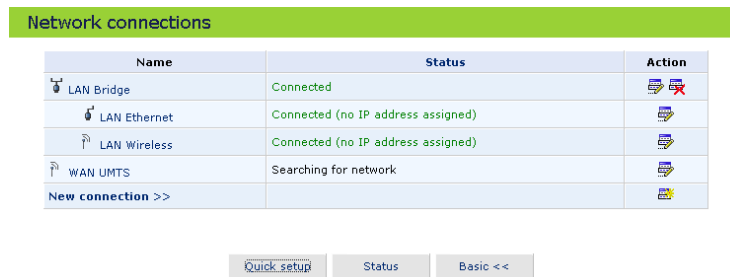
4.6 VPN L2TP







Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your GlobeSurfer 3G to create VPN connections. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP remote access concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP network server (LNS).

4.6.1 Creating an L2TP Connection

To create a L2TP client connection, perform the following steps:

1. Click *Network Connections* on the sidebar – the *Network Connections* screen will appear (see figure 4.88).



Name	Status	Action
LAN Bridge	Connected	 
LAN Ethernet	Connected (no IP address assigned)	
LAN Wireless	Connected (no IP address assigned)	
WAN UMTS	Searching for network	
New connection >>		

[Quick setup](#) [Status](#) [Basic <<](#)

Figure 4.88: Network Connections

2. Click the *New connection* link to list the connection alternatives.

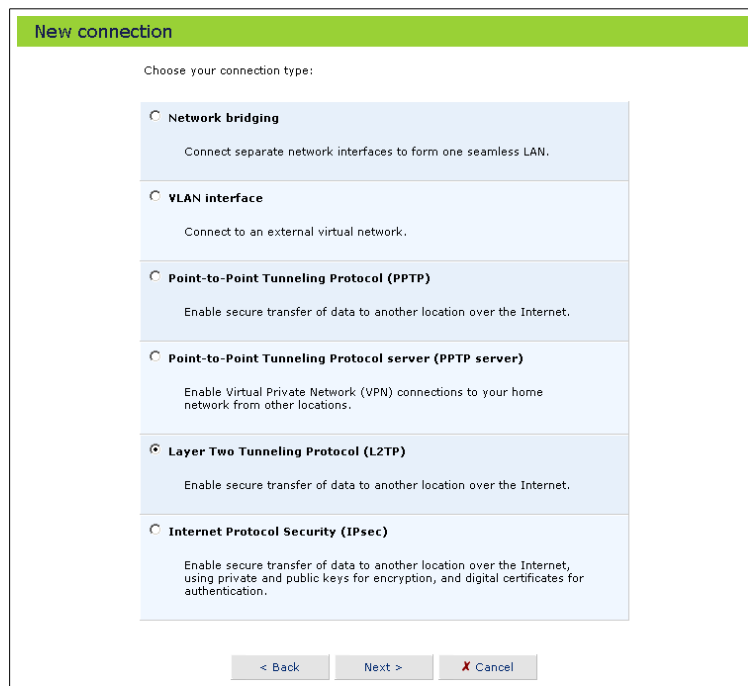


Figure 4.89: New Connection Alternatives

3. Select the *Layer Two Tunneling Protocol (L2TP)* radio button and click *Next*. The *Layer Two Tunneling Protocol (L2TP)* configuration screen will appear (see figure 4.90).

Enter the following parameters, supplied by your VPN server.

Hostname or IP address of destination Hostname or IP address of the VPN host server.

Shared secret A secret key represented as a sequence of characters that you jointly decide upon and share with the second party.

Use IPsec Use IPsec on the L2TP connection. See section 4.7.

Login username Your username.

Login password Your password.

Figure 4.90: L2TP Connection Properties

Click *Next* when ready. The wizard will display a connection summary (see figure 4.91).

Click *Finish* to create your VPN L2TP client connection.

Figure 4.91: L2TP Client Connection Summary

4.6.2 Configuring an L2TP Connection

Clicking on the *Settings* button at the bottom-right of the connection's Properties window, will open its Configuration window.

4.6.2.1 General

Schedule You can configure scheduler rules in order to define time segments during which the connection is active. To configure scheduler rules click the *New* link. To learn how to configure scheduler rules please refer to Section 6.11.

Network Select whether the parameters you are configuring relate to a LAN/WAN connection, by selecting LAN/WAN from the drop down list.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The setting *Manual*, allows you to enter the largest packet size that will be transmitted. To have the GlobeSurfer 3G select the best MTU for your Internet connection, select *Automatic*.

New connection

Choose your connection type:

Network bridging
 Connect separate network interfaces to form one seamless LAN.

VLAN interface
 Connect to an external virtual network.

Point-to-Point Tunneling Protocol (PPTP)
 Enable secure transfer of data to another location over the Internet.

Point-to-Point Tunneling Protocol server (PPTP server)
 Enable Virtual Private Network (VPN) connections to your home network from other locations.

Layer Two Tunneling Protocol (L2TP)
 Enable secure transfer of data to another location over the Internet.

Internet Protocol Security (IPsec)
 Enable secure transfer of data to another location over the Internet, using private and public keys for encryption, and digital certificates for authentication.

< Back
Next >
X Cancel

Figure 4.92: L2TP General Settings

4.6.2.2 PPP Settings

Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

L2TP Server Host name and shared secret should be configured according to your ISP information.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time between reconnect attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

PPP

Host Name or IP Address of Destination:

Shared Secret:

On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: Seconds

Figure 4.93: L2TP PPP Settings

4.6.2.3 PPP Authentication

Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2.

Please note that encryption is performed only if *Microsoft CHAP*, *Microsoft CHAP version 2*, or both are selected.

PPP	
PPP authentication	
Login username (case sensitive):	<input type="text" value="dina"/>
Login password:	<input type="password" value="xxxxxxxx"/>
<input type="checkbox"/> Support unencrypted password (PAP)	
<input type="checkbox"/> Support Challenge Handshake Authentication (CHAP)	
<input checked="" type="checkbox"/> Support Microsoft CHAP (MS-CHAP)	
<input checked="" type="checkbox"/> Support Microsoft CHAP Version 2 (MS-CHAP v2)	

Figure 4.94: PPP Authentication Settings

Login username As agreed with ISP.

Login password As agreed with ISP.

Support unencrypted password (PAP) Password Authentication Protocol (PAP) is a simple, plaintext authentication scheme. The user name and password are requested by your networking peer in plaintext. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

4.6.2.4 PPP Encryption

PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link.

Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication algorithms.

PPP Encryption	
<input type="checkbox"/>	Require Encryption (Disconnect If Server Declines)
<input type="checkbox"/>	Support Encryption (40 Bit Keys)
<input type="checkbox"/>	Support Maximum Strength Encryption (128 Bit Keys)

Figure 4.95: PPP Encryption

Require encryption Select this check box to ensure that the PPP connection is encrypted.

Support encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support maximum strength encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

4.6.2.5 PPP Compression

The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner.

PPP Compression	
BSD:	Reject ▾
Deflate:	Reject ▾

Figure 4.96: PPP Compression

For each compression algorithm, select one of the following from the drop down menu:

Reject Reject PPP connections with peers that use the compression algorithm.

Allow Allow PPP connections with peers that use the compression algorithm.

Require Ensure a connection with a peer is using the compression algorithm.

4.6.2.6 Internet Protocol

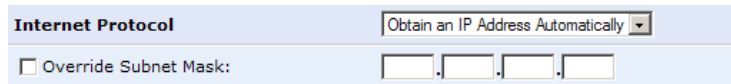
Select one of the following Internet protocol options from the *Internet protocol* drop down menu:

- Obtain an IP address automatically
- Use the following IP address

Please note that according to the selection you make in the *Internet protocol* drop down menu, the screen will refresh and display relevant configuration settings.

Obtain an IP address automatically Your PPP connection is configured by default to obtain an IP address automatically. You should change this configuration in case your service provider requires it.

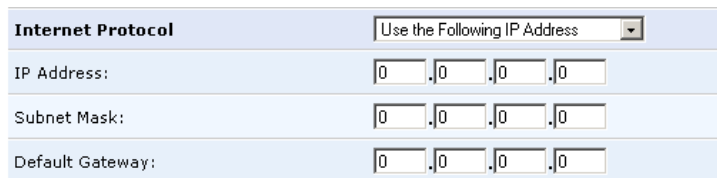
The server that assigns the GlobeSurfer 3G with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the *Override subnet mask* and specifying your own mask instead.



Internet Protocol	Obtain an IP Address Automatically
<input type="checkbox"/> Override Subnet Mask:

Figure 4.97: Internet Protocol Settings – Automatic IP

Use the following IP address Your WAN connection can be configured using a permanent (static) IP address. Your service provider should provide you with this IP address, subnet mask and the default gateway IP address.



Internet Protocol	Use the Following IP Address
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0

Figure 4.98: Internet Protocol Settings – Static IP

4.6.2.7 DNS Server

Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP.

To configure the connection to automatically obtain a DNS server address, select *Obtain DNS Server Address Automatically* from the *DNS Server* drop down menu.



DNS Server	Obtain DNS Server Address Automatically
-------------------	---

Figure 4.99: Automatic DNS Settings

To manually configure DNS server addresses, select *Use the following DNS server addresses* from the *DNS server* drop down menu (see figure 4.100). Specify up to two different DNS server addresses, one primary and one secondary.

DNS Server	
	Use the Following DNS Server Addresses ▾
Primary DNS Server:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS Server:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Figure 4.100: DNS Settings

To learn more about this feature, refer to Section 6.2.

4.6.2.8 Routing

You can choose to setup your GlobeSurfer 3G to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

Routing Select *Advanced* or *Basic* routing.

Device metric The device metric is a value used by the GlobeSurfer 3G to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default route Select this check box to define this device as the default route.

Multicast - IGMP proxy internal IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of LAN devices asking to join multicast groups. Select the *Multicast IGMP proxy internal* check-box to enable this feature.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

- Listen to RIP messages - select *None*, *RIPv1*, *RIPv2* or *RIPv1/2*.
- Send RIP messages - select *None*, *RIPv1*, *RIPv2-broadcast* or *RIPv2-multicast*.

Routing table Allows you to add or modify routes when this device is active. Click the link to an existing route to edit it, or click *New route* to add a route.

Routing Advanced ▾						
Routing mode:	Route					
Device metric:	<input type="text" value="4"/>					
<input type="checkbox"/> Default route						
<input checked="" type="checkbox"/> Multicast - IGMP proxy internal						
<input type="checkbox"/> Routing Information Protocol (RIP)						
Routing table						
Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Wireless	192.168.22.3	192.168.2.1	255.255.255.255	0	Applied	
New route >>						
Internet connection firewall		<input type="checkbox"/> Enabled				

Figure 4.101: Advanced Routing Properties

To learn more about this feature, refer to Section 6.7.

4.6.2.9 Internet Connection Firewall

The GlobeSurfer 3G firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network or the Internet. The firewall applies security per network connection, for example the firewall can be applied on the UMTS WAN and the Wireless LAN, but not on the Ethernet LAN.

To enable the firewall on this network connection, select the *Enabled* check box.

Internet Connection Firewall	<input type="checkbox"/> Enabled
-------------------------------------	----------------------------------

Figure 4.102: Enable Firewall Connection

To learn more about the security features of the GlobeSurfer 3G, please refer to Chapter 5.

4.7 VPN IPsec

4.7.1 IPsec Network-to-Host Scenario Connection

In order to create an IPsec connection between GlobeSurfer 3G and a Windows host, you need to configure both the gateway and the host. This section describes both GlobeSurfer 3G's configuration and a Windows XP client configuration.

4.7.1.1 Configuring IPsec on GlobeSurfer 3G

1. Click the *Network connections* icon on the sidebar, the *Network connections* screen will appear (see figure 4.103).

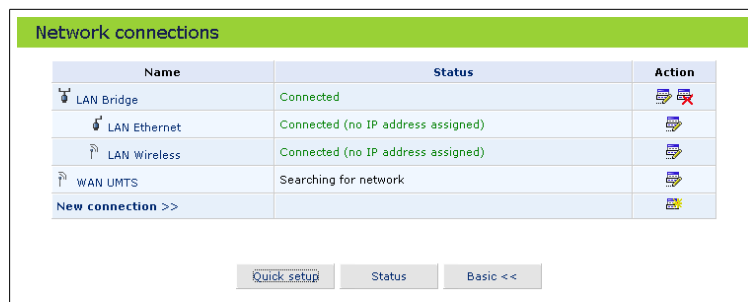


Figure 4.103: Network Connections

2. Click the *New connection* link. The *New connection* screen will appear (see figure 4.133).

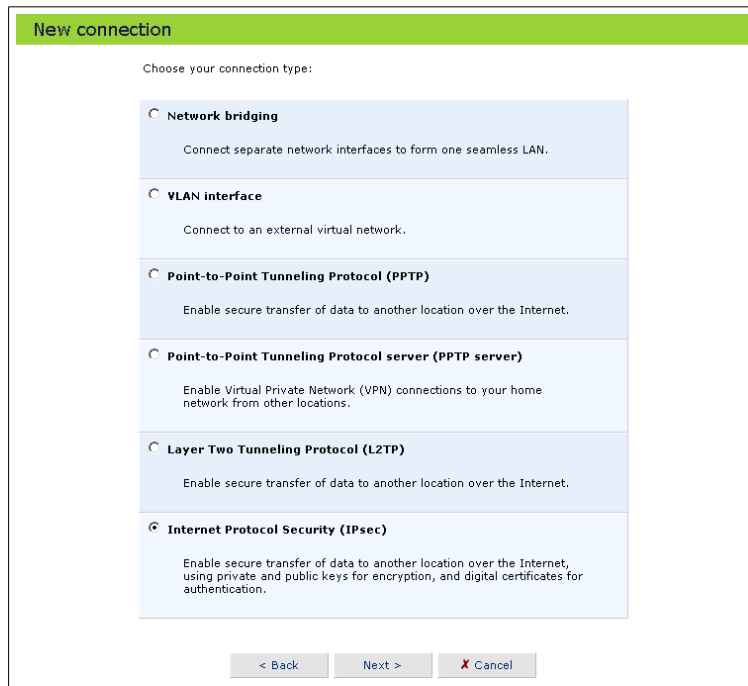


Figure 4.104: New Connection

3. Select the *Internet Protocol Security (IPsec)* radio button and click *Next*. The *Internet Protocol Security (IPsec) topology* screen will appear (see figure 4.105).

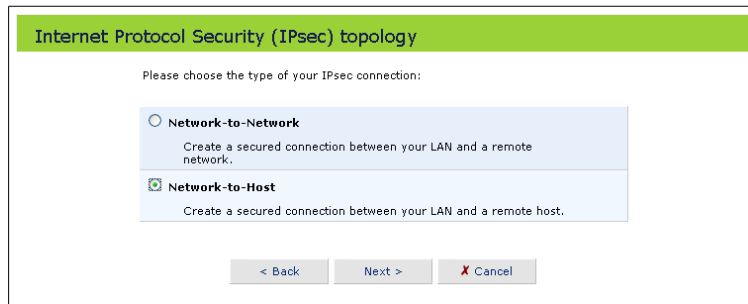


Figure 4.105: IPsec Topology

Select the *Network-to-Host* radio button to create a secure connection between your LAN and a remote host. Click *Next*, the *IPsec remote address type* screen will appear (see figure 4.106).

Figure 4.106: IPsec Remote Address Type

Select the *Remote gateway address* radio button to allow an IPsec connection from a specific address. Alternatively, select the *Any remote gateway* radio button to allow a connection from any address holding the shared secret. Click *Next*, the *IPsec connection properties* screen will appear (see figure 4.107).

Figure 4.107: IPsec Connection Properties

Specify the following parameters:

Remote tunnel endpoint address Specify 22.23.24.25

Shared secret Specify "hr5x"

Click *Next*, the *Connection summary* screen will appear (see figure 4.137).

Figure 4.108: Connection Summary

Click *Finish*. The *Network connections* screen will now list the newly created IPsec connection (see figure 4.138).

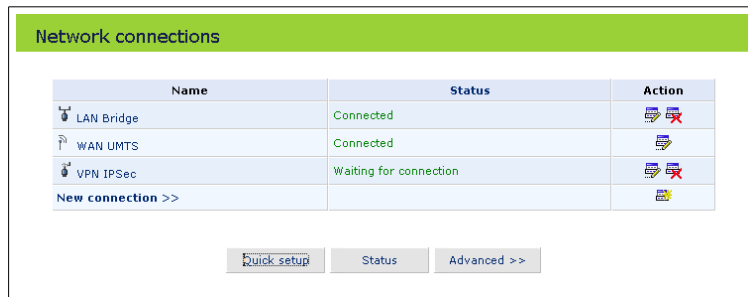


Figure 4.109: Network Connections

4.7.1.2 Configuring IPsec on the Windows Host

The following IP addresses are needed for the host configuration:

- Windows IP address - referred to as "windows.ip".
- GlobeSurfer 3G WAN IP address - referred to as "openrg_wan.ip".
- GlobeSurfer 3G LAN subnet address - referred to as "openrg_lan_subnet".

The configuration sequence:

1. The first step is to create the IPsec policy:
 - (a) Click the Start button and select Run. Type "secpol.msc" and click OK. The *Local Security Settings* window will appear (see figure 4.110).

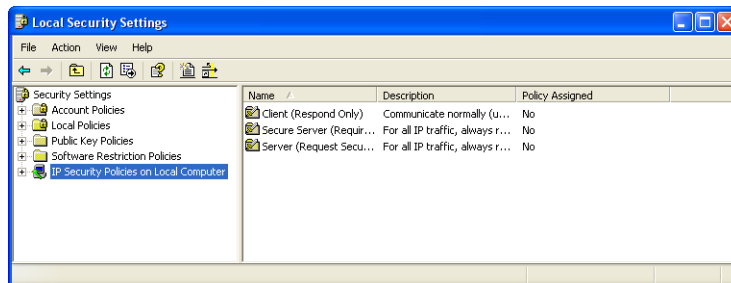


Figure 4.110: Local Security Settings

- (b) Right-click the *IP Security Policies on Local Computer* and choose *Create IP Security Policy....* The IP Security Policy Wizard will appear (see figure 4.111).

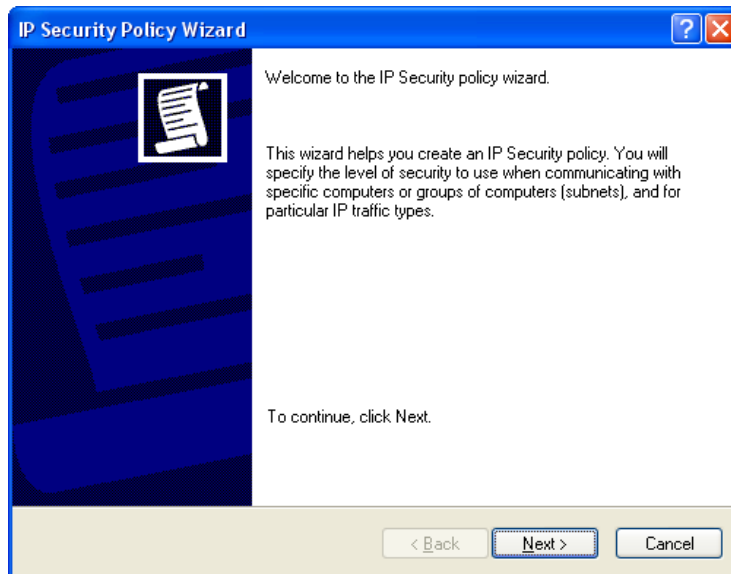


Figure 4.111: IP Security Policy Wizard

- (c) Click *Next* and type a name for your policy, for example "GlobeSurfer 3G Connection" (see figure 4.112). Click *Next*.

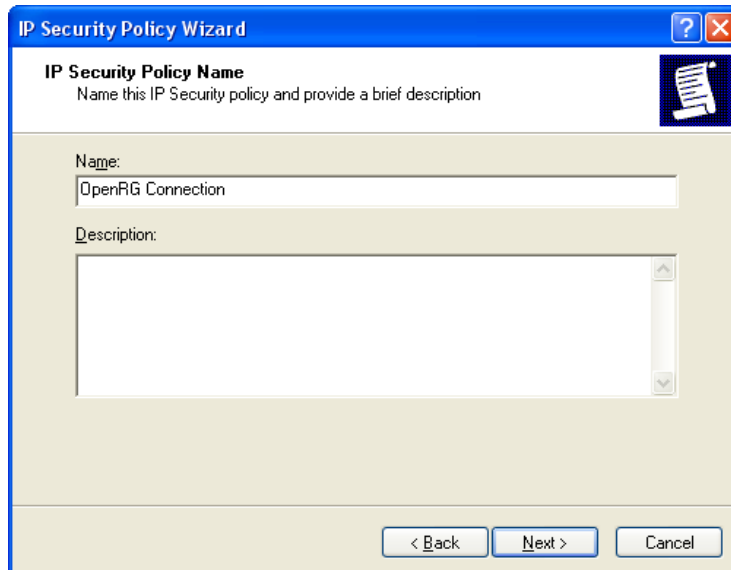


Figure 4.112: IP Security Policy Name

- (d) Deselect the *Activate the default response rule* check box (see figure 4.113) and click *Next*.

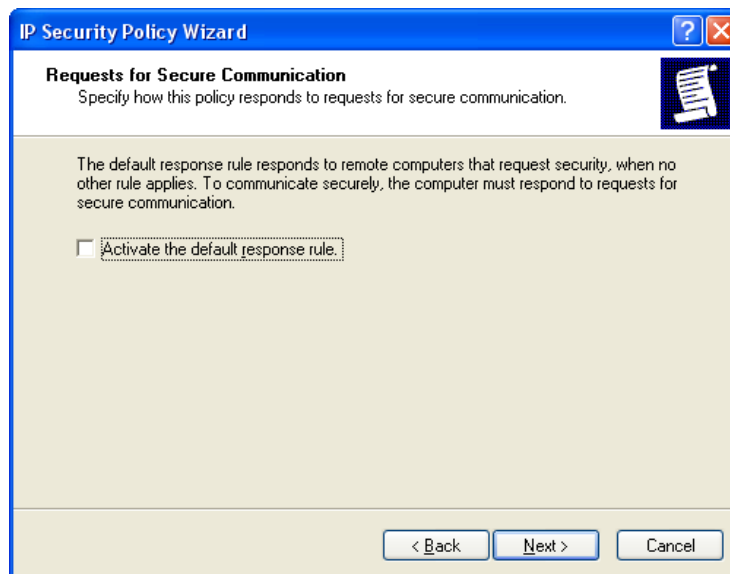


Figure 4.113: Requests for Secure Communication

- (e) Make sure that the *Edit Properties* check box is checked (see figure 4.114) and click the Finish button.

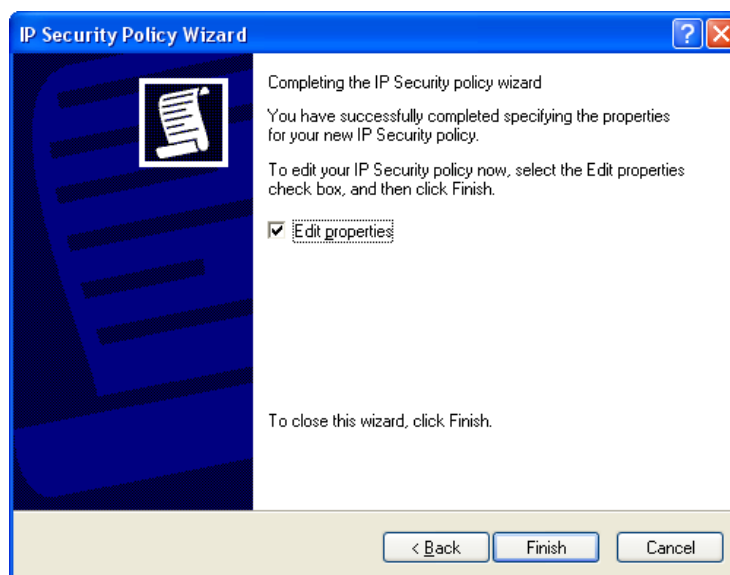


Figure 4.114: Completing the IP Security Policy Wizard

- (f) On the *GlobeSurfer 3G Connection Properties* window that will appear (see figure 4.115), click OK.

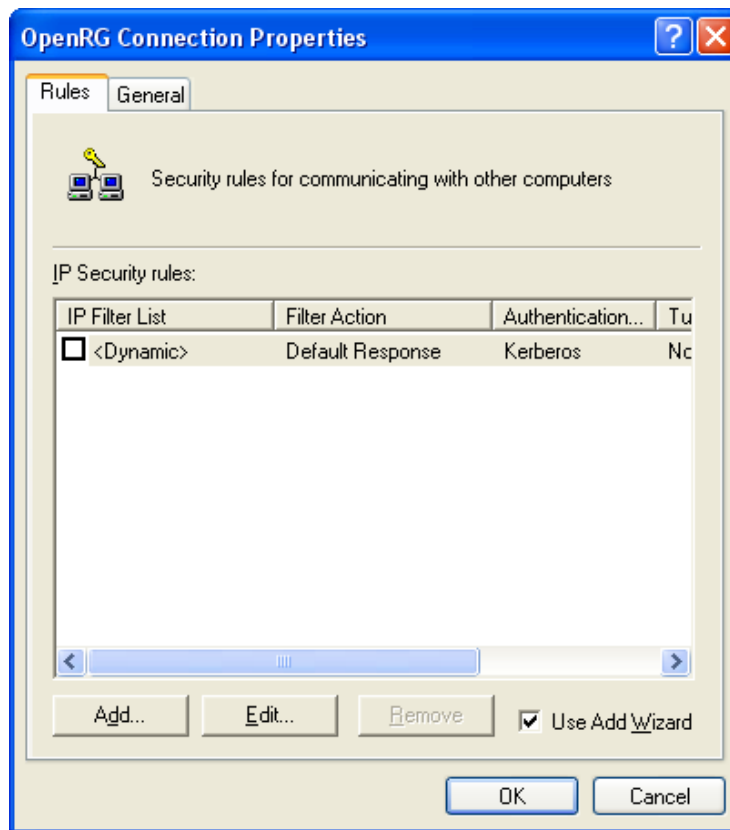


Figure 4.115: GlobeSurfer 3G Connection Properties

2. Building Filter List 1 - Windows XP to GlobeSurfer 3G:
 - (a) In the *Local Security Settings* window, right-click the new *GlobeSurfer 3G Connection* policy, created in the previous step, and select *Properties*. The *Properties* window will appear (see figure 4.115).
 - (b) Deselect the *Use Add Wizard* check box and click the *Add* button to create a new IP Security rule. The *New Rule Properties* window will appear (see figure 4.116).

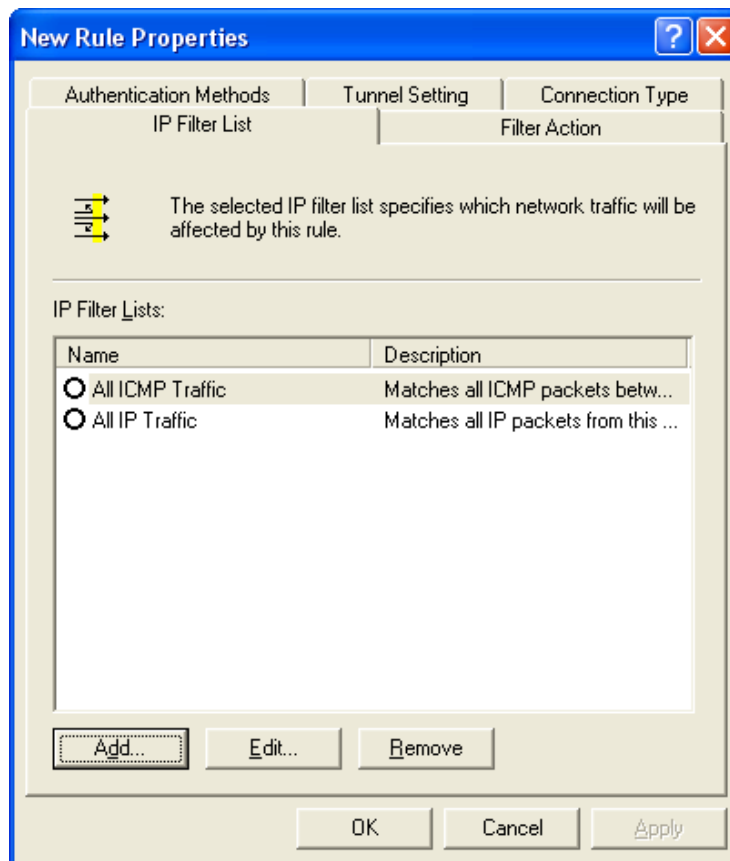


Figure 4.116: New Rule Properties

- (c) Under the IP Filter List tab, click the *Add* button. The *IP Filter List* window will appear (see figure 4.117).

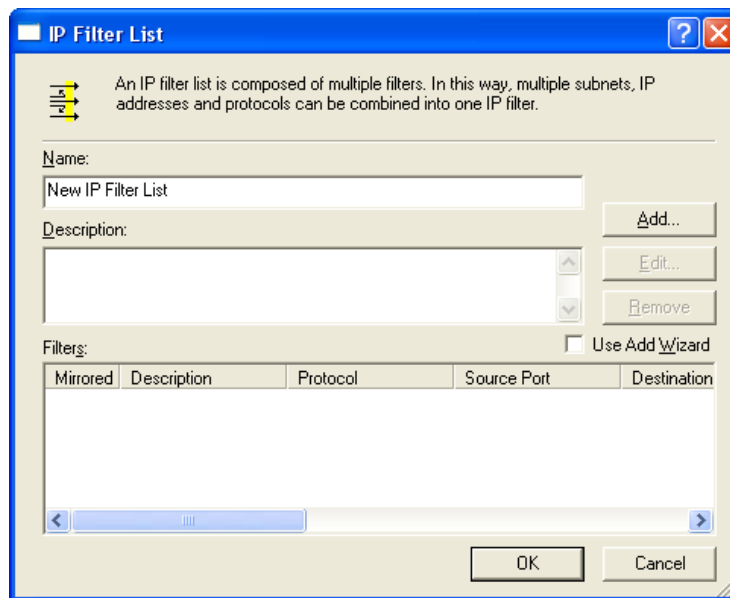


Figure 4.117: IP Filter List

- (d) Enter the name "Windows XP to GlobeSurfer 3G" for the filter list, deselect the *Use Add Wizard* check box, and click the *Add* button. The *Filter Properties* window will appear (see figure 4.118).

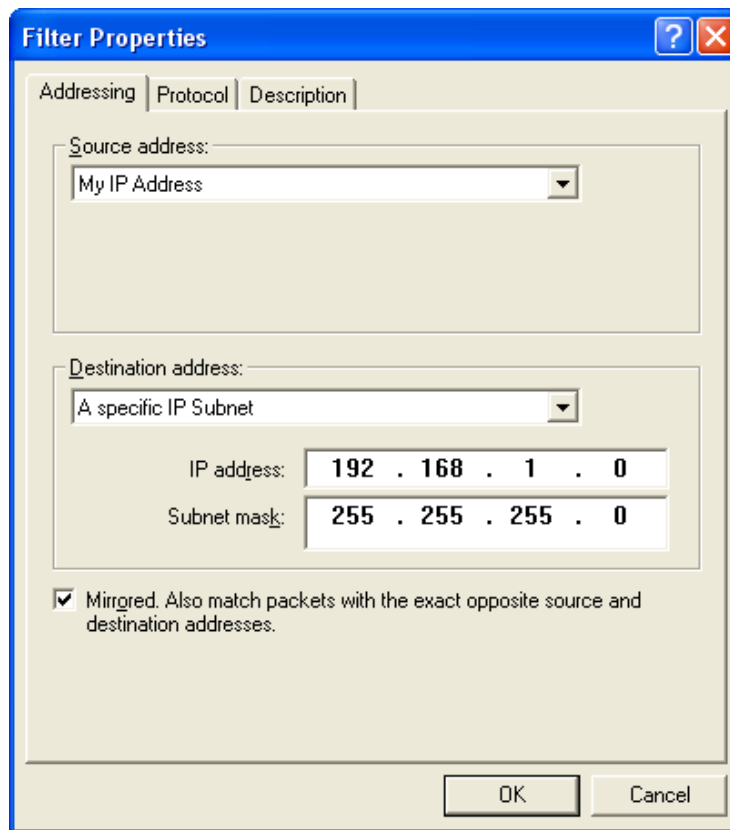


Figure 4.118: Filter Properties

- (e) In the *Source address* combo box, select *My IP Address*.
 - (f) In the *Destination address* combo box, select *A Specific IP Subnet*. In the *IP Address* field enter the LAN Subnet ("*openrg.lan.subnet*"), and in the *Subnet mask* field enter *255.255.255.0*.
 - (g) Click the *Description* tab if you would like to enter a description for your filter.
 - (h) Click *OK*. Click *OK* again in the *IP Filter List* window to save the settings.
3. Building Filter List 2 - GlobeSurfer 3G to Windows XP:
- (a) Under the *IP Filter List* tab of the *New Rule Properties* window, click the *Add* button. The *IP Filter List* window will appear (see figure 4.117).
 - (b) Enter the name "*GlobeSurfer 3G to Windows XP*" for the filter list, deselect the *Use Add Wizard* check box, and click the *Add* button. The *Filter Properties* window will appear (see figure 4.119).

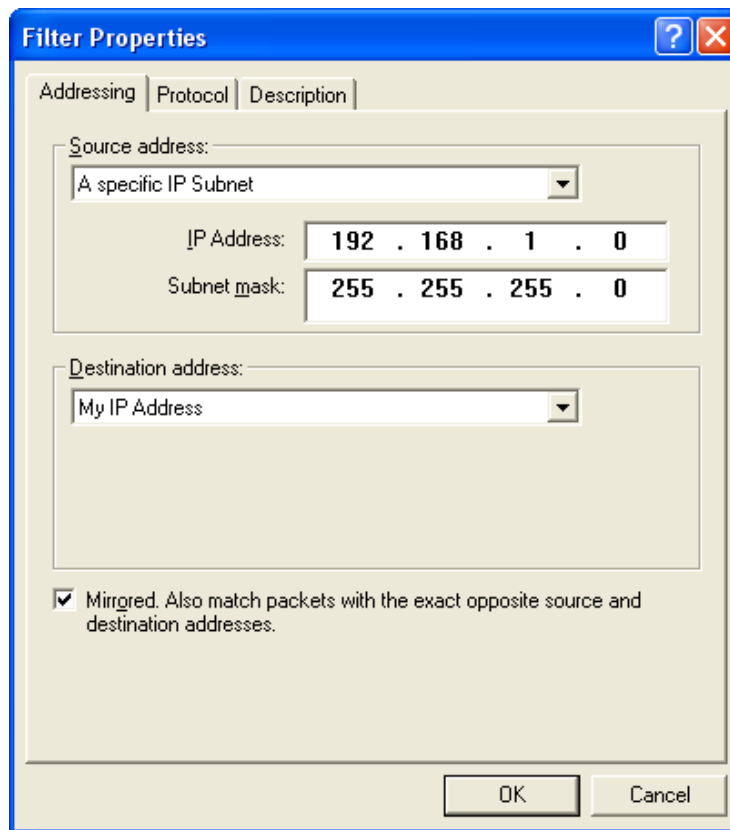


Figure 4.119: Filter Properties

- (c) In the *Source address* combo box, select *A Specific IP Subnet*. In the *IP Address* field enter the LAN Subnet ("openrg_lan_subnet"), and in the *Subnet mask* field enter 255.255.255.0.
 - (d) In the *Destination address* combo box, select *My IP Address*.
 - (e) Click the *Description* tab if you would like to enter a description for your filter.
 - (f) Click *OK*. Click *OK* again in the *IP Filter List* window to save the settings.
4. Configuring Individual Rule of Tunnel 1 (Windows XP to GlobeSurfer 3G):
- (a) Under the *IP Filter List* tab of the *New Rule Properties* window, select the *Windows XP to GlobeSurfer 3G* radio button (see figure 4.120).

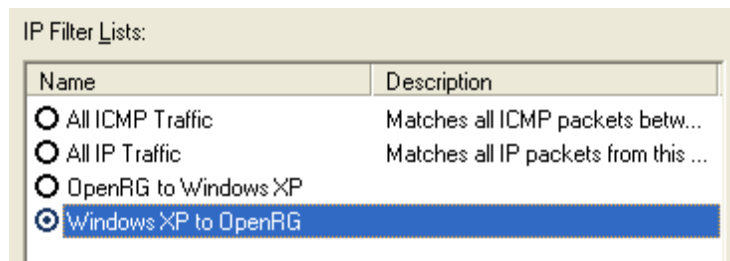


Figure 4.120: IP Filter List

- (b) Click the *Filter Action* tab (see figure 4.121).

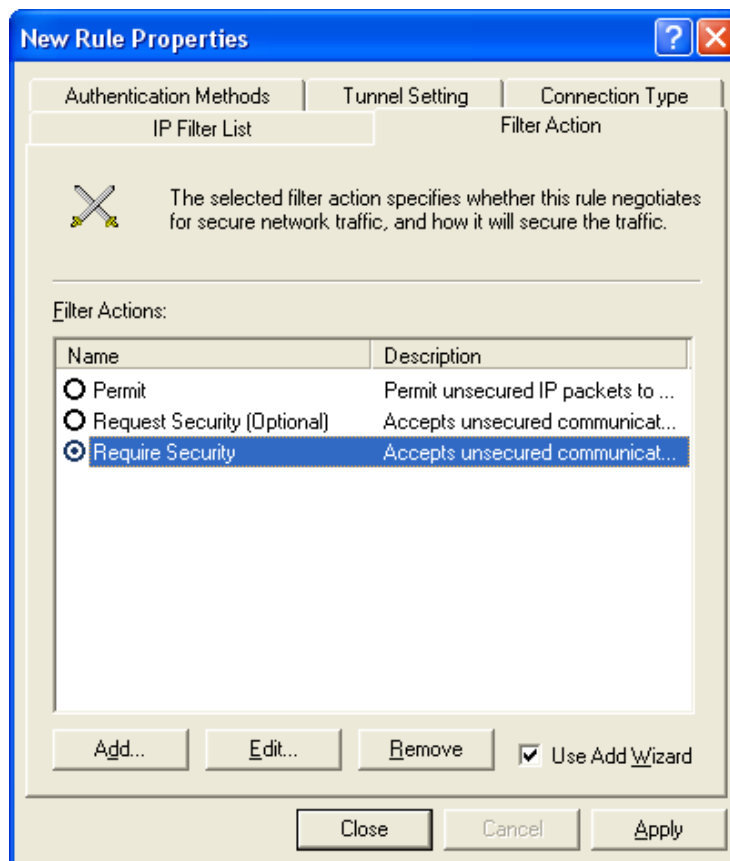


Figure 4.121: Filter Action

- (c) Select the *Require Security* radio button, and click the *Edit* button. The *Require Security Properties* window will appear (see figure 4.122).

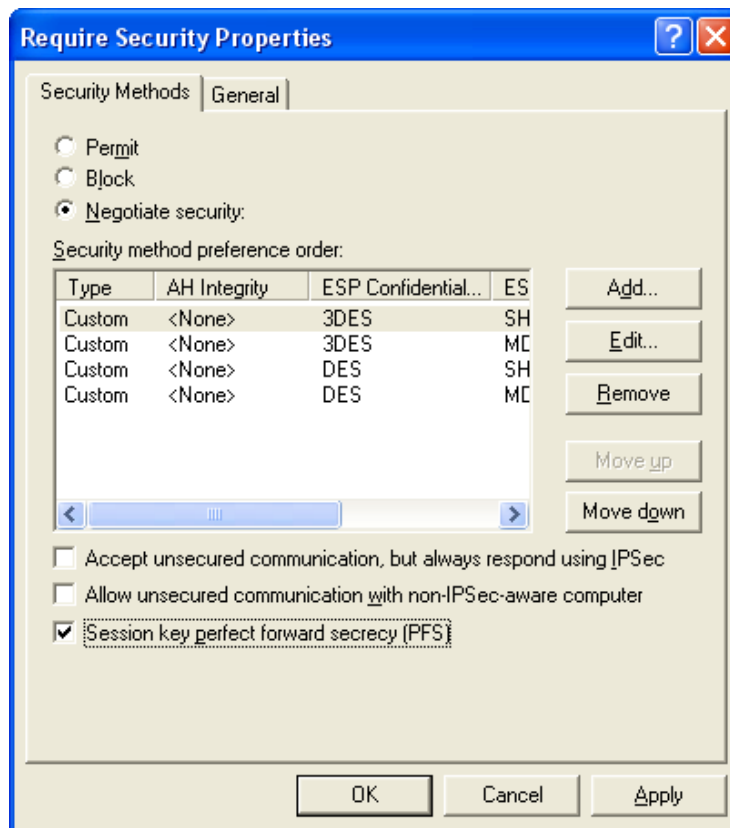


Figure 4.122: Require Security Properties

- (d) Verify that the *Negotiate security* option is enabled, and deselect the *Accept unsecured communication, but always respond using IPsec* check box. Select the *Session key Perfect Forward Secrecy (PFS)* (the PFS option must be enabled on GlobeSurfer 3G), and click the *OK* button.
- (e) Under the *Authentication Methods* tab, click the *Edit* button. The *Edit Authentication Method Properties* window will appear (see figure 4.123).

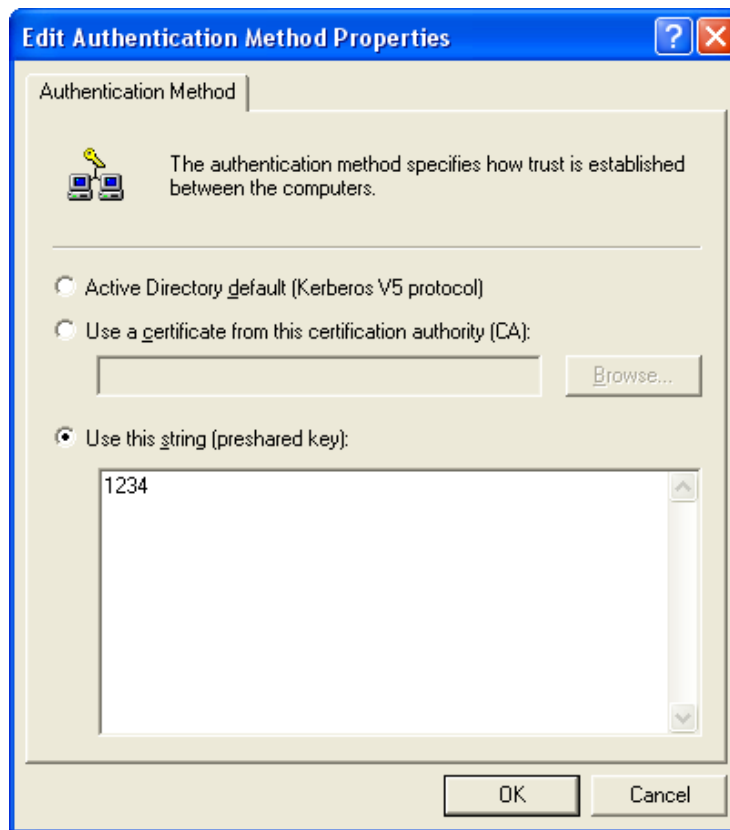


Figure 4.123: Edit Authentication Method Properties

- (f) Select the *Use this string (preshared key)* radio button, and enter a string that will be used as the key (for example, 1234). Click the OK button.
- (g) Under the *Tunnel Setting* tab, select the *The tunnel endpoint is specified by this IP Address* radio button, and enter "openrg-wan.ip" (see figure 4.124).

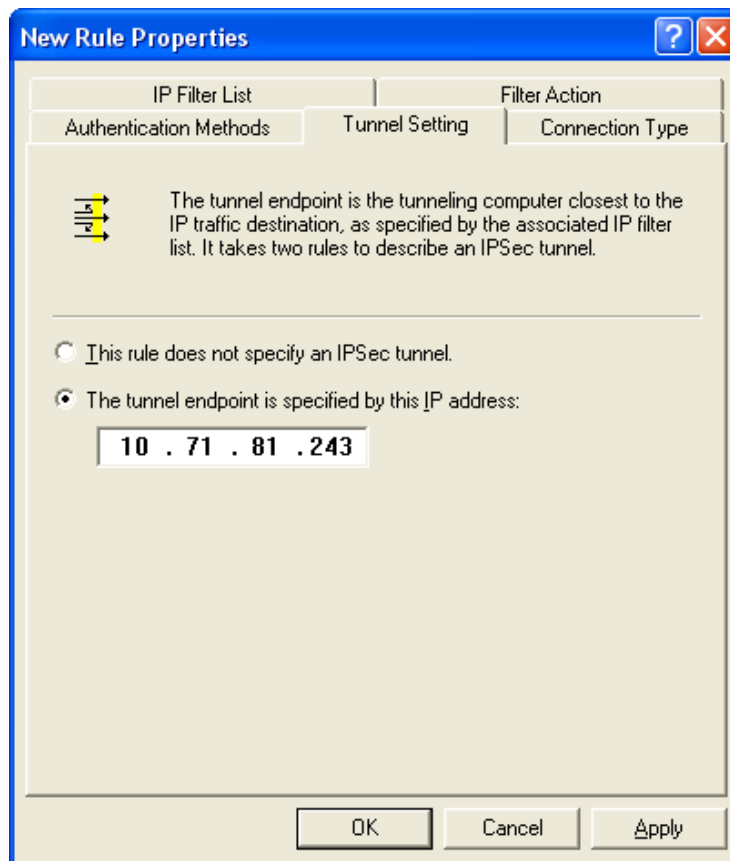


Figure 4.124: Tunnel Setting

- (h) Under the *Connection Type* tab, verify that *All network connections* is selected.
 - (i) Click *Apply* and then click *OK* to save this rule.
5. Configuring Individual Rule of Tunnel 2 (GlobeSurfer 3G to Windows XP):
- (a) Under the *IP Filter List* tab of the *New Rule Properties* window, select the *GlobeSurfer 3G to Windows XP* radio button (see figure 4.125).

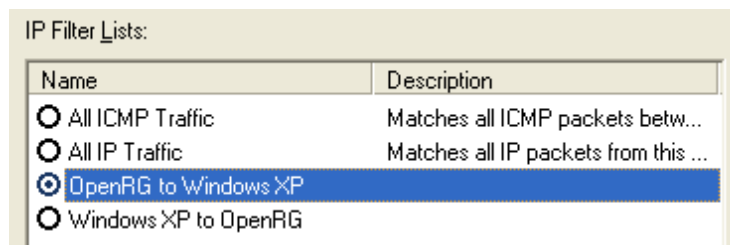


Figure 4.125: IP Filter List

- (b) Click the *Filter Action* tab (see figure 4.121).
- (c) Select the *Require Security* radio button, and click the *Edit* button. The *Require Security Properties* window will appear (see figure 4.122).
- (d) Verify that the *Negotiate security* option is enabled, and deselect the *Accept unsecured communication, but always respond using IPsec* check box. Select the *Session key Perfect Forward Secrecy (PFS)* (the PFS option must be enabled on GlobeSurfer 3G), and click the *OK* button.
- (e) Under the *Authentication Methods* tab, click the *Edit* button. The *Edit Authentication Method Properties* window will appear (see figure 4.123).
- (f) Select the *Use this string (preshared key)* radio button, and enter a string that will be used as the key (for example, 1234). Click the *OK* button.
- (g) Under the *Tunnel Setting* tab, select the *The tunnel endpoint is specified by this IP Address* radio button, and enter "windows.ip" (see figure 4.126).

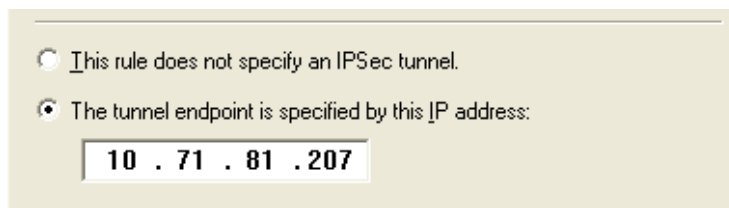


Figure 4.126: Tunnel Setting

- (h) Under the *Connection Type* tab, verify that *All network connections* is selected.
- (i) Click *Apply* and then click *OK* to save this rule.
- (j) Back on the *GlobeSurfer 3G Connection Properties* window, note that the two new rules have been added to the *IP Security rules* list (see figure 4.127).

IP Filter List	Filter Action	Authentication...
<input checked="" type="checkbox"/> Windows XP to OpenRG	Require Security	Preshared Key
<input checked="" type="checkbox"/> OpenRG to Windows XP	Require Security	Preshared Key
<input type="checkbox"/> <Dynamic>	Default Response	Kerberos

Figure 4.127: GlobeSurfer 3G Connection Properties

Click *Close* to go back to the *Local Security Settings* window (see figure 4.110).

6. To assign the new IPsec policy:

In the *Local Security Settings* window, right-click the *GlobeSurfer 3G Connection* policy, and select *Assign*. A small green arrow will appear on the policy's folder icon and its status under the *Policy Assigned* column will change to *Yes* (see figure 4.128).

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (u...	No
OpenRG Connection		Yes
Secure Server (Requir...	For all IP traffic, always r...	No
Server (Request Secu...	For all IP traffic, always r...	No

Figure 4.128: Local Security Settings

4.7.2 IPsec Network-to-Network Scenario Connection

This section describes how to configure IPsec network-to-network with a pre-shared secret scenario, developed by the VPN Consortium (VPNC) using GlobeSurfer 3G. GlobeSurfer 3G's VPN feature is VPNC certified.

4.7.2.1 Network Configuration

Establishing an IPsec tunnel between gateways A and B creates a transparent and secure network for clients from subnets A and B, communicating with clients on the other network. Assuming both gateways are running GlobeSurfer 3G, their configurations are the same, except for their IP addresses. As such, this section describes only the configuration of gateway A. The configuration of Gateway B is identical, where A and B are replaced by B and A respectively.

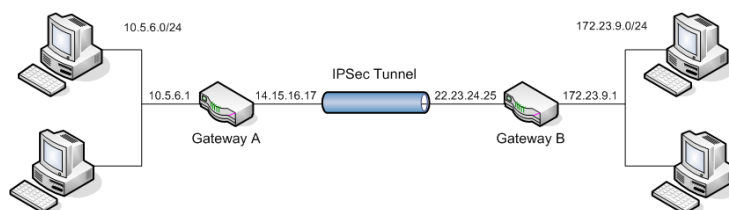


Figure 4.129: Configuration Diagram

4.7.2.1.1 LAN Interface Settings

1. Login to the GlobeSurfer 3G management console.
2. Click *Network connections* on the sidebar, the *Network connections* screen will appear (see figure 4.130).

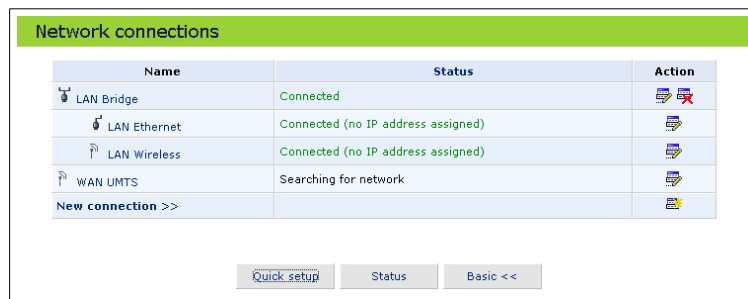


Figure 4.130: Network Connections

- Click the *LAN Bridge* link, the *LAN Bridge properties* screen will appear.

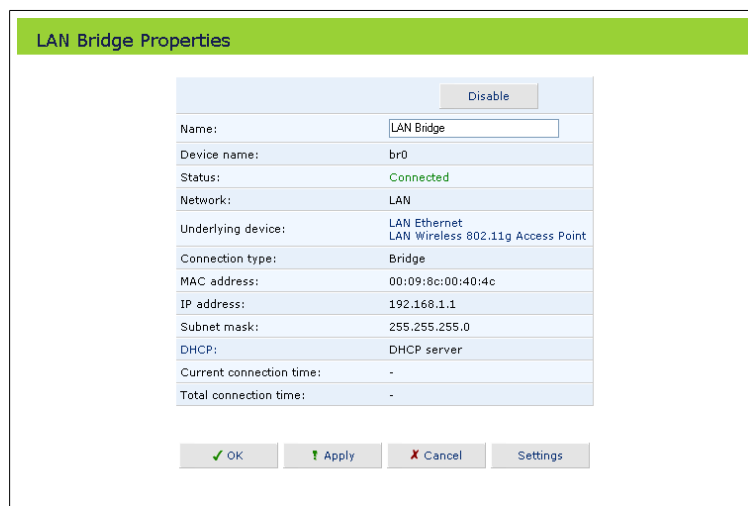


Figure 4.131: LAN Bridge Properties

- Click the *Settings* button, the *Configure LAN Bridge* screen will appear. Configure the following parameters (see figure 4.132).

Internet protocol Select *Use the following IP address*.

IP address Specify 10.5.6.1

Subnet mask Specify 255.255.255.0

DHCP Select *DHCP server*.

Start IP address Specify 10.5.6.1

End IP address Specify 10.5.6.254

Subnet mask Specify 255.255.255.0

Note: When configuring gateway B, the IP address should be 172.23.9.1, according to the example depicted here.

Internet Protocol	Use the Following IP Address ▼
IP Address:	10 . 5 . 6 . 1
Subnet Mask:	255 . 255 . 255 . 0
IP Address Distribution	DHCP Server ▼
Start IP Address:	10 . 5 . 6 . 1
End IP Address:	10 . 5 . 6 . 254
Subnet Mask:	255 . 255 . 255 . 0

Figure 4.132: LAN Bridge Settings

5. Click OK.

4.7.2.2 Network-to-Network with Pre-shared Secrets

A typical network-to-network VPN uses a pre-shared secret for authentication. Gateway A connects its internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25.

The Internet Key Exchange (IKE) Phase 1 parameters used are:

- Main mode
- 3DES (Triple DES)
- SHA-1
- MODP group 2 (1024 bits)
- Pre-shared secret of "hr5x"
- SA lifetime of 28800 seconds (eight hours) with no Kbytes re-keying

The IKE Phase 2 parameters used are:

- 3DES (Triple DES)
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for re-keying
- SA lifetime of 3600 seconds (one hour) with no Kbytes re-keying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To set up Gateway A for this scenario, follow these steps:

1. Click the *Network connections* icon on the sidebar, the *Network connections* screen will appear (see figure 4.130).
2. Click the *New connection* link, the *New connection* screen will appear (see figure 4.133).

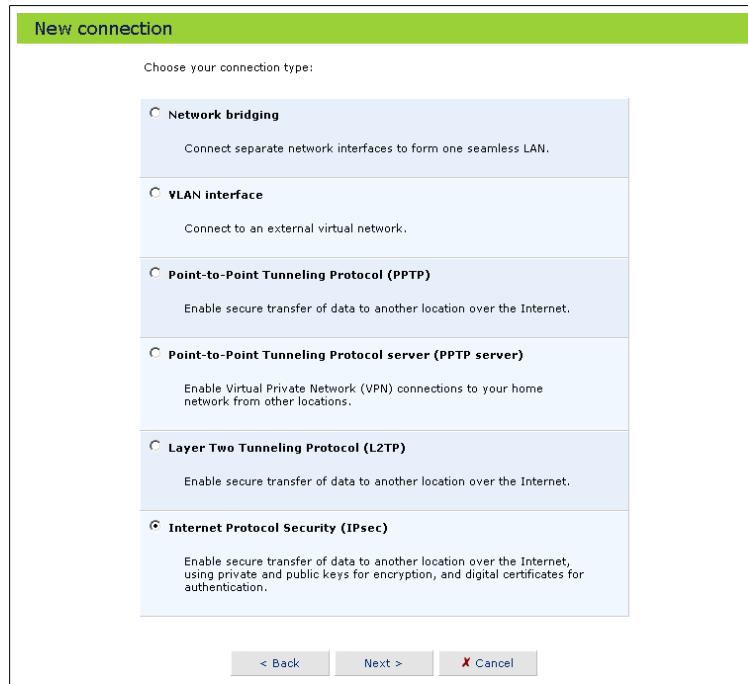


Figure 4.133: New Connection

3. Select the *Internet Protocol Security (IPsec)* radio button and click *Next*. The *Internet Protocol Security (IPsec) topology* screen will appear (see figure 4.134).

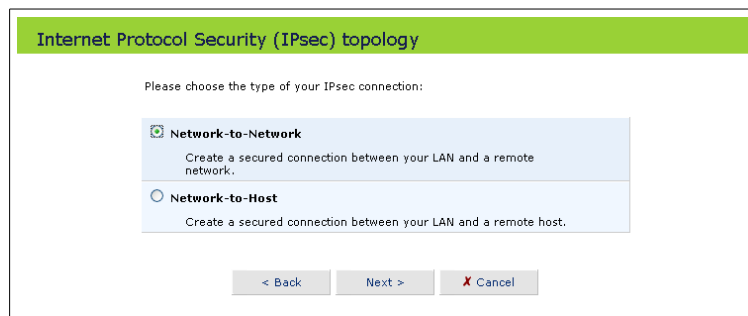


Figure 4.134: IPsec Topology

4. Select the *Network-to-Network* radio button to create a secure connection between your LAN and a remote network. Click *Next*, the *IPsec remote*

address type screen will appear (see figure 4.135).

Internet Protocol Security (IPsec) remote address type

Please choose the type of remote address and the type of remote subnet of your IPsec connection:

Remote gateway address
Allow IPsec connection from a specific address.

Any remote gateway
Allow incoming IPsec connection from any address.

Remote subnet
Allow IPsec connection from a specific remote subnet.

Any remote subnet
Allow IPsec connection from any remote subnet.

< Back Next > Cancel

Figure 4.135: Remote Address Type

5. Select the *Remote gateway address* radio button to allow an IPsec connection from a specific address.
6. Select the *Remote subnet* radio button to allow an IPsec connection from a specific remote subnet.
7. Click *Next*, the *Internet Protocol Security (IPsec)* screen will appear (see figure 4.136).

Internet Protocol Security (IPsec) remote address type

Configure your IPsec connection properties:

Remote tunnel endpoint address: 22.23.24.25

Remote subnet

Remote subnet IP address: 172.23.9.0

Remote subnet mask: 255.255.255.0

Shared Secret: hr5x

< Back Next > Cancel

Figure 4.136: IPsec Connection Properties

8. Specify the following parameters:
Remote tunnel endpoint address Specify 22.23.24.25
Remote subnet IP address Specify 172.23.9.0
Remote subnet mask Specify 255.255.255.0
Shared secret Specify "hr5x"

9. Click *Next*, the *Connection summary* screen will appear (see figure 4.137).

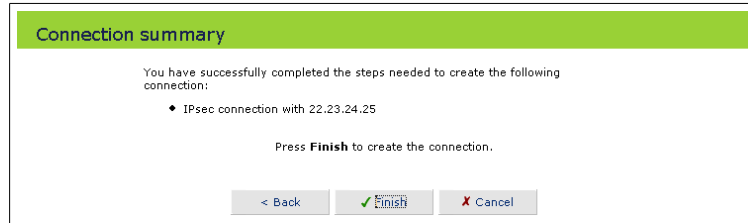


Figure 4.137: Connection Summary

10. Click *Finish*. The *Network connections* screen will now list the newly created IPsec connection (see figure 4.138).

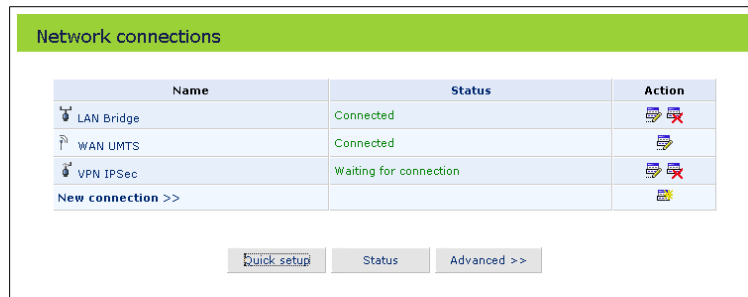


Figure 4.138: Network Connections

11. Click the *Edit* action icon for *VPN IPsec*, the *VPN IPsec properties* screen will appear (see figure 4.139).

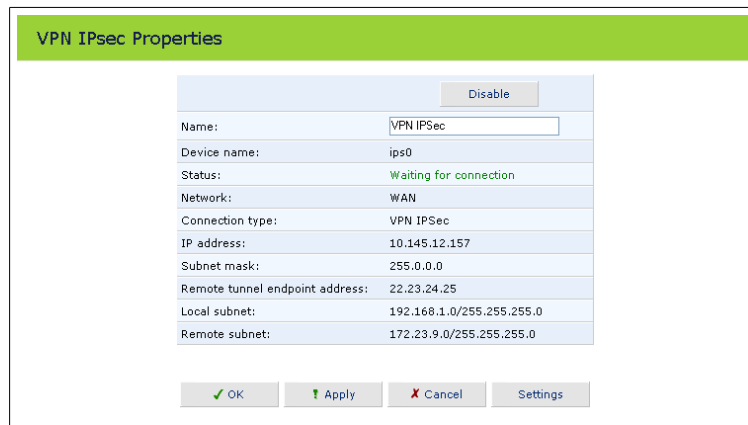


Figure 4.139: Connection Properties

12. Click the *Settings* button, the *Configure VPN IPsec* screen will appear.

-
13. Deselect the *Compress* check box.
 14. Under *Hash algorithm*, deselect the *Allow peers to use MD5* check box.
 15. Under *Group description attribute*, deselect the *DH Group 5 (1536 bit)* check box.
 16. Under *Encryption algorithm*, deselect the *Allow AH Protocol (no encryption)* check box.
 17. Click OK. The *VPN IPsec properties* screen will appear.
 18. Click OK. The *Network connections* screen will appear (see figure 4.140). Note that the IPsec connection's status has changed to *Connected*.

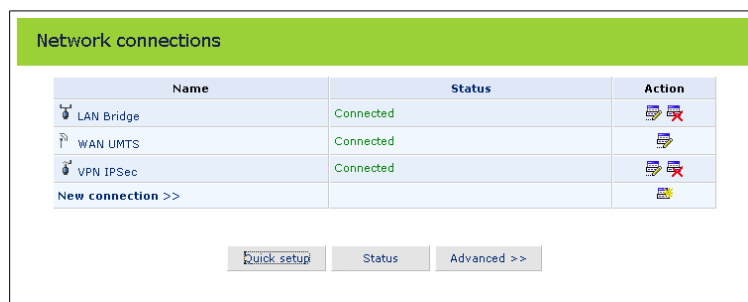


Figure 4.140: Connection Properties

5

Security

The GlobeSurfer 3G includes comprehensive and robust security services: Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet.

The firewall, the cornerstone of the GlobeSurfer 3G security services, has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security (see figure 5.1).

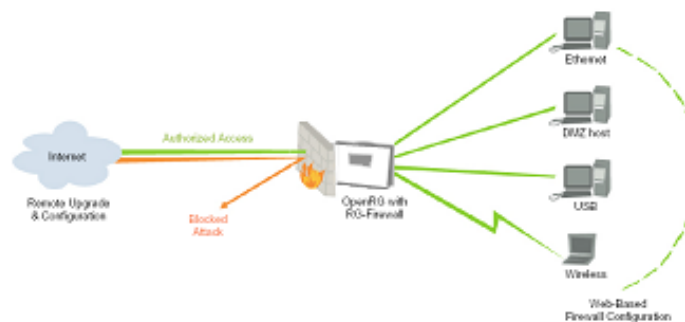


Figure 5.1: GlobeSurfer 3G's Firewall in Action

The GlobeSurfer 3G firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing.

The GlobeSurfer 3G firewall supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

The Security screen of the GlobeSurfer 3G management console is divided into tabs that feature the following:

- The *General* tab allows you to choose the security level for the firewall (see section 5.1)
- The *Access control* tab can be used to restrict access from the local network to the Internet (see section 5.2).
- The *Local servers* tab can be used to enable access from the Internet to specified services provided by computers in the local network and special Internet applications (see section 5.3). *Local servers* is sometimes referred to as *Port forwarding*.
- The *DMZ host* tab allows you to configure a LAN host to receive all traffic arriving at your GlobeSurfer 3G, which does not belong to a known session (see section 5.4).
- The *Port triggering* tab allows you to define port triggering entries, to dynamically open the firewall for some protocols or ports. (see section 5.5).
- The *Remote administration* tab can be used to enable remote configuration of GlobeSurfer 3G from any Internet-accessible computer (see section 5.6).
- The *IP/Hostname filtering* tab allows you to block LAN access to a certain host or web site on the Internet. (see section 5.7).
- *Advanced filtering* tab allows you to implicitly control the firewall setting and rules (see section 5.8).
- *Security log* tab allows you to view and configure the firewall Log (see section 5.9)

5.1 General Security Level Settings

Use the *Security* screen to configure the basic security settings of the GlobeSurfer 3G (see figure 5.2).



Figure 5.2: General Security Level Settings

The firewall regulates the flow of data between the local network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through GlobeSurfer 3G) or rejected (barred from passing through GlobeSurfer 3G) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing local users access to the Internet services that they require.

The firewall rules specify what types of services available on the Internet may be accessed from the local network and what types of services available in the local network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating in the Internet or from a computer in the local network, is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") will also be allowed to pass, regardless of its direction. For example, when you point your Web browser to a Web page on the Internet, a request is sent out to the Internet for this page. When the request reaches GlobeSurfer 3G the firewall will identify the request type and origin—HTTP and a specific PC in your local network, in this case. Unless you have configured access control to block requests of this type from this computer, the firewall will allow this request to pass out onto the Internet (see section 5.2 for more on setting access controls). When the Web page is returned from the Web server the firewall will associate it with this session and allow it to pass,

regardless of whether HTTP access from the Internet to the local network is blocked or permitted.

The important thing to note here is that it is the *origin of the request*, not subsequent responses to this request, that determines whether a session can be established or not.

You may choose from among three pre-defined security levels for GlobeSurfer 3G: Minimum, Typical (the default setting), and Maximum. The table below summarizes the behavior of GlobeSurfer 3G for each of the three security levels.

Security level	Requests originating in the WAN (incoming traffic)	Requests originating in the LAN (outgoing traffic)
Maximum security	<i>Blocked:</i> No access to local network from Internet, except as configured in the <i>Local servers, DMZ host</i> and <i>Remote administration</i> screens	<i>Limited:</i> Only commonly-used services, such as Web-browsing and e-mail, are permitted *
Typical security (default)	<i>Blocked:</i> No access to local network from Internet, except as configured in the <i>Local servers, DMZ host</i> and <i>Remote administration</i> screens	<i>Unrestricted:</i> All services are permitted, except as configured in the <i>Access control</i> screen
Minimum security	<i>Unrestricted:</i> Permits full access from Internet to local network; all connection attempts permitted.	<i>Unrestricted:</i> All services are permitted, except as configured in the <i>Access control</i> screen

* These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

Attention: Some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use these ports, if they cannot connect with their own default ports. When applying this behaviour, these applications will not be blocked outbound, even at *Maximum security* level.

To configure GlobeSurfer 3G's general security settings (see figure 5.2):

1. Choose from among the three predefined security levels described in the table above. *Typical security* is the default setting.

Caution: Using the *Minimum security* setting may expose the local network to significant security risks, and thus should only be used, when necessary, for short periods of time.

-
2. Check the *Block IP fragments* box in order to protect your local network from a common type of hacker attack that could make use of fragmented data packets to sabotage your local network. Note that VPN over IPsec and some UDP-based services make legitimate use of IP fragments. You will need to allow IP fragments to pass into the local network in order to make use of these select services.
 3. Click *OK* to save your changes.

5.2 Access Control

You may want to block specific computers within the local network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from surfing the Web, another computer from transferring files using FTP, and the whole network from receiving incoming e-mail.

Access Control defines restrictions on the types of requests that may pass from the local network out to the Internet, and thus may block traffic flowing in both directions. In the e-mail example given above, you may prevent computers in the local network from receiving e-mail by blocking their *outgoing* requests to POP3 servers on the Internet. The Access Control feature incorporates a list of preset services in the form of applications and common port settings, allowing you to specifically select those that you want to restrict or grant access.

- To view and allow/restrict these services:
 1. Select the *Access control* tab in the *Security* management screen. The *Access control* screen will appear (see figure 5.3).

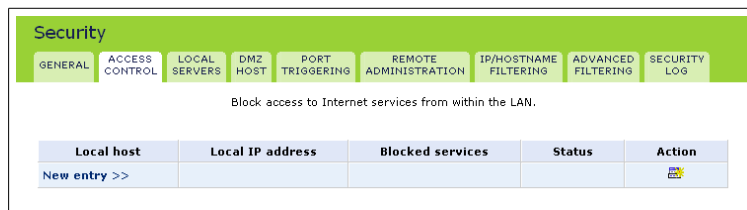


Figure 5.3: Access Control

2. Click the *New entry* link. The *Add access control rule* screen will appear (see figure 5.4).



Figure 5.4: Add Access Control Rule

Note: Figure 5.4 represents only the top portion of the actual screen, which lists many more services.

The above screen displays the list of predefined services that you can choose to block, including many popular game servers and many lesser-known services. For example, if you want to make sure that your employees won't put your business at risk from illegally traded copyright files, you may want to block several popular P2P and file sharing applications.

3. Select the service or services that you would like to block.
4. In the top section of the screen, select the group of computers to which you would like to apply the access control rule. You can either select from a predefined list of groups, by selecting one from the *Applied to* combo box, or create a new group by clicking the *New* link. Such a group of LAN devices is called a *Network object*. To learn more about network objects, see Section 6.6.
5. You might want to define the time period during which the access control rule will take effect. You can either select from a predefined list of schedules by selecting one from the *Schedule* combo box, or create a new schedule by clicking the *New* link. To learn how to create a new time schedule, see Section 6.11. The default is *Always*.
6. Click *OK* to save your changes. The *Access control* tab will display a summary of the access control rule that you just added (see figure 5.5).

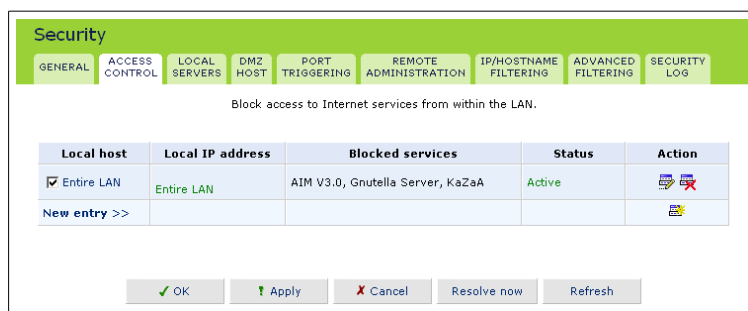


Figure 5.5: Access Control Rule

Note: To block a service that is not included in the list, click the *New User-Defined Service* link. The *Edit Service* screen will appear. Define the service, then click *OK* to save your changes (see section 5.10 for assistance). The service will then be automatically added to the top section of the *Add access control rule* screen. You may now select the service, just as you would a pre-defined service.

You may change the computer (or computers) prohibited from accessing a particular service, by modifying the appropriate entry under the *Local host* column

in the Access control table.

- To modify an entry in the Access control table:
 1. Click the **Edit** button for the service. The *Edit Service* screen will appear.
 2. Select the network group to which you would like to apply the rule, and the schedule during which the rule will take effect.
 3. Click *OK* to save your changes and return to the *Access control* screen.

You may disable an access control and make the service available without having to remove the service from the Access control table. This may be useful if you wish to make the service available only temporarily and expect that you will want to reinstate the restriction in the future.

- To temporarily disable an access control clear the check box next to the service name.
- To reinstate the restriction at a later time select the check box next to the service name.
- To remove an access restriction from the Access control table click the **Remove** button for the service. The service will be removed from the Access control table.

Please note that when Web Filtering is enabled, HTTP services cannot be blocked by Access control.

5.3 Local Servers (Port Forwarding)

In its default state, GlobeSurfer 3G blocks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the local network. The Local Servers feature supports both of these functions. If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as "Port Forwarding".

The *Local servers* tab shows the most commonly used applications that require special handling by GlobeSurfer 3G—all you have to do is identify which of them you want to use and the local IP address of the computer that will be using the service. For example, if you wanted to use the Net2Phone voice application on one of your PCs you would simply select *Net2Phone* from the list and enter the local IP address or host name of that computer in the right-hand column. All Net2Phone-related data arriving at GlobeSurfer 3G from the Internet will henceforth be forwarded to the specified computer.

Similarly, if you want to grant Internet users access to servers inside your local network, you must identify each service that you want to provide and the PC that will provide it. For example, if you want to host a Web server inside the local network you must select *HTTP - Web server* from the list and enter the local IP address or host name of the computer that will host the Web server in the right-hand column. Then when an Internet user points her browser to the external IP address of GlobeSurfer 3G, it will forward the incoming HTTP request to the computer that is hosting the Web server.

Additionally, *Local servers* enable you to redirect traffic to a port different than the port it was designated. Lets say, that you have a web server running on your PC on port 8080 and you want to grant access to this server to anyone who accesses GlobeSurfer 3G via HTTP. To accomplish this, do the following:

- Define a local server for the HTTP service, with the PC's IP or host name.
- Specify 8080 in the *Forwarded port* field.

All incoming HTTP traffic will now be forwarded to the PC running the web server on port 8080.

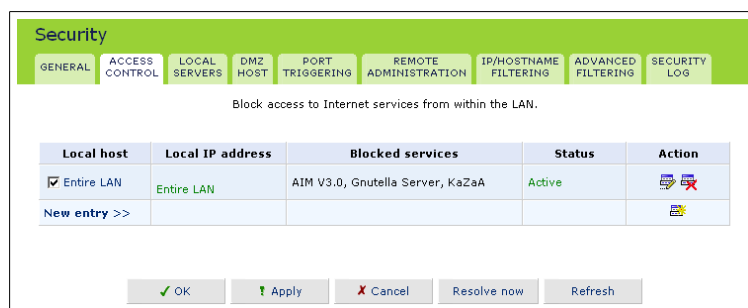


Figure 5.6: Local Servers

Note: Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific Application Level Gateway (ALG) modules in order to work inside the local network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. GlobeSurfer 3G is equipped with a robust list of ALG modules in order to enable maximum functionality in the local network. The ALG is automatically assigned based on the destination port.

Select the *Local servers* tab to view the list of special services and local servers that are currently enabled in the local network (see figure 5.6).

- To add a new service to the active local servers:
 1. Click the *New entry* button. The *Add local server* screen will appear (see figure 5.7).
 2. Select the service that you would like to provide.
 3. Enter the local IP address or the host name of the computer that will provide the service (the *server*). Note that only one LAN computer can be assigned to provide a specific service or application.
 4. Select a port to forward communications to (note that this parameter is optional). If not specified, data will be forwarded to the original port number.
 5. Define the time period during which the local server will be active. You can either select from a predefined list of schedules by selecting one from the *Schedule* combo box, or create a new schedule by clicking the *New* link. To learn how to create a new time schedule, see Section 6.11.
 6. Click *OK* to save your changes and return to the *Local servers* screen.

Note: To add a service that is not included in the list click the *New user-defined service* link. The *Edit Service* screen will appear. Define the service, then click *OK* to save your changes (see section 5.10 for assistance). The service will then be automatically added to the top section of the *Add local server* screen. You may now select the service, just as you would a pre-defined service.

Service name	Protocols and ports	Action
User-defined services		
New user-defined service >>		
Basic Web utilities		
<input type="checkbox"/> All Traffic	Protocol Any	
<input type="checkbox"/> DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
<input type="checkbox"/> HTTP - Web Server	TCP Any -> 80	

Figure 5.7: Add Local Servers

- To edit an entry in the *Local servers* table so that a service can be provided by a different local computer:
 1. Click the **Edit** button for the service. The *Edit Service* screen will appear.
 2. Enter the IP address or the host name of the computer that you would like to provide this service.
 3. Click *OK* to save your changes and return to the *Local servers* screen.

You may disable a service and make the service unavailable without having to remove the service from the *Local servers* table. This may be useful if you wish to make the service unavailable only temporarily and expect that you will want to make it available again in the future.

† How many computers can use a service or play a game simultaneously? Well, the answer may be a bit confusing. All the computers on the network can use a specific service as clients simultaneously. Being a client means that the computer within the network initiates the connection—for example, opens an FTP connection with an FTP server on the Internet. But only one computer can serve as a server, meaning responding to requests from computers on the Internet. Assigning a specific computer as a server is done from the *Local Servers* tab of the *Security* screen of the management console.

5.4 DMZ Host

The DMZ (Demilitarized) host feature allows one local computer to be exposed to the Internet. Designate a DMZ host when:

- You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the *Local servers* list and for which no port range information is available.
- You are not concerned with security and wish to expose one computer to all services without restriction.

Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the local network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

An incoming request for access to a service in the local network, such as a Web-server, is fielded by GlobeSurfer 3G. GlobeSurfer 3G will forward this request to the DMZ host (if one is designated) unless the service is being provided by another PC in the local network (assigned in *Local servers*), in which case that PC will receive the request instead.

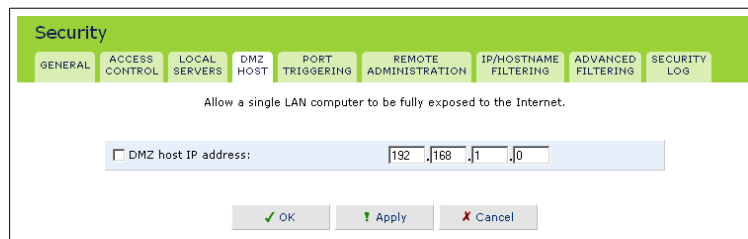


Figure 5.8: DMZ Host

- To designate a local computer as a DMZ Host:
 1. Select the *DMZ Host* tab. The *DMZ Host* screen will appear (see figure 5.8).
 2. Enter the local IP address of the computer that you would like to designate as a DMZ host. Note that only one LAN computer may be a DMZ host at any time.
 3. Click *OK* to save your changes and return to the *DMZ Host* screen.

You may disable the DMZ host so that it will not be fully exposed to the Internet, but keep its IP address recorded on the *DMZ Host* screen. This may be useful if you wish to disable the DMZ host but expect that you will want to enable it again in the future.

- To disable the DMZ host, so that it will not be fully exposed to the Internet: clear the check-box next to the DMZ IP designation.
- To enable the DMZ host: select the check-box next to the DMZ IP designation.

5.5 Port Triggering

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

For example, consider a gaming server that is accessed using UDP protocol on port 2222. The gaming server responds by connecting the user using UDP on port 3333 when starting gaming sessions. In such a case you must use port triggering, since this scenario conflicts with the following default firewall settings:

- The firewall blocks inbound traffic by default.
- The server replies to GlobeSurfer 3G's IP, and the connection is not sent back to your host, since it is not part of a session.

In order to solve this you need to define a port triggering entry, which allows inbound traffic on UDP port 3333, only after a LAN host generated traffic to UDP port 2222. This will result in accepting the inbound traffic from the gaming server, and sending it back to the LAN host which originated the outgoing traffic to UDP port 2222. Select the *Port triggering* tab on the security screen, the *Port triggering* screen will appear (see figure 5.9). This screen will list all of the port triggering entries.

Port Triggering Services	Action
<input checked="" type="checkbox"/> L2TP	
<input checked="" type="checkbox"/> TFTP	
New Entry >>	

Figure 5.9: Port Triggering

- Let's add an entry for the gaming example above:
 1. Click the *New entry* link to add an entry (see figure 5.10).

Port Triggering Service Name	Server Ports	Opened Ports	Action
User-Defined Services			
New User-Defined Service >>			

Figure 5.10: Adding Port Triggering Rules

2. Click the *New user-defined service* link to add an entry (see figure 5.11).

Service Name:	<input type="text" value="g_server"/>
Service Description:	<input type="text" value="Gaming Server"/>

Server Ports

Protocol	Server Ports	Action
New Server Ports >>		

Opened Ports

Protocol	Opened Ports	Action
New Opened Ports >>		

Figure 5.11: New User-Defined Service

- Specify the following port triggering entries in the *New server ports* and *New opened ports* respectively (see figure 5.12):

Edit service server ports

Protocol	<input type="text" value="UDP"/>
Source ports:	<input type="text" value="Any"/>
Destination ports:	<input type="text" value="Single"/> <input type="text" value="2222"/>

Figure 5.12: Define Service Server Ports

- Server Ports: UDP ANY-2222
 - Opened Ports: UDP ANY-3333
- Select the *Add port triggering rule* check-box next to your service description in the general *Port triggering* screen to enable port redirection.

Edit service

Service name:	<input type="text" value="g_server"/>
Service description:	<input type="text" value="Gaming Server"/>

Server ports

Protocol	Server ports	Action
UDP	any -> 2222	<input checked="" type="checkbox"/>
New server ports >>		

Opened ports

Protocol	Opened ports	Action
UDP	any -> 3333	<input checked="" type="checkbox"/>
New opened ports >>		

Figure 5.13: User-Defined Service

There may be a few default port triggering rules listed when you first access

the port triggering screen. Please note that disabling these rules may result in impaired gateway functionality.

5.6 Remote Administration

In its default state, GlobeSurfer 3G blocks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may wish to enable certain services that grant remote users administrative privileges in your network. For example, you may allow yourself to view or change settings while travelling. It may also be necessary to allow your ISP to change settings or help you troubleshoot functionality or communication issues from a remote location.

Remote access is supported by the following services, and you may use the *Remote administration* screen to selectively enable these services if they are needed.

Allow Incoming Access to the Telnet Server
<input type="checkbox"/> Using Primary Telnet Port (23)
<input type="checkbox"/> Using Secondary Telnet Port (8023)
<input type="checkbox"/> Using Secure Telnet over SSL Port (992)
Allow Incoming Access to the Web-Management
<input checked="" type="checkbox"/> Using Primary HTTP Port (80)
<input checked="" type="checkbox"/> Using Secondary HTTP Port (8080)
<input checked="" type="checkbox"/> Using Primary HTTPS Port (443)
<input checked="" type="checkbox"/> Using Secondary HTTPS Port (8443)
Allow SNMP Control and Diagnostic Requests
<input type="checkbox"/> Allow Incoming SNMP Requests
Diagnostic Tools
<input type="checkbox"/> Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)
<input type="checkbox"/> Allow Incoming UDP Traceroute Queries

Figure 5.14: Remote Administration

- To allow remote access to GlobeSurfer 3G services:
 1. Click the *Remote administration* icon on the *Advanced* screen of the management console, or select the *Remote administration* tab on the *Security* screen. The *Remote administration* screen will appear (see figure 6.49).
 2. Select the services that you would like to make available to remote computers on the Internet. These services include:
 - Allow incoming access to the Telnet server** Used to allow command-line access to all system settings and parameters (using a telnet client). While this service is password-protected, it is not considered a secure protocol. If a local server is configured to use port 23 select port 8023 to avoid conflicts.

Allow incoming access to the Web management Used to allow password-protected management console access to all system settings and parameters (using a browser). Both secure (HTTPS) and non-secure (HTTP) access is available. If a local server is configured to use port 80 select port 8080 to avoid conflicts.

Allow SNMP control and diagnostic requests Used to allow access to incoming SNMP requests.

Diagnostic tools Used for troubleshooting and remote system management by you or your Internet Service Provider.

3. Click *OK* to save your changes.

Note: Telnet and Web management may be used to modify settings of the firewall or disable it. The user may also change local IP addresses and other settings, making it difficult or impossible to access the GlobeSurfer 3G from the local network. Therefore, remote access to Telnet or HTTP services **should be blocked** and should only be permitted when absolutely necessary.

Encrypted remote administration is done using a secure SSL connection, that requires an SSL certificate. When accessing GlobeSurfer 3G for the first time using encrypted remote administration, you will be prompted by your browser with a warning regarding certificate authentication. This is due to the fact that GlobeSurfer 3G's SSL certificate is self generated. When encountering this message under these circumstances, ignore it and continue. The self generated certificate is safe, and provides you with a secure SSL connection.

It is also possible to assign a user-defined certificate to GlobeSurfer 3G. To learn about certificates, see Section [6.9](#).

5.7 IP-Hostname Filtering

You may configure GlobeSurfer 3G to block specific Internet web sites so that they can not be accessed from computers in the local network. Moreover, restrictions can be applied to a comprehensive, automatically updated, table of sites to which access is not recommended.

- To view the table of web sites currently being blocked: Click the *IP/Hostname filtering* tab (see figure 5.15).

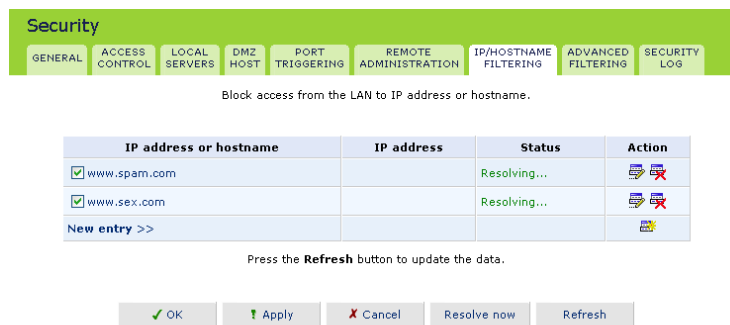


Figure 5.15: IP/Hostname Filtering

- To add a new web site to the table of web sites currently being blocked:
 1. Click the *New entry* button. The *Restricted IP address or hostname* screen will appear (see figure 5.15).
 2. Enter the web site address (IP or URL) that you would like to make inaccessible from your local network (all web pages within the site will also be blocked). If the web site address has multiple IP addresses, GlobeSurfer 3G will resolve all additional addresses and automatically add them to the restrictions table.
 3. You can select (this is optional, not compulsory) the group of computers to which you would like to apply the filtering rule. You can either select from a predefined table of groups by selecting one from the *Applied to* combo box, or create a new group by clicking the *New* link. To learn how to create groups to which you can apply rules, see Section 6.6.
 4. You can define (this is optional, not compulsory) the time period during which the rule will take effect. You can either select from a predefined table of schedules by selecting one from the *Schedule* combo box, or create a new schedule by clicking the *New* link. To learn how to create a new time schedule, see Section 6.11.
 5. Click *OK* to add the web site to the table. You will be returned to the previous screen while GlobeSurfer 3G attempts to find the site. *Resolving...* will appear in the Status column while the site is being located (the URL is being *resolved* into one or more IP addresses).

-
6. If the site is successfully located then *Resolved* will appear in the status bar, otherwise *Hostname Resolution Failed* will appear. Click the *Refresh* button to update the status if necessary. In case GlobeSurfer 3G fails to locate the web site, do the following:
 - Use a web browser to verify that the web site is available. If it is then you probably entered the web site address incorrectly. See below *To modify a web site address currently in the table*.
 - If the web site is not available return to the restrictions list screen at a later time and click the *Resolve now* button to verify that the web site can be found and blocked by GlobeSurfer 3G.

Restricted IP address or hostname

Enter the IP address or hostname you wish to block:

IP address or hostname:	<input type="text" value="www.sitename.com"/>
Applied to:	<input type="button" value="Entire LAN"/> <input type="button" value="New"/>
Schedule:	<input type="button" value="Always"/> <input type="button" value="New"/>

Figure 5.16: Restricted Web Site Address

- To modify a web site address currently in the table:
 1. Click the *Edit* icon that appears in the Action column. The *Restricted IP address or hostname* screen will appear (see figure 5.16).
 2. Modify the web site address, group and schedule as necessary. If it is long and/or complicated you may want to use your browser's copy and paste functions to copy the address from the address bar to the management console. Be sure to omit the 'http://' at the beginning and the '/' at the end of the address.
 3. Click *OK* to save your changes.
- To ensure that all current IP addresses corresponding to web sites in the table are blocked:
 1. Click the *Resolve now* button. GlobeSurfer 3G will check each of the web site addresses in the table and ensure that all IP addresses at which this web site can be found are included in the IP addresses column.

You may disable a restriction and make the web site available again without having to remove the site from the restrictions list. This may be useful if you wish to make the web site available only temporarily and expect that you will want to block it again in the future.

- To temporarily disable a restriction: clear the check box next to the restricted URL.
- To reinstate the restriction at a later time: select the check box next to the URL.

-
- To remove a restriction: click the **Remove** button. The restriction will be removed from the restrictions list.

5.8 Advanced Filtering

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.

To access the Advanced Filtering screen, select the *Advanced Filtering* tab. The *Advanced Filtering* screen will appear (see figure 5.17).

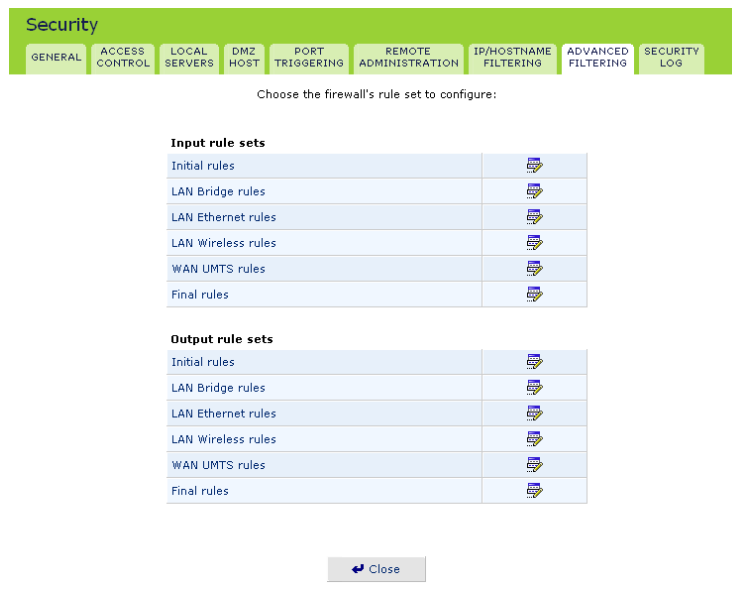


Figure 5.17: Advanced Filtering

You can configure two sets of rules, Input rules and Output rules. Each set of rules is comprised of three subsets: Initial rules, Network devices rules and Final rules. These subsets determine the sequence by which the rules will be applied. Following is a description of the set ordering for inbound and outbound packets.

Inbound packets – Input rule sets

- Initial rules.
- All rules defined for the network device on which the packet is.
- Local servers rules from the *Local servers* tab in the security screen.
- Rules to accept all the packets on a device in case the firewall check box *Internet connection firewall* in the connection settings screen is unchecked.
- Remote administration rules from the *Remote administration* tab.
- DMZ host rules from the *DMZ host* tab.
- Final rules.

Outbound packets – Output rules sets

- Initial rules.
- All rules defined for the network device on which the packet is.
- Rules to accept all the packets on a device in case the firewall check box *Internet connection firewall* in the connection settings screen is unchecked.
- IP/hostname filtering rules and access control rules from the tabs in the security screen.
- Final rules.

There are numerous rules automatically inserted by the firewall in order to provide improved security and block harmful attacks.

To configure advanced filtering rules, click the *Edit* button next to the rule title, or click on the title directly. The *Configure rules* screen will appear, displaying the entries currently constituting the rule subset you selected (see figure 5.18).



Figure 5.18: Configure Advanced Filtering Rules

Use the action buttons in the *Action* column to add, edit or delete rules.

5.8.1 Adding an Advanced Filtering Rule

To add an advanced filtering rule, carefully define the following rule parameters:

Add advanced filter

Matching	
Source IP address:	<input type="text" value="Any"/>
Destination IP address:	<input type="text" value="Any"/>
<input type="checkbox"/> IP fragments	
Operation	
<input checked="" type="radio"/> Drop	(11)
<input type="radio"/> Reject	
Drop packets, and send TCP Reset or ICMP Host Unreachable packets to sender.	
<input type="radio"/> Accept	
Accept all packets related to this session. This session is handled by Stateful Packet Inspection (SPI).	
<input type="radio"/> Accept packet	
Accept packets matching this rule only. Do not use Stateful Packet Inspection (SPI) to also automatically accept packets related to this session.	
Logging	
<input type="checkbox"/> Log packets matched by this rule.	
Scheduler	
Schedule:	Always New

Figure 5.19: Configure Advanced Filtering Rules

1. Matching

To apply a firewall rule, a matching must be made between IP addresses or ranges and ports. Use the *Source IP* and *Destination IP* to define the coupling of source and destination traffic. Port matching will be defined when selecting services (see step 5). For example, if you select the FTP service, port 21 will be checked for matching traffic flow between the defined source and destination IPs.

2. Operation

This is where you define what action the rule will take, by selecting one of the following radio buttons:

- **Drop:** Deny access to packets that match the source and destination IP addresses and service ports defined in *Matching*.
- **Reject:** Deny access to packets that match the source and destination IP addresses and service ports defined in *Matching* and sends and sends an ICMP error or a TCP reset to the origination peer.
- **Accept:** Allow access to packets that match the source and destination IP addresses and service ports defined in *Matching*. The data transfer session will be handled using Stateful Packet Inspection (SPI).
- **Accept packet:** Allow access to packets that match the source and destination IP addresses and service ports defined in *Matching*. The data transfer session will not be handled using Stateful Packet Inspection (SPI), meaning that other packets that match this rule will not be automatically allowed access. For example, this can useful when creating rules that allow broadcasting.

3. **Logging**

Select this check-box to add entries relating to this rule to the security log (this is optional, not compulsory).

4. **Scheduler**

Select or create a schedule for the rule. A schedule sets the time period during which the rules are active/inactive. For information on how to configure Scheduler Rules refer to [6.11](#).

5. **Services**

Select the services to which you would like to apply this rule. You can add user defined services by clicking the *New user-defined service*. Detailed instruction on how to add user defined services are described in [Section 5.10](#).

5.9 Security Log

The security log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface (GlobeSurfer 3G management console or Telnet terminal), firewall configuration and system start-up.

Time	Event	Event-Type	Details
Jun 14 16:00:08 2004	WBM Login	User authentication success	Username: admin
Jun 14 15:12:26 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 15:12:26 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 14 14:24:41 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 14:24:41 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 13 13:01:01 2004	WBM Login	User authentication success	Username: admin [repeated 6 times, last time on Jun 14 14:23:16 2004]
Jun 13 13:00:26 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 13 13:00:26 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 13 12:59:25 2004	CLI Login	User authentication success	Username: admin

Figure 5.20: Security Log

To view the Security Log, select the *Security Log* tab which appears on the *Security* screen (see figure 5.20).

The columns of the Security Log table show the following information:

Time The time the event occurred.

Event There are five kinds of events:

- Inbound traffic: The event is a result of an incoming packet.
- Outbound traffic: The event is a result of outgoing packet.
- Firewall setup: Configuration message.
- WBM Login: Indicates that a user has logged in to WBM.
- CLI Login: Indicates that a user has logged in to CLI (via Telnet).

Event type Textual description of the event (see full description below).

- Blocked: Means that the packet was blocked. Message is colored red.
- Accepted: Means that the packet was accepted. Message is colored green, e.g. *User authentication success*.

Details More details about the packet or the event, Such as protocol, IP addresses, ports, etc.

The following are the available event types that can be recorded in the firewall log:

1. Firewall internal - from the firewall internal mechanism, in case this event-type is recorded, an accompanying explanation will be added.

-
2. Firewall status changed - the firewall changed status from up to down or the other way around, as specified in the event type description.
 3. STP packet - an STP packet has been accepted/rejected.
 4. Illegal packet options - the options field in the packet's header is either illegal or forbidden.
 5. Fragmented packet - a fragment has been rejected.
 6. WinNuke protection - a WinNuke attack has been blocked.
 7. ICMP replay - an ICMP replay message has been blocked.
 8. ICMP redirect protection - an ICMP redirected message has been blocked.
 9. Packet invalid in connection - a packet has been blocked because of it being on an invalid connection.
 10. ICMP protection - a broadcast ICMP message has been blocked.
 11. Broadcast/Multicast protection - a packet with a broadcast/multicast source IP has been blocked.
 12. Spoofing protection - a packet from the WAN with a source IP of the LAN has been blocked.
 13. DMZ network packet - a packet from a demilitarized zone network has been blocked.
 14. Trusted device - a packet from a trusted device has been accepted.
 15. Default policy - a packet has been accepted/blocked according to the default policy.
 16. Remote administration - a packet that is designated for GlobeSurfer 3G management has been accepted/blocked.
 17. Access control - a packet has been accepted/blocked because of an access control rule.
 18. Parental control - a packet has been blocked because of parental control.
 19. NAT out failed - NAT failed for this packet.
 20. DHCP request - GlobeSurfer 3G sent a DHCP request (depends on the distribution)
 21. DHCP response - GlobeSurfer 3G received a DHCP response (depends on the distribution)
 22. DHCP relay agent - a DHCP relay packet has been received (depends on the distribution)
 23. IGMP packet - an IGMP packet has been accepted.
 24. Multicast IGMP connection - a multicast packet has been accepted.
 25. RIP packet - a RIP packet has been accepted.
 26. PPTP connection - a packet inquiring whether GlobeSurfer 3G is ready to receive a PPTP connection has been accepted.
 27. Kerberos key management 1293 - security related, for future use.
 28. Kerberos 88 - for future use.

-
29. AUTH:113 request - an outbound packet for AUTH protocol has been accepted (for maximum security level).
 30. Packet-Cable - for future use.
 31. IPV6 over IPV4 - an IPv6 over IPv4 packet has been accepted.
 32. ARP - an ARP packet has been accepted.
 33. PPP Discover - a PPP discover packet has been accepted.
 34. PPP Session - a PPP session packet has been accepted.
 35. 802.1Q - a 802.1Q (VLAN) packet has been accepted.
 36. Outbound Auth1X - an outbound Auth1X packet has been accepted.
 37. IP Version 6 - an IPv6 packet has been accepted.
 38. GlobeSurfer 3G initiated traffic - all traffic that GlobeSurfer 3G initiates is recorded.
 39. Maximum security enabled service - a packet that is accepted because it belongs to a permitted service in the maximum security level.
 40. SynCookies Protection - a SynCookies packet has been blocked.
 41. ICMP Flood Protection - a packet has been blocked, stopping an ICMP flood.
 42. UDP Flood Protection - a packet has been blocked, stopping a UDP flood.
 43. Service - a packet has been accepted because of a certain service, as specified in the event type.
 44. Advanced Filter Rule - a packet has been accepted/blocked because of an advanced filter rule.
 45. Fragmented packet, header too small - a packet has been blocked because after the defragmentation, the header was too small.
 46. Fragmented packet, header too big - a packet has been blocked because after the defragmentation, the header was too big.
 47. Fragmented packet, drop all - not used.
 48. Fragmented packet, bad align - a packet has been blocked because after the defragmentation, the packet was badly aligned.
 49. Fragmented packet, packet too big - a packet has been blocked because after the defragmentation, the packet was too big.
 50. Fragmented packet, packet exceeds - a packet has been blocked because after the defragmentation, the packet exceeded.
 51. Fragmented packet, no memory - a fragmented packet has been blocked because there is no memory for fragments.
 52. Fragmented packet, overlapped - a packet has been blocked because after the defragmentation, there were overlapping fragments.
 53. Defragmentation failed - the fragment has been stored in memory, and blocked, until all fragments have arrived and defragmentation can be performed.

-
54. Connection opened - usually debug message regarding connection.
 55. Wildcard connection opened - usually debug message regarding connection.
 56. Wildcard connection hooked - usually debug message regarding connection.
 57. Connection closed - usually debug message regarding connection.
 58. Echo/Chargen/Quote/Snork protection - a packet has been blocked, protecting from Echo/Chargen/Quote/Snork.
 59. First packet in connection is not a SYN packet - a packet has been blocked because of a TCP connection that has started without a SYN packet.
 60. Error : No memory - a message notifying that a new connection has not been established because of lack of memory.
 61. NAT Error : connection pool is full. No connection created - a message notifying that a connection has not been created because the connection pool is full.
 62. NAT Error: No free NAT IP - a message notifying that there is no free NAT IP, therefore NAT has failed.
 63. NAT Error: Conflict Mapping already exists - a message notifying that there is a conflict since the NAT mapping already exists, therefore NAT has failed.
 64. Malformed packet: Failed parsing - a packet has been blocked because it is malformed.
 65. Passive attack on ftp-server: Client attempted to open Server ports - a packet has been blocked.
 66. FTP port request to 3rd party is forbidden (Possible bounce attack) - a packet has been blocked.
 67. Firewall Rules were changed - the firewall rule set has been modified.
 68. User authentication - a message during login time, including both successful and failed authentication.

5.9.1 Security Log Settings

Security log settings

Accepted events

- Accepted incoming connections
- Accepted outgoing connections

Blocked events

- Blocked connection attempts
- Winnuke
- Defragmentation error
- Blocked fragments
- Syn flood
- Echo Chargen
- Multicast/Broadcast
- Spoofed connection
- Illegal packet options
- UDP flood
- ICMP replay
- ICMP redirect
- ICMP multicast
- ICMP flood

Other events

- Remote administration attempts
- Connection states

Log buffer

- Prevent log overrun

OK Apply Cancel

Figure 5.21: Security Log Settings

To view or change the firewall log settings:

1. Click the *Settings* button that appears at the top of the *Firewall Log* screen. The *Security Log Settings* screen will appear (see figure 5.21).
2. Select the types of activities for which you would like to have a log message generated:
 - Accepted incoming connections: write a log message for each successful attempt to establish an inbound connection to the local network.
 - Accepted outgoing connections: write a log message for each successful attempt to establish an outgoing connection to the public network.
 - Blocked connection attempts: write a log message for each blocked attempt to establish an inbound connection to the local network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.
 - Specify the blocked events that should be monitored. Use this to monitor specific event such as synflood. A log message will be generated if either the corresponding check-box is checked, or the *Blocked connection attempts* check-box is checked.
 - Remote administration attempts: write a log message for each remote-administration connection attempt, whether successful or not.

-
- **Connection states:** Give extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).
 - Select the *Prevent log overrun* checkbox in order to stop logging firewall activities when the memory allocated for the log fills up.
3. Click *OK* to save your changes and return to the *Firewall Log* screen.

5.10 User-defined Services

The tables that appear on the *Add access control rule*(see figure 5.4) and *Add local server*(see figure 5.7) screens are pre-configured to include most of the services that users may wish to block or activate. Sometimes, however, the need arises to add a new service. GlobeSurfer 3G provides the *User-defined services* table (see figure 5.22) for this purpose. This table can be accessed from the *Add access control rule* and *Add local server* screens. When a service is added in one place it automatically appears in the other. In this way, user-defined services never need to be entered twice.

- To add a new service:
 1. Click the *New user-defined service* link at the top of either the *Add access control rule* screen or the *Add local server* screen. The *Edit service* screen will appear (see figure 5.22).

Server ports		
Protocol	Server ports	Action
UDP	20000 -> 20000-65535	
New server ports >>		

Figure 5.22: User-Defined Services

2. Enter a name for the service.
3. Enter a description for the service.
4. Click the *New server ports* link. The *Edit service server ports* screen will appear (see figure 5.23).

Protocol	UDP
Source ports:	Single 20000
Destination ports:	Range 20000 - 65535

Figure 5.23: User -Defined Services

5. Choose the source and/or destination port types and enter the port number or range for this service to use appropriately. This information is usually available as part of the documentation that accompanies the program that needs access to or from the Internet.

6. Click *OK* to save your changes and return to the previous screen.

Note: You have now completed defining this service, and may go to the *Add access control rule* or *Add local server* screen to block or activate the service. Refer to sections [5.2](#) and [5.3](#) for further instruction.

- To modify a user-defined service:
 1. Click the **Edit** button for the service. The *Edit service* screen will appear (see figure [5.22](#)).
 2. Modify the service name or description as necessary.
 3. To modify the port settings, click the **Edit** button for the server port and change the settings as described above.
 4. Click *OK* to save your changes and return to the previous screen.
- To remove a user-defined service:
 1. Click the **Remove** button for the service. The service will be removed from the list.

5.11 Applying Corporate-Grade Security

The following set of instructions is designed to assist you in applying corporate-grade security standards to your network. When implementing these instructions, it is important to execute the configuration steps in the exact order they are presented.

To apply corporate-grade firewall security standards perform the following:

- Do not allow non-administrative services access to the LAN:
 1. Open a Telnet session from a LAN host that is connected to GlobeSurfer 3G.
 2. Telnet to GlobeSurfer 3G at address 192.168.1.1.
 3. Logon to GlobeSurfer 3G as an administrator (The default username and password are both *admin*).
 4. After logging on, issue the following command at the prompt:

```
OpenRG> rg_conf_set fw/protect/allow_rg_remote_administration_only 1
OpenRG> reconf 1
OpenRG> exit
```

- Configure GlobeSurfer 3G to permit only HTTPS as means of remote administration:
 1. Click *Security* on the sidebar.
 2. Click the *Remote Administration* tab.
 3. Enable the following check boxes:
 - Using Primary HTTPS Port (443)
 - Using Secondary HTTPS Port (8443)

Allow Incoming Access to the Telnet Server	
<input type="checkbox"/>	Using Primary Telnet Port (23)
<input type="checkbox"/>	Using Secondary Telnet Port (8023)
<input type="checkbox"/>	Using Secure Telnet over SSL Port (992)
Allow Incoming Access to the Web-Management	
<input type="checkbox"/>	Using Primary HTTP Port (80)
<input type="checkbox"/>	Using Secondary HTTP Port (8080)
<input checked="" type="checkbox"/>	Using Primary HTTPS Port (443)
<input checked="" type="checkbox"/>	Using Secondary HTTPS Port (8443)
Allow SNMP Control and Diagnostic Requests	
<input type="checkbox"/>	Allow Incoming SNMP Requests
Diagnostic Tools	
<input type="checkbox"/>	Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)
<input type="checkbox"/>	Allow Incoming UDP Traceroute Queries

Figure 5.24: Enabling Secure Remote Administration

4. Click *OK* to save your changes.
- Apply firewall protection on the LAN:
 1. Click *Network Connections* on the sidebar.
 2. Click the *LAN Ethernet* connection link.
 3. Click the *Settings* button.
 4. Enable the *Internet Connection Firewall* check box.

Lease Time In Minutes:	<input type="text" value="60"/>
<input checked="" type="checkbox"/>	Provide Host Name If Not Specified by Client
Routing	Basic
Internet Connection Firewall	<input checked="" type="checkbox"/> Enabled
Allow Unrestricted Administration	<input type="checkbox"/> Enabled
Additional IP Addresses	New IP Address >>

Figure 5.25: Apply Firewall Protection

5. Click *OK* to save your changes.

At this point you have set your firewall to corporate-grade security. If you wish to allow additional LAN services, or other outbound services, refer to the *Advanced Filtering* Section 5.8.

6

Advanced

This section of the GlobeSurfer 3G management console is intended primarily for more advanced users. Some changes to settings within this section could adversely affect the operation of GlobeSurfer 3G and your local network, and should be made with caution.

From the *Advanced* screen you can access the following advanced settings by clicking their respective icons.



DNS Server: View and modify the DNS Hosts table (see Section 6.2)



Network Map: Display a map representation of your current local network (see Section 6.4)



DHCP: Modify the behavior of the DHCP server for each LAN device and view a list of DHCP clients in the local network (see Section 6.5)



Network objects: Define groups of LAN devices for system rules (see Section 6.6)



















Routing: Manage routing policies (see Section 6.7)



Users: Configure remote VPN clients (see Section 6.8)



Certificates: Manage digital certificates (see Section 6.9)

-
-  **Date and time:** Set the local date and time (see Section 6.10)
-  **Scheduler rules:** Define time segments for system rules (see Section 6.11)
-  **Firmware upgrade:** Perform a firmware upgrade (see Section 6.12)
-  **PPTP:** Configure Point-to-Point Tunneling Protocol parameters (see Section 6.13)
-  **IPsec:** Configure IPsec parameters (see Section 6.14)
-  **Universal Plug and Play:** Configure Universal Plug and Play (UPnP) parameters (see Section 6.15)
-  **Simple Network Management Protocol:** Configure GlobeSurfer 3G's SNMP agent (see Section 6.16)
-  **System settings:** Modify administrator settings, including GlobeSurfer 3G's hostname (see Section 6.1)
-  **Diagnostics:** Perform networking diagnostics (see Section 6.17)
-  **Remote administration:** Configure remote administration privileges (see Section 6.18)
-  **SIM Setup:** Change the settings of the SIM (see Section 6.19)
-  **Unlock device:** Unlock the GlobeSurfer 3G (see Section 6.20)
-  **SMS Manager:** Send, read and manage SMS messages (see Section 3)
-  **Restore defaults:** Restore default factory settings (see Section 6.21)
-  **Restart:** Restart the GlobeSurfer 3G (see Section 6.22)
-  **Technical information:** View technical information, including version number (see Section 6.23)

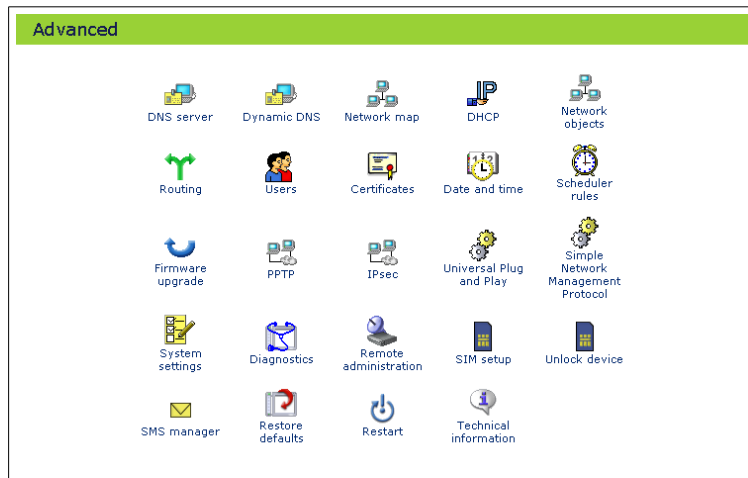
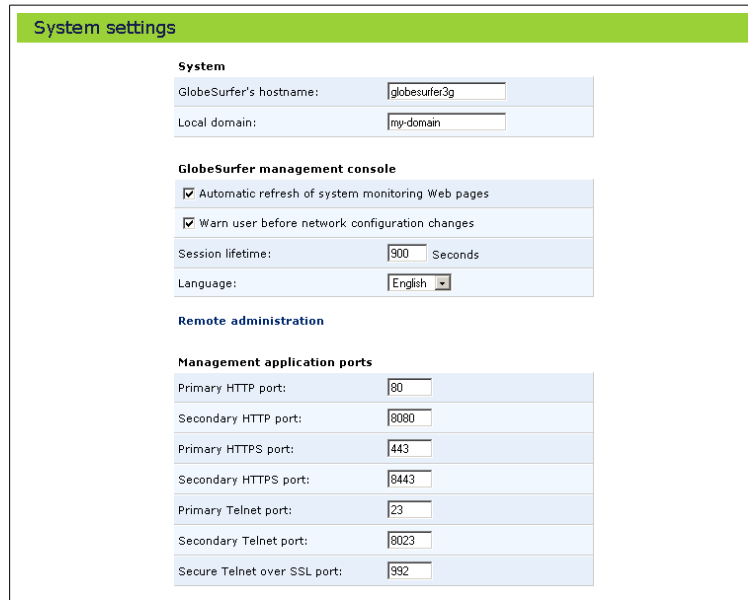


Figure 6.1: Advanced Settings

6.1 System Settings

The system settings screen allows you to configure various system and management parameters.



The screenshot shows the 'System settings' web interface. It is organized into several sections:

- System**: Contains two input fields: 'GlobeSurfer's hostname' with the value 'globesurfer3g' and 'Local domain' with the value 'my-domain'.
- GlobeSurfer management console**: Contains two checked checkboxes: 'Automatic refresh of system monitoring Web pages' and 'Warn user before network configuration changes'. It also has a 'Session lifetime' field set to '900' with the unit 'Seconds', and a 'Language' dropdown menu set to 'English'.
- Remote administration**: This section is further divided into 'Management application ports', which includes seven input fields for different protocols:
 - Primary HTTP port: 80
 - Secondary HTTP port: 8080
 - Primary HTTPS port: 443
 - Secondary HTTPS port: 8443
 - Primary Telnet port: 23
 - Secondary Telnet port: 8023
 - Secure Telnet over SSL port: 992

Figure 6.2: System Settings

6.1.1 System

Use this section to configure the following:

1. Specify the GlobeSurfer 3G host name. The host name is the URL address of the GlobeSurfer 3G.
2. Specify your network's local domain.

6.1.2 GlobeSurfer 3G Management Console Settings

Use this section to configure the following:

Automatic refresh of system monitoring web pages Select this checkbox to enable the automatic refresh of system monitoring web pages.

Warn user before network configuration changes Select this checkbox to activate user warnings before network configuration changes take effect.

6.1.3 Management Application Ports Settings

This section allows you to configure the following management application ports:

-
1. Primary/secondary HTTP ports
 2. Primary/secondary HTTPS ports
 3. Primary/secondary Telnet ports
 4. Secure Telnet over SSL ports

6.1.4 System Logging Settings

Use this section to configure the following:

1. System log buffer size
2. Remote system notify level
 - None
 - Error
 - Warning
 - Information

6.1.5 Security Logging Settings

Use this section to configure the following:

1. Security log buffer size
2. Remote security notify level
 - None
 - Error
 - Warning
 - Information

6.1.6 Outgoing Mail Server Settings

Use this section to configure the following:

1. Enter the hostname of your outgoing (SMTP) server in the *Server* field.
2. Each email requires a *from* address and some outgoing servers refuse to forward email without a valid *from* address for anti-spam considerations. Enter a *from* email address in the *From email address* field.
3. If your outgoing email server requires authentication check the *Server requires authentication* checkbox and enter your username and password in the *Username* and *Password* fields respectively.

6.1.7 HTTP interception

By default the GlobeSurfer 3G is configured to intercept HTTP access to Internet web sites when no Internet connection is established. Interception means that you are directed to a page with information on how to connect the GlobeSurfer 3G to the Internet.

6.2 DNS Server

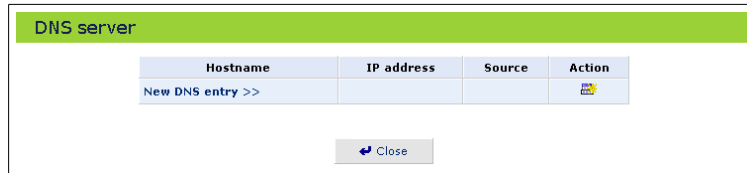
Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa. The DNS server of the GlobeSurfer 3G is an auto-learning DNS, which means that when a new computer is connected to the network the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address.


In addition, the DNS server:

- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the LAN simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using the GlobeSurfer 3G management console.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

6.2.1 Viewing and Modifying the DNS Table



Hostname	IP address	Source	Action
New DNS entry >>			

[Close](#)

Figure 6.3: DNS Table

- To view the list of computers stored in the DNS table:
 1. Click *DNS server* on the *Advanced* screen of the management console. The DNS table is displayed, showing the list of computers stored (see figure 6.3).

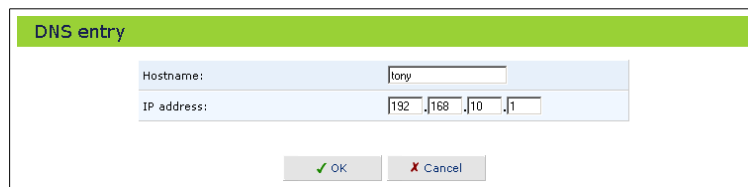


Figure 6.4: Add or Edit a DNS Entry

- To add a new entry to the DNS table:
 1. Click the *New DNS entry* link. The *DNS entry* screen will appear (see figure 6.4).
 2. Enter the computer's host name and IP address.
 3. Click *OK* to save your changes.
- To edit the host name or IP address of an entry:
 1. Click the *Edit* icon in the *Action* column. The *DNS entry* screen will appear (see figure 6.4).
 2. If the host was manually added to the DNS Table then you may modify its host name and/or IP address, otherwise you may only modify its host name.
 3. Click *OK* to save your changes.
- To remove a host from the DNS table:
 1. Click the *Delete* icon that appears in the *Action* column. The entry will be removed from the table.

6.3 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static host name, allowing your computer to be more easily accessible from various locations on the Internet. Typically, when you connect to the Internet, your service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, whilst maintaining a constant domain name. Each time the IP address provided by your ISP changes, the DNS database will change accordingly to reflect the change in IP address. In this way, even though a domain name's IP address will change often, your domain name will still be accessible.

To be able to use the Dynamic DNS feature you must open a DDNS account, free of charge, at

<http://www.dyndns.org/account/create.html>

When applying for an account, you will need to specify a user name and password. Please have them readily available when customizing GlobeSurfer 3G's DDNS support. For more information regarding Dynamic DNS, please refer to <http://www.dyndns.org>.

□

Figure 6.5: Dynamic DNS Settings

6.3.1 Using Dynamic DNS

1. Click *Dynamic DNS* on the *Advanced* screen of the Management Console. The *Dynamic DNS* table will appear (see figure 6.5).

2. Specify the Dynamic DNS parameters:

Connection to Update Select the connection to which you would like to couple the Dynamic DNS service.

Offline Enable the Dyndns offline feature by selecting this check box. This feature is available only to users who have purchased some type of upgrade credit from Dyndns.org. Please note that changing the redirection URL can only be performed via the Dyndns web site.

Username Enter your Dyndns user name.

Password Enter your Dyndns password.

Hostname Enter a your full Dyndns domain.

Wildcard Select the *Wildcard* checkbox if you want anything-here.yourhost.dyndns.org to work (i.e. to make things like www.yourhost.dyndns.org work).

Mail Exchanger Enter your mail exchange server address, to redirect all e-mails arriving at your Dyndns address to your mail server.

Backup MX Select this check box to designate the mail exchange server to be a backup server.

6.4 Network Map

The network map depicts the various elements and connections that currently constitute your local network.

To display the network map:

1. Click the *Advanced* icon on the sidebar.
2. Click the *Network Map* icon. The *Network Map* screen will appear.

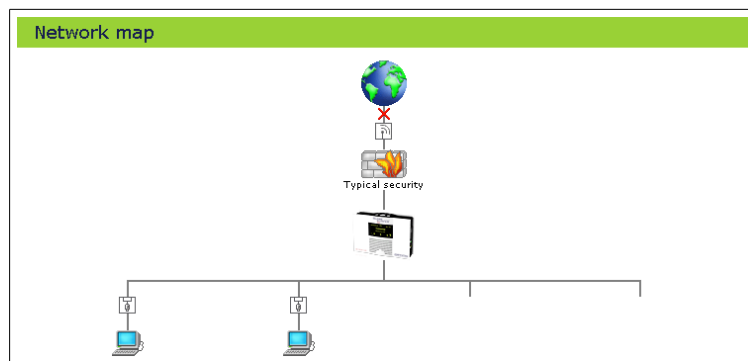





Figure 6.6: Network Map

From top going down:

1. External network interface (Internet connection)
2. Firewall
3. GlobeSurfer 3G
4. Internal network interface (Ethernet or WLAN)
5. Local network computers and peripherals

Clicking a network element takes you to a configuration screen to configure the corresponding network element.

The following table explains the meaning of different network map symbols:

	Represents the Internet
	Represents the WAN UMTS connection. Click this icon to configure network parameters for the WAN UMTS connection (see Chapter 4).
	Represents the GlobeSurfer 3G firewall. The height of the wall corresponds to the security level currently selected: Minimum, Typical or Maximum. Click this icon to configure security settings (see Chapter 5).

The local network will use the following icons:



Represents an Ethernet Local Area Network (LAN) connection. Click this icon to configure network parameters for the Ethernet LAN device (see Section 4).



Represents a Wireless LAN connection. Click this icon to configure network parameters for the Wireless LAN device (see Section 4).



Represents a bridge connected in the local network. Click this icon to view the bridge's underlying devices.



Represents a computer connected in the local network. Each computer connected to the network appears below the network symbol of the network through which it is connected. Click an icon to view network information for the corresponding computer (see figure 6.7).

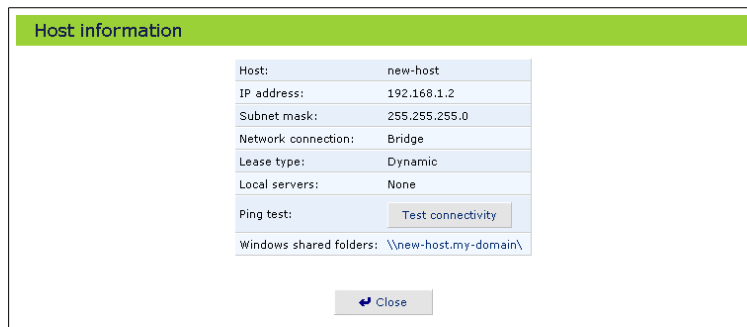


Figure 6.7: Host Information

6.5 DHCP

The DHCP server of the GlobeSurfer 3G makes it possible to easily add computers that are configured as DHCP clients to the local network. It provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to them.

A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as *taken*. At this point the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which will then make the IP address available for use by others.

The DHCP server:

- Displays a list of all DHCP hosts devices connected to GlobeSurfer 3G
- Defines the range of IP addresses that can be allocated in the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled/disabled separately for each LAN device
- Can assign a static lease to a LAN PC so that it receives the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers
- Provides the DNS server with the host name and IP address of each PC that is connected to the LAN

6.5.1 DHCP Server Summary

To view a summary of the services currently being provided by the DHCP server:

1. Click *DHCP* on the *Advanced* screen of the management console. The *DHCP* summary screen will appear (see figure 6.8).
2. Click the *Name* of a device to display the DHCP settings for that device.

Name	Service	Subnet mask	Dynamic IP range	Action
LAN Bridge	DHCP server	255.255.255.0	192.168.1.1 - 192.168.1.244	

Figure 6.8: DHCP Summary

6.5.2 DHCP Server Settings

To edit the DHCP server settings for a device:

1. Click the *Edit* icon in the *Action* column. The DHCP settings for this device will appear (see figure 6.9).
2. Choose whether to enable or disable the DHCP server for this device. This can also be done on the *DHCP Server Summary* screen.
3. Select DHCP server option from the *DHCP* drop-down menu.
4. Complete the following fields:
 - IP Address Range (*Start IP address* and *End IP address*): determines the number of hosts that may be connected to the network in this subnet. *Start IP address* specifies the first IP address that may be assigned in this subnet and *End IP address* specifies the last IP address in the range.
 - Subnet Mask: A mask used to determine what subnet an IP address belongs to. An example of a subnet mask value is 255.255.0.0.
 - Lease Time: each device will be assigned an IP address by the DHCP server for a limited time (*Lease Time*) when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, then the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.
 - Provide host name if not specified by client: If the DHCP client does not have a host name, the GlobeSurfer 3G will assign the client a default name.
5. Click *OK* to save your changes.

DHCP settings for LAN Bridge

Service
 DHCP:

DHCP server
 Start IP address: . . .
 End IP address: . . .
 Subnet mask: . . .
 WINS server IP address: . . .
 Lease time in minutes:
 Provide hostname if not specified by client

Figure 6.9: DHCP Settings

6.5.3 DHCP Server Relay Settings

To edit the DHCP server relay settings:

1. Click the *Edit* icon in the *Action* column (see figure 6.8).
2. Select the DHCP relay option from the *DHCP* drop-down menu.
3. Click the *New IP Address* link under the *DHCP Relay* section. The *DHCP Server Relay Address* screen will appear (see figure 6.10). Use this screen to specify your DHCP server's IP address.

DHCP Relay server address



IP address: . . .

Figure 6.10: DHCP Server Relay

4. Click *OK* to save your changes.

6.5.4 DHCP Connections

To view a list of computers currently recognized by the DHCP server click the *Connection List* button that appears at the bottom of the *DHCP* screen. The *DHCP Connections* screen is displayed (see 6.11).

DHCP connections							
Hostname	IP address	Physical address	Lease type	Connection name	Status	Expires in	Action
d-bates-ws	192.168.1.3	00:08:74:41:61:9e	Dynamic	LAN Bridge	Active	57 minutes	 
New static connection >>							

Press the **Refresh** button to update the data.

Figure 6.11: DHCP Connections

Note: If a device is listed as *Disabled* in the Status column then DHCP services are not being provided to hosts connected to the network through that device. This means that the GlobeSurfer 3G will not assign IP addresses to these computers—useful if you wish to work with static IP addresses only.

- To edit the properties for a static connection:
 - Click the *Edit* icon that appears in the *Action* column. The *DHCP Connection Settings* screen will appear (see figure 6.12).

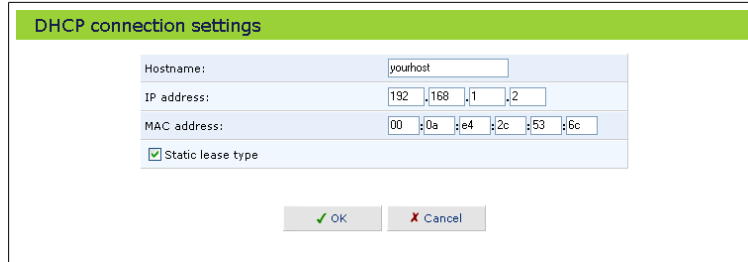
DHCP connection settings	
Hostname:	<input type="text"/>
IP address:	<input type="text"/> <input type="text"/> <input type="text"/>
MAC address:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input checked="" type="checkbox"/> Static lease type	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 6.12: DHCP Connection Properties

- Continue with step 2 below.
 - To define a new connection with a fixed IP address:
 - Click the *New Static Connection* button that appears on top of the *DHCP Connections* screen. The *DHCP Connection Settings* screen will appear (see figure 6.13).
 - Enter a host name for this connection.
 - Enter the fixed IP address that you would like to have assigned to the computer.
 - Enter the MAC address of the computer's network card.
 - Click *OK* to save your changes.

Note: A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

-
- To remove a host from the table click the *Delete* icon in the *Action* column.



The image shows a dialog box titled "DHCP connection settings" with a green header. It contains the following fields and options:

Hostname:	yourhost
IP address:	192 . 168 . 1 . 2
MAC address:	00 : 0a : e4 : 2c : 53 : 6c
<input checked="" type="checkbox"/> Static lease type	

At the bottom of the dialog box are two buttons: "OK" with a green checkmark icon and "Cancel" with a red X icon.

Figure 6.13: Editing a DHCP Connection

6.6 Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to one or more MAC address, IP address, and hostname. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring GlobeSurfer 3G's security filtering settings such as IP address filtering, hostname filtering or MAC address filtering.

You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. Moreover, it is possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings.

To define a network object:

1. Click the *Advanced* icon on the sidebar.
2. Click the *Network objects* icon. The *Network objects* screen will appear (see figure 6.14).

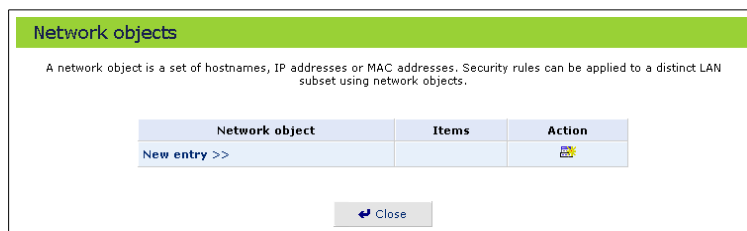


Figure 6.14: Network Objects

3. Click the *New entry* link. The *Network object* screen will appear (see figure 6.15).

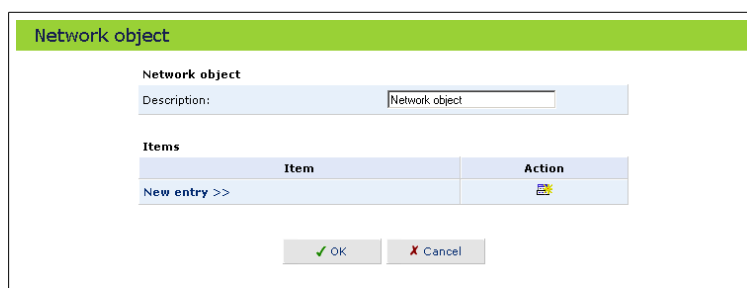
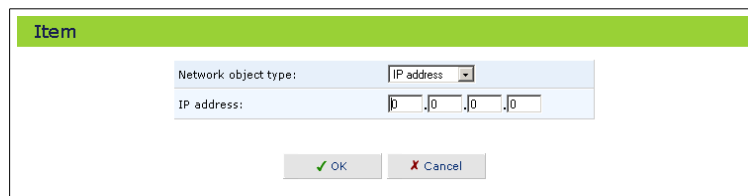


Figure 6.15: Network Object

4. Specify a name for the network object in the *Description* field.
5. Click the *New entry* link. The *Item* screen will appear (see figure 6.16).



The screenshot shows a dialog box titled "Item". It contains a "Network object type:" label with a dropdown menu currently set to "IP address". Below this is an "IP address:" label followed by four input fields, each containing the digit "0". At the bottom of the dialog are two buttons: "OK" with a green checkmark icon and "Cancel" with a red X icon.

Figure 6.16: Item

6. Select the type of the network object from the *Network object type* combo-box:
 - IP address
 - MAC address
 - Hostname
7. Specify the appropriate description for the network object type.
8. You may repeat the actions described above several times, after which you must click the *OK* button.

6.7 Routing

6.7.1 Managing Routing Table Rules

To access the routing table rules click the *Routing* icon from the *Advanced* screen. The *Routing* screen will appear (see figure 6.17).

Name	Destination	Gateway	Netmask	Metric	Status	Action
New route >>						

Routing protocols

Routing Information Protocol (RIP)

Multicasting

OK Apply Cancel

Figure 6.17: Routing Rules

You can add, edit and delete routing rules from the routing table in the manner described in Section 2.5. When adding a routing rule, you need to specify:

- **Name:** Select the type of network device (LAN Bridge or WAN UMTS)
- **Destination:** The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
- **Netmask:** The network mask is used in conjunction with the destination to determine when a route is used.
- **Gateway:** Enter the IP address of the GlobeSurfer 3G.
- **Metric:** A measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.

Route settings

Name: LAN Bridge

Destination: 192.168.2.1

Netmask: 255.255.255.255

Gateway: 192.168.1.1

Metric: 20

OK Apply Cancel

Figure 6.18: Routing Rule Settings

6.7.2 Multicasting

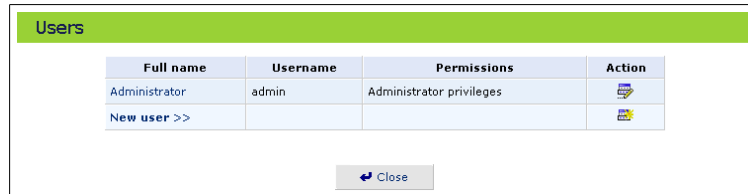
GlobeSurfer 3G provides support for IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a pre-defined group of recipients. When you join a multicast group you will receive all messages addressed to the group, much like what happens when an e-mail message is sent to a mailing list.



IGMP multicasting enables UPnP capabilities over wireless networks and may also be useful when connected to the Internet through a router. When an application running on a computer in the local network sends out a request to join a multicast group GlobeSurfer 3G intercepts and processes the request.

1. Click *Routing* on the *Advanced* screen of the management console (see figure 6.17).
2. Select the check-box for *Multicasting*.
3. Click *OK*.

6.8 Managing Users

To access the list of defined remote users, click the *Users* icon from the *Advanced* screen. The *Users* table will be displayed.



Full name	Username	Permissions	Action
Administrator	admin	Administrator privileges	
New user >>			




Figure 6.19: User table

You can add, edit and delete users allowed to access the GlobeSurfer 3G and your local network by managing the user table as described in Section 2.5. To add a new user click *New user* in the table and specify the following parameters:

- **Full name:** The remote user's full name.
- **Username:** The name the remote user will use to access your local network.
- **New password:** Type a new password for the remote user. If you do not want to assign a password to the remote user leave this field empty.
- **Retype new password:** If a new password was assigned, type it again to verify correctness.
- **Permissions:** Select the remote user's privileges on your local network.
 - **Administrator privileges:** Grants remote system setting modification via the web-based management console or telnet.
 - **Remote access by PPTP:** Grants access with no system modification privileges.
 - **SMS access only:** Grants access to the SMS manager only, for example to send and read SMS messages. Other parts of the management console will be hidden and can not be accessed.

Figure 6.20: Managing Users

Please note, that changing any of the user parameters will prompt the connection associated with the user to terminate. For changes to take effect you should activate the connection manually after modifying user parameters.

You can use email notification to receive indications of system events for a predefined severity classification. The available types of events are *System* or *Security* events. The available severity of events are *Error*, *Warning* and *Information*. If the *Information* level is selected the user will receive notification of *Information*, *Warning* and *Error* events. If the *Warning* level is selected the user will receive notification of *Warning* and *Error* events etc.

To configure email notification for a specific user:

- First make sure you have configured an outgoing mail server in *System settings*. A click on the *Configure mail server* link will display the *System settings* screen where you can configure the outgoing mail server.
- Enter the user's email address in the *Address* field in the *Email* section.
- Select the *System* and *Security* notification levels in the *System notify level* and *Security notify level* combo boxes respectively.

6.9 Certificates

Public-key cryptography uses a pair of keys: a public key, which encrypts data, and a corresponding private key, for decryption. Your public key is made known to the world, while your private key is kept secret. Anyone with access to your public key can encrypt information that only you can read.

The public and private keys are mathematically associated; however it is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt your information.

Technically, both public and private keys are large numbers that work with cryptographic algorithms to produce encrypted material. The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to authenticate each other and exchange messages securely.

GlobeSurfer 3G makes use of public-key cryptography to authenticate and encrypt Wireless and VPN data communication.

6.9.1 Digital Certificates

When working with public-key cryptography, you should be careful and make sure that you are using the correct person's public key. Man-in-the-middle attacks pose a potential threat, where an ill-intending 3rd party posts a phony key with the name and user ID of an intended recipient. Data transfer that is intercepted by the owner of the counterfeit key can fall in the wrong hands.

Digital certificates provide a means for establishing whether a public key truly belongs to the supposed owner. It is a digital form of credential. It has information on it that identifies you, and an authorized statement to the effect that someone else has confirmed your identity.

Digital certificates are used to foil attempts by an ill-intending party to use an unauthorized public key. A digital certificate consists of the following:

A public key

Certificate information the "identity" of the user, such as name, user ID and so on.

Digital signatures A statement stating that the information enclosed in the certificate has been vouched for by a Certificate Authority (CA).

Binding this information together, a certificate is a public key with identification forms attached, coupled with a stamp of approval by a trusted party.

6.9.2 X.509 Certificate Format

GlobeSurfer 3G supports X.509 certificates that comply with the ITU-T X.509 international standard. An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding

public key. The X.509 standard defines what information goes into the certificate, and describes how to encode it (the data format). All X.509 certificates have the following data:

The certificate holder's public key the public key of the certificate holder, together with an algorithm identifier that specifies which cryptosystem the key belongs to and any associated key parameters.

The serial number of the certificate the entity (application or person) that created the certificate is responsible for assigning it a unique serial number to distinguish it from other certificates it issues. This information is used in numerous ways; for example when a certificate is revoked, its serial number is placed on a Certificate Revocation List (CRL).

The certificate holder's unique identifier this name is intended to be unique across the Internet. A DN consists of multiple subsections and may look something like this: CN=John Smith, EMAIL=globesurfer@option.com, OU=R&D, O=Option, C=SE (These refer to the subject's Common Name, Organizational Unit, Organization, and Country.)

The certificate's validity period the certificate's start date/time and expiration date/time; indicates when the certificate will expire.

The unique name of the certificate issuer the unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate. (Note that in some cases, such as root or top-level CA certificates, the issuer signs its own certificate.)

The digital signature of the issuer the signature using the private key of the entity that issued the certificate.

The signature algorithm identifier identifies the algorithm used by the CA to sign the certificate.

6.9.3 Obtaining an X.509 Certificate

To obtain an X.509 certificate, you must ask a CA to issue one for you. You provide your public key, proof that you possess the corresponding private key, and some specific information about yourself. You then digitally sign the information and send the whole package – the certificate request – to the CA. The CA then performs some due diligence in verifying that the information you provided is correct and, if so, generates the certificate and returns it.

You might think of an X.509 certificate as a standard paper certificate with a public key taped to it. It has your name and some information about you on it, plus the signature of the person who issued it to you.

To obtain an X.509 certificate:

1. Click *Certificates* on the *Advanced* screen of the management console. The Certificates screen will appear (see figure 6.21).

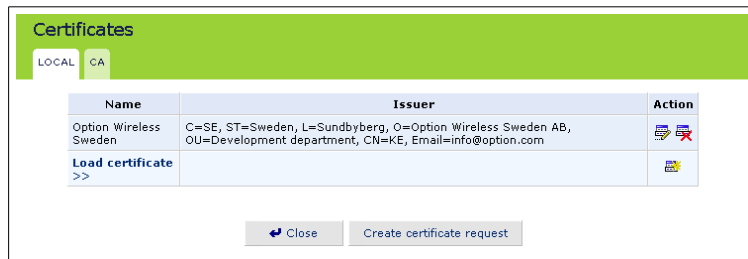


Figure 6.21: Certificate Management

2. Click the *Local* tab.
3. Click the *Create certificate request* button. The *Create X.509 Request* screen will appear (see figure 6.22).

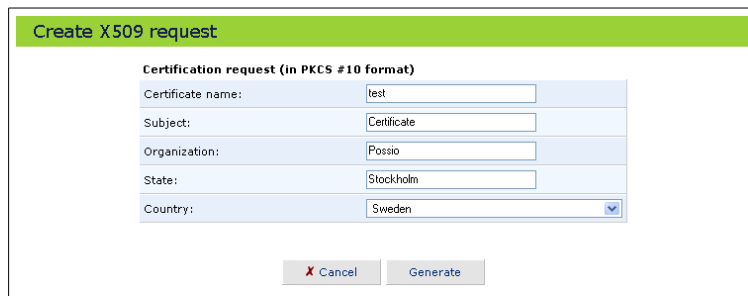


Figure 6.22: Create X.509 Request

4. Enter the following certification request parameters:
 - Certificate Name
 - Subject
 - Organization
 - State
 - Country
5. Click the *Generate* button. A screen will appear stating that the certification request is being generated (see figure 6.23).

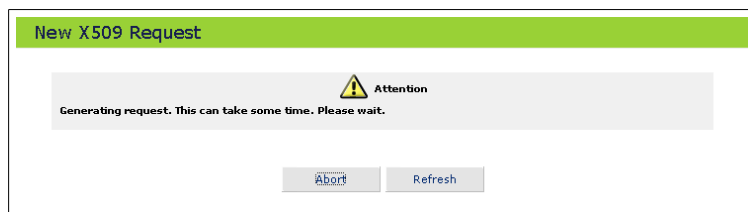


Figure 6.23: Generating a Request

- After a short while, click the *Refresh* button to display your certification request (see figure 6.24).

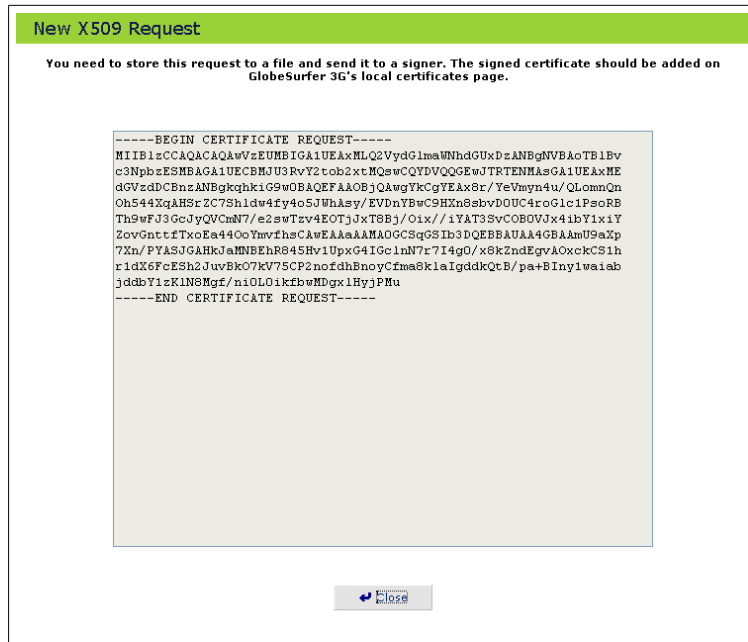


Figure 6.24: X.509 Certificate Request

- Store the exact contents of this request to a file, and send it to a CA for signing.
- Click the *Close* button. The main certificate management screen will appear, listing your certificate as "Unsigned".

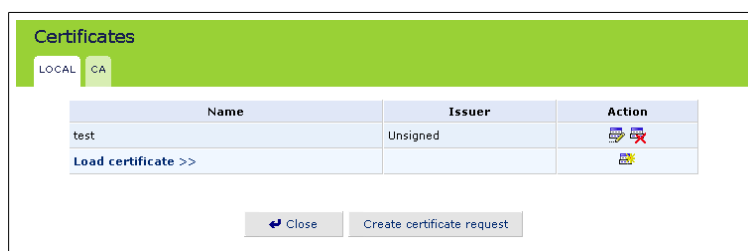


Figure 6.25: Unsigned Certification Request

- After receiving a reply from the CA in form of a signed request, click the *Load certificate* link. The *Load GlobeSurfer 3G's local certificate* screen will appear (see figure 6.26).

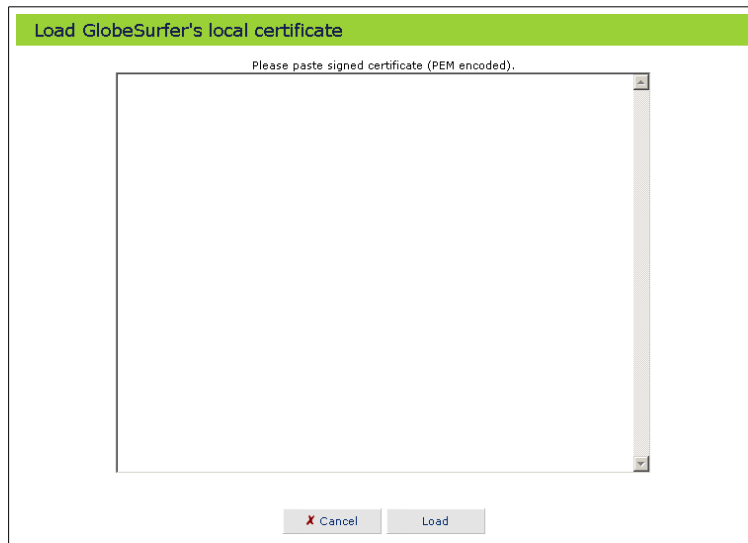


Figure 6.26: Load Certificate

10. Paste the signed request. The contents of the signed request should resemble what you see in figure 6.27.

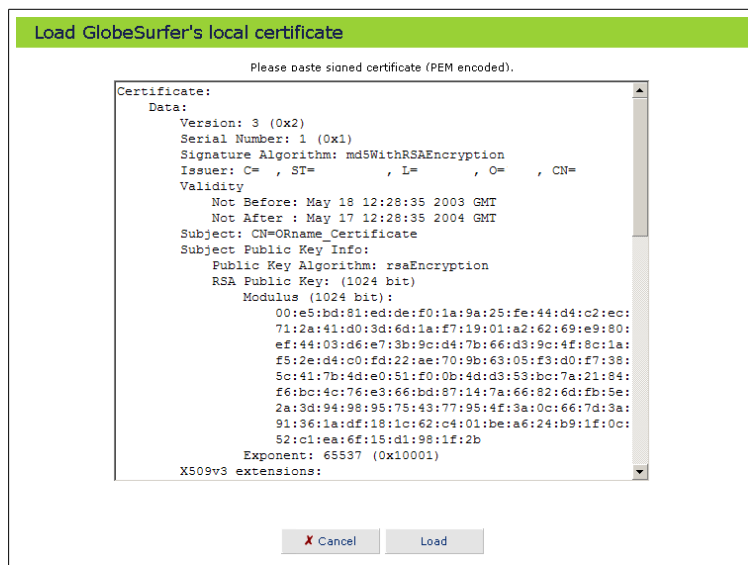


Figure 6.27: Loading a Signed Certificate

11. Click the *Load* button to register the signed certificate. If the registration is successful, the certificate management screen will appear, displaying the certificate name and issuer (see figure 6.28).

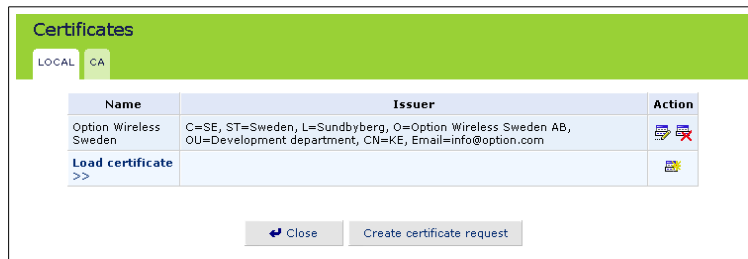


Figure 6.28: Registered Certificate

6.9.4 Registering a CA's Certificate

To register and load a certificate received from a CA:

1. Click *Certificates* on the *Advanced* screen of the management console. The *Certificates* screen will appear (see figure 6.21).
2. Click the *CA* tab.
3. Click the *Load Certificate* entry in the table, the *Load CA's Certificate* screen will appear.
4. Paste the CA's certificate into the window (see figure 6.29).

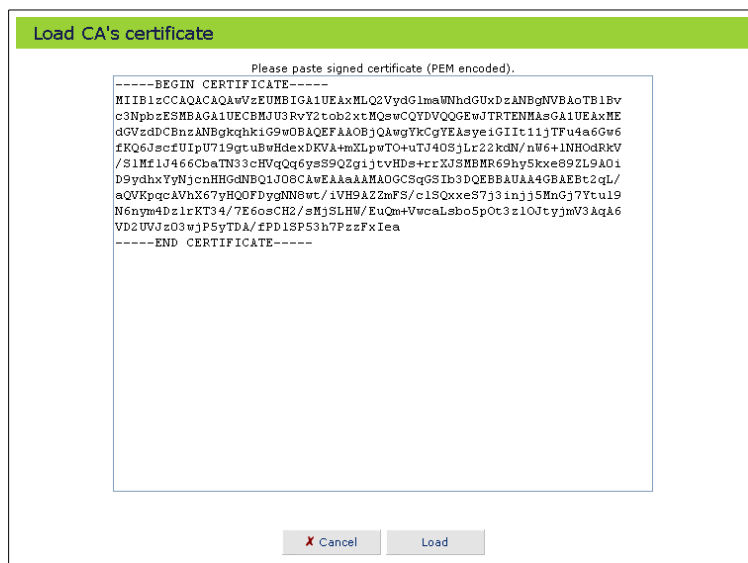


Figure 6.29: Load CA's Certificate

5. Click the *Load* button.

6.10 Date and Time

To configure date, time and daylight savings time settings perform the following:

1. Click *Date and time* on the *Advanced* screen of the management console. The *Date and time* settings screen will be displayed (see figure 6.30).

Date and time

Localization

Local time: Dec 14, 2005 10:30:51

Time zone: Europe/Stockholm [GMT+01:00]

Automatic time update

Enabled

Protocol: Time of day (TOD) Network Time Protocol (NTP)

Update every: 24 hours

Time server	Action
de.pool.ntp.org	
New entry >>	

Status: Got time update from server, Last update: 2005-12-14 10:29:29

Press the **Refresh** button to update the status.

Figure 6.30: Date and time settings

2. Select the local time zone from the pull-down menu. GlobeSurfer 3G can automatically detect daylight saving setting for the selected time zone. If the daylight saving settings for your time zone are not automatically detected, the following fields will be displayed:
 - Enabled** Select this check box to enable daylight saving time.
 - Start** Date and time when daylight saving starts.
 - End** Date and time when daylight saving ends.
 - Offset** Daylight saving time offset.
3. If you want the GlobeSurfer 3G to perform an automatic time update, perform the following:
 - Select the *Enabled* checkbox under the *Automatic time update* section.
 - Select the protocol to be used to perform the time update by selecting either the *Time of Day (TOD)* or *Network Time Protocol (NTP)* radio button.
 - Specify how often to perform the update in the *Update every* field.
 - You can change the default time server address by clicking the *New entry* link in the bottom of the *Automatic time update* section.

6.11 Scheduler Rules

Scheduler rules are used for limiting the activation of settings, such as firewall rules, to specific time periods, specified in days of the week, and hours.

To define a Rule:

1. Click *Scheduler rules* on the *Advanced* screen of the management console. The *Scheduler rules* screen will appear (see figure 6.31).

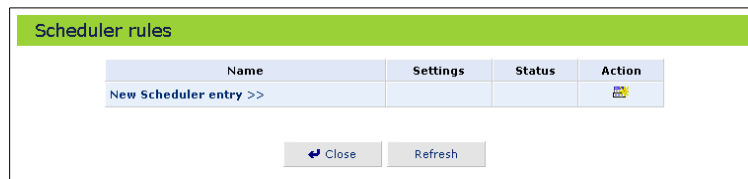


Figure 6.31: Scheduler Rules

2. Click the *New scheduler entry* link. The *Scheduler rule edit* screen will appear (see figure 6.32).

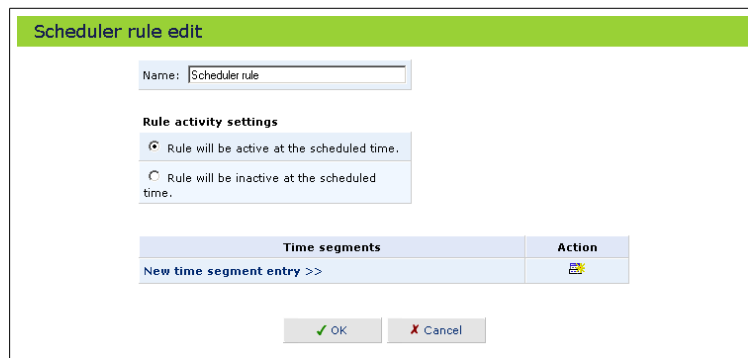


Figure 6.32: Scheduler Rule Edit

3. Specify a name for the rule in the *Name* field.
4. Specify if the rule will be active/inactive during the designated time period, by selecting the appropriate *Rule activity settings* check-box.
5. Click the *New time segment entry* link to define the time segment to which the rule will apply — the *Time segment edit* screen will appear (see figure 6.33).
 - (a) Select active/inactive days of the week.
 - (b) Click the *New time segment entry* link to define an active/inactive hourly range.
6. Click *OK*.

Time segment edit

Days of week

<input type="checkbox"/> Monday
<input type="checkbox"/> Tuesday
<input type="checkbox"/> Wednesday
<input type="checkbox"/> Thursday
<input type="checkbox"/> Friday
<input type="checkbox"/> Saturday
<input type="checkbox"/> Sunday

Hours range


Start	End	Action
New time segment entry >>		

Figure 6.33: Time Segment Edit

6.12 Firmware Upgrade

GlobeSurfer 3G offers a built-in mechanism for upgrading its software, without losing any of your custom configurations and settings. The software is upgraded by loading a software image file that you have previously downloaded from the Internet or received on CD.

6.12.1 Upgrading From a Local Computer

To upgrade GlobeSurfer 3G using a locally stored file:

1. Click the *Firmware upgrade* icon from the *Advanced* screen. The *GlobeSurfer 3G Firmware upgrade* screen will appear (see figure 6.34).

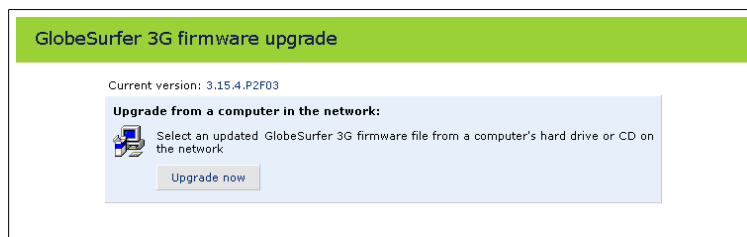


Figure 6.34: GlobeSurfer 3G Firmware Upgrade

2. Click the *Firmware upgrade* button. The *Firmware upgrade* screen will appear (see figure 6.35).

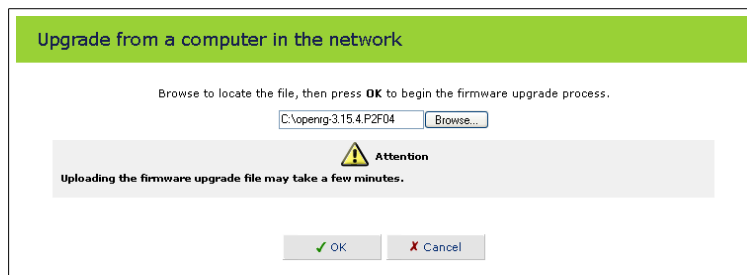


Figure 6.35: Firmware upgrade

3. Enter the path of the software image file, or click the *Browse* button to browse for the file on your PC. Click *OK* when ready.

Note: You can only use files with an **rmt** extension when performing the firmware upgrade procedure.

The file will start loading into your GlobeSurfer 3G. When loading is completed, a confirmation screen will appear, asking you if you want to upgrade to the new version:

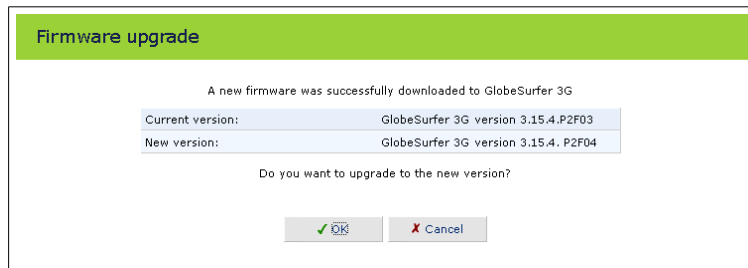


Figure 6.36: Confirm Upgrade

4. Click *OK* to confirm. The upgrade process will begin and should take no longer than one minute to complete (see figure 6.37).

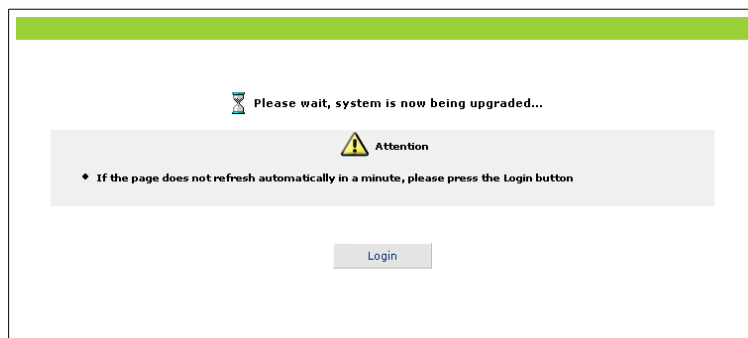


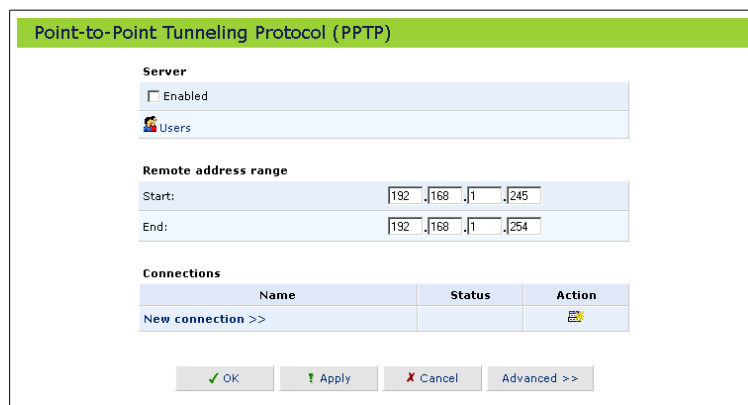
Figure 6.37: Upgrade in Progress

When the upgrading is ready the GlobeSurfer 3G will automatically reboot. The new software version will run, maintaining your custom configurations and settings.

6.13 Point-to-Point Tunneling Protocol (PPTP)

To access the PPTP settings click the PPTP icon from the *Advanced* screen. The *Point-to-Point Tunneling Protocol (PPTP)* screen will appear (see figure 6.38). This screen enables you to configure:

- The remote users that will be granted access to your local network.
- The IP address range an authorized remote user can use when accessing your local network.
- Advanced PPTP client/server connection settings.



Point-to-Point Tunneling Protocol (PPTP)

Server

Enabled

[Users](#)

Remote address range

Start: 192.168.1.245

End: 192.168.1.254

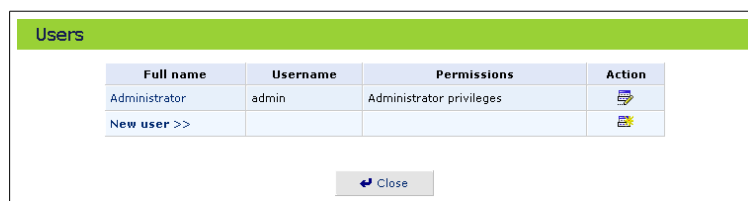
Connections

Name	Status	Action
New connection >>		

Figure 6.38: PPTP Settings

6.13.1 Managing Remote Users

Select the *Users* link to define and manage remote users (see figure 6.39).



Users

Full name	Username	Permissions	Action
Administrator	admin	Administrator privileges	
New user >>			

Figure 6.39: User table

You can add, edit and delete users allowed to access the GlobeSurfer 3G and your local network by managing the user table as described in Section 2.5. To add a new user click *New user* in the table and specify the following parameters:

- **Full name:** The remote user's full name.
- **Username:** The name the remote user will use to access your local network.

- **New password:** Type a new password for the remote user. If you do not want to assign a password to the remote user leave this field empty.
- **Retype new password:** If a new password was assigned, type it again to verify correctness.
- **Permissions:** Select the remote user's privileges on your local network.
 - **Administrator privileges:** Grants remote system setting modification via the web-based management console or telnet.
 - **Remote access by PPTP:** Grants access with no system modification privileges.
 - **SMS access only:** Grants access to the SMS manager only, for example to send and read SMS messages. Other parts of the management console will be hidden and can not be accessed.

Figure 6.40: Managing Users

Please note, that changing any of the user parameters will prompt the connection associated with the user to terminate. For changes to take effect you should activate the connection manually after modifying user parameters.

You can use email notification to receive indications of system events for a predefined severity classification. The available types of events are *System* or *Security* events. The available severity of events are *Error*, *Warning* and *Information*. If the *Information* level is selected the user will receive notification of *Information*, *Warning* and *Error* events. If the *Warning* level is selected the user will receive notification of *Warning* and *Error* events etc.

To configure email notification for a specific user:

- First make sure you have configured an outgoing mail server in *System settings*. A click on the *Configure mail server* link will display the *System settings* screen where you can configure the outgoing mail server.
- Enter the user's email address in the *Address* field in the *Email* section.

- Select the *System* and *Security* notification levels in the *System notify level* and *Security notify level* combo boxes respectively.

6.13.2 Advanced PPTP Server Settings

To configure advanced PPTP server settings click the *Advanced* button on the *Point-to-Point Tunneling Protocol (PPTP)* screen (see figure 6.38). The advanced settings will appear (see figure 6.41). This screen enables you to configure the following:

- **Enabled:** Enable or disable the PPTP server.
- **Max. idle time to disconnect in seconds:** Specify the amount of idle time (during which no data is sent or received) that should elapse before the GlobeSurfer 3G disconnects a PPTP connection.
- **Authentication/Encryption required:** Select whether PPTP will use authentication, encryption, or both.
- **Allowed authentication algorithms:** Select the algorithms the server may use when authenticating its clients.
- **Allowed encryption algorithms:** Select the algorithms the server may use when encrypting data.
- **Remote address range:** Specify the range of IP addresses remote users can use to access your local network.

Please note that the client settings must be in tune with the server settings.

The screenshot shows the 'Advanced PPTP Server Settings' interface. It features a green header bar with the title 'Point-to-Point Tunneling Protocol (PPTP)'. Below this, the settings are organized into several sections:

- Server:** A checkbox labeled 'Enabled' is currently unchecked.
- Users:** A section with a 'Users' icon and a text input field for 'Max. idle time to disconnect in seconds' containing the value '1200'.
- Authentication/Encryption:** A checkbox for 'Authentication required' is checked. Below it, 'Allowed authentication algorithms' includes checkboxes for 'PAP', 'CHAP', 'MS-CHAP', and 'MS-CHAP v2', with the latter two checked.
- Encryption:** A checkbox for 'Encryption required' is checked. Below it, 'Allowed encryption algorithms' includes checkboxes for 'MPPE-40' and 'MPPE-128', both of which are checked.
- MPPE encryption mode:** A dropdown menu is set to 'Stateless'.
- Remote address range:** Two IP address input fields are shown. The 'Start' field is '192.168.1.245' and the 'End' field is '192.168.1.254'.

Figure 6.41: Advanced PPTP Server Settings

6.13.3 Advanced PPTP Client Settings

The PPTP connections are displayed in the *Point-to-Point Tunneling Protocol (PPTP)* screen (see figure 6.38). To configure advanced PPTP client settings

perform the following steps:

1. Click the connection's *Edit* icon in the *Action* column. The *Connection properties* screen will appear (see figure 6.42).

VPN PPTP Properties	
	<input type="button" value="Disable"/>
Name:	VPN PPTP
Device name:	ppp200
Status:	In progress...
Network:	WAN
Connection type:	VPN PPTP
Username:	admin
Current connection time:	-
Total connection time:	-

Figure 6.42: PPTP Connection properties

2. Click the *Settings* button. A screen will appear, enabling you to configure the following advanced PPTP client settings.
 - **PPP Settings**
 - **Hostname:** The host name of your PPTP server.
 - **Login username:** Your user name.
 - **Login password:** Your password.
 - **PPP authentication:** Select the authentication algorithms your GlobeSurfer 3G may use when negotiating with a PPTP server. Select all the check-boxes if no information is available about the server's authentication methods.
 - **PPP encryption:** Select the encryption algorithms your GlobeSurfer 3G may use when negotiating with a PPTP server. Select all the check-boxes if no information is available about the server's encryption methods.
 - **Routing:** Define the connection's routing rules. Please refer to Section 6.7 for instructions about creating routing rules.
 - **DNS server:** Select whether the PPTP client should obtain a DNS server address automatically. If not, configure the DNS server's IP address.
 - **Internet connection firewall:** Select this check-box to include the PPTP client connection as a network interface monitored by the Firewall of the GlobeSurfer 3G.

6.14 IP Security (IPsec)

IPsec is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks. The IPsec protocols include:

- AH (Authentication Header) provides packet-level authentication.
- ESP (Encapsulating Security Payload) provides encryption and authentication.
- IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two services.

Services supported by the IPsec protocols (AH, ESP) include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering), and replay protection (defense against unauthorized resending of data).

IPsec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPsec key management protocol, defines a series of steps to establish keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet Engineering Task Force (IETF), IPsec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to interoperate.

6.14.1 Technical Specifications

- Security architecture for the Internet Protocol
- IP Security Document Roadmap
- Connection type: Tunnel, Transport
- Key management: Manual, Automatic, Internet Key Exchange
- Gateway authentication: X.509, RSA signatures, pre-shared secret key, ISAKMP (manual and aggressive modes)
- IP protocols: ESP, AH
- Encryption: AES, 3DES, DES, HW encryption integration
- Authentication: MD5, SHA-1
- IP Payload compression
- Interoperability: Windows 2000, FreeS/WAN, OpenBSD, FreeBSD, Cisco Routers, Nortel, Windows NT, Checkpoint Firewall-1, F-Secure VPN for Windows, Xedia Access Point/QVPN, PGP 6.5 Mac and Windows IPsec Client, PGPnet, IRE Safenet/Intel LANrover, Sun Solaris, NetScreen

6.14.2 Basic IPsec Connection Settings

Click the *IPsec* icon from the *Advanced* screen to access the IPsec settings screen (see figure 6.43).

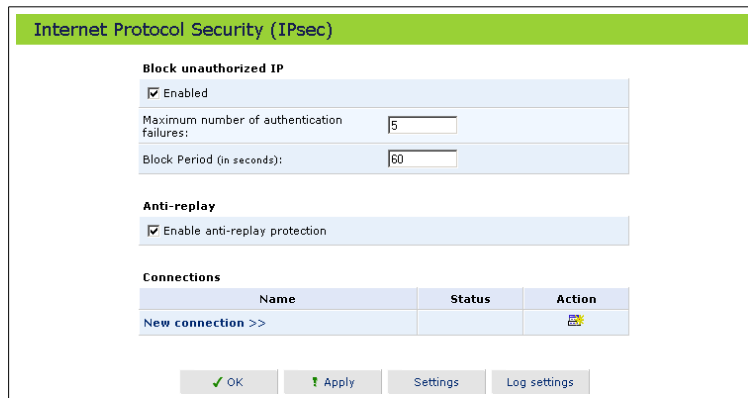


Figure 6.43: IPsec Settings

Select the *Enabled* checkbox to block unauthorized IPsec network connection to GlobeSurfer 3G. To define what an unauthorized IPsec connection means and how long to block it, specify the following:

- Maximum number of authentication failures
- The block period (in seconds)

6.14.2.1 Key Management

1. Click the *IPsec* icon from the *Advanced* screen to access the IPsec settings screen (see figure 6.43).
2. Click the *Settings* button to view the public key (see figure 6.44). If necessary, you can copy the public key from this screen.

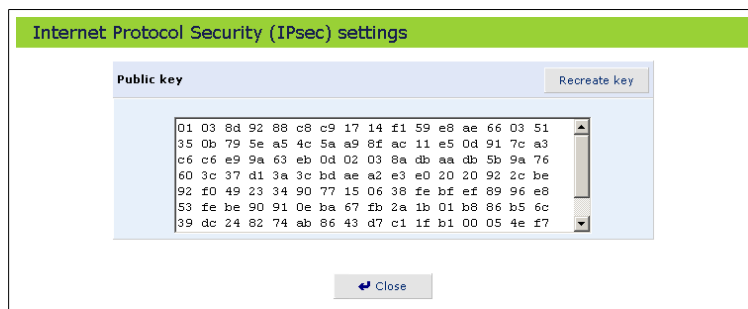


Figure 6.44: Advanced IPsec Settings

3. Click *Recreate key* to recreate the public key, or *Refresh* to refresh the key displayed in this screen.

6.14.2.2 Log Settings

The IPsec Log can be used to identify and analyze the history of the IPsec package commands, attempts to create connections, etc. IPsec activity, as well as that of other GlobeSurfer 3G modules, is displayed together in this view.

1. Click the *IPsec* icon from the *Advanced* screen.
2. Click *Log settings*. The *IPsec log settings* screen will appear.
3. Select the check-boxes relevant to the information you would like the IPsec log to record.

6.14.3 Advanced IPsec Connection Settings

The IPsec connections are displayed in the *Connections* section of the IPsec settings screen (see figure 6.43). To configure advanced IPsec settings perform the following steps:

1. Click the connection's *Edit* icon in the *Action* column. The *Connection properties* screen will appear (see figure 6.45)

VPN IPsec Properties properties	
<input type="button" value="Disable"/>	
Name:	VPN IPsec
Device name:	ips0
Status:	Resolving hostname...
Network:	WAN
Connection type:	VPN IPsec
Remote tunnel endpoint address:	192.168.10.10
Local subnet:	192.168.1.0/255.255.255.0
Remote subnet:	192.168.2.0/255.255.255.0

Figure 6.45: IPsec Connection Properties

2. Click the *Settings* button. The *Configure IPsec connection* screen will appear, enabling you to configure the following advanced IPsec settings:

Remote tunnel endpoint address The IP address of your IPsec peer.

Security Association Mode Mode can be *Tunneling* or *Transport*. *Transport* mode needs no explicit configuration. *Tunneling* mode requires that you configure the following parameters:

- Local subnet
- Local subnet mask
- Remote subnet
- Remote subnet mask
- Compress (Support IPCOMP protocol): Select this check-box to use the IPComp protocol.

Key exchange method The key exchange method can be *Manual* or *Automatic*. The following are the parameters that are required to configure an *Automatic* key exchange:

Negotiation attempts Select the number of negotiation attempts to be performed in Phase 1 of the automatic key exchange method.

Lifetime in seconds The length of time before a security association automatically performs a renegotiation. A short lifetime increases security by forcing the VPN hosts to update the encryption and authentication keys. However, every time the VPN Tunnel renegotiates, users accessing remote resources are disconnected. Therefore, the default lifetime is recommended.

Rekey Margin Specifies how long before connection expiry attempts to negotiate a replacement should begin. It is similar to that of the Key Lifetime and is given as an integer denoting seconds.

Rekey Fuzz Percent Specifies the maximum percentage by which Rekey Margin should be randomly increased to randomize rekeying intervals.

Phase 1 peer authentication Select the method by which GlobeSurfer 3G will authenticate your IPsec peer:

- Shared secret
- RSA signature
- Certificate

Phase 1 encryption algorithm Select the encryption algorithms that GlobeSurfer 3G will attempt to use when negotiating with the IPsec peer.

Hash algorithm Select the hash algorithms that GlobeSurfer 3G will attempt to use when negotiating with the IPsec peer.

Use Perfect Forward Secrecy (PFS) Select whether Perfect Forward Secrecy of keys is desired on the connection's keying channel (with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier).

ESP Select the encryption and authentication algorithms the GlobeSurfer 3G will use during Phase 2 of the automatic key exchange method. You can choose 3DES-CBC, DES-CBC or NULL encryption algorithms; MD5 or SHA1 authentication algorithms.

AH Select the hash algorithms the GlobeSurfer 3G will use during Phase 2 of the automatic key exchange method. You can choose MD5 or SHA1 authentication header algorithms.

The following are the parameters that are required to configure a *Manual* key exchange:

Security Parameter Index – SPI a 32 bit value which together with IP address and security protocol uniquely identifies a particular security association. This value must be the same for both Local and Remote Tunnel.

IPsec protocol Select the encryption and authentication algorithms.
All algorithms values should be entered in HEX format.

Routing Define the connection's routing rules. Please refer to Section [6.7](#) for instructions about creating routing rules.

Internet connection firewall Select this check-box to include the IPsec connection as a network interface monitored by the gateway's Firewall.

6.15 Universal Plug and Play (UPnP)

To access the UPnP settings perform the following:

1. Click *Universal Plug and Play* on the *Advanced* screen of the management console. The *Universal Plug and Play* settings screen will be displayed (see figure 6.46).

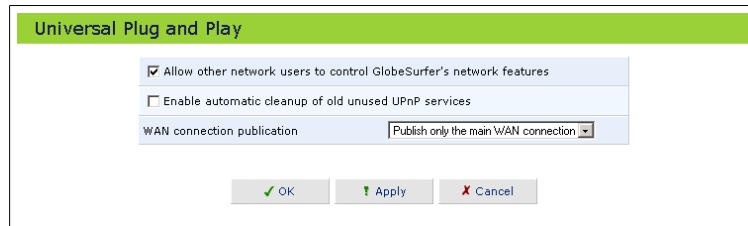


Figure 6.46: Universal Plug and Play

2. Check the *Allow other network users to control GlobeSurfer 3G's network features* checkbox, to enable the UPnP feature. This will enable you to define UPnP services on any of the LAN hosts.
3. Check the *Enable automatic cleanup of old unused UPnP services* checkbox, to enable automatic cleanup of invalid rules. When enabled, this feature checks validity of all the UPnP services and rules every 5 minutes. Any UPnP defined service which is found to be old and not in use, is removed, unless any user defined rule (see *Security* screen) depends on it. This feature is disabled by default.

Since there is a limitation on the maximum number of UPnP defined services to 256, you should want to enable the cleanup feature if you might exceed this limit.

In which case might the limit be exceeded? UPnP services are not deleted when disconnecting a computer without proper shutdown of the UPnP application (e.g. messenger). Thus, if you are running a boingo, services may often not be deleted, and will eventually lead to exhaustion of rules and services, and no new services could be defined. In this scenario the cleanup feature will find the services which are no longer valid and will remove them, preventing services exhaustion.

6.16 Simple Network Management Protocol (SNMP)

SNMP enables network management systems to remotely configure and monitor GlobeSurfer 3G. Your Internet service provider (ISP) may use SNMP in order to identify and resolve technical problems.

6.16.1 Configuring GlobeSurfer 3G's SNMP Agent

Technical information regarding the properties of GlobeSurfer 3G's SNMP agent should be provided by your ISP.

To configure GlobeSurfer 3G's SNMP agent perform the following:

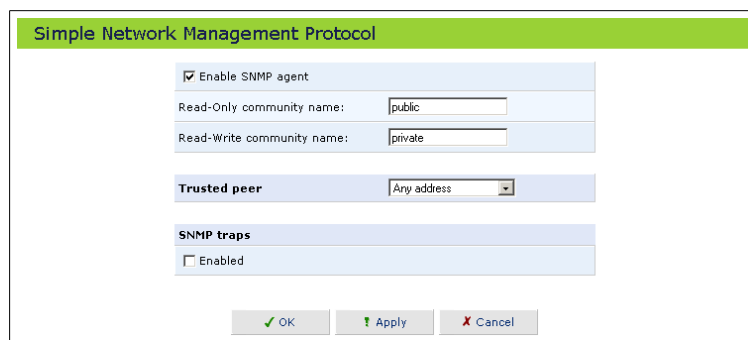
1. Click *Simple Network Management Protocol* on the *Advanced* screen of the Management Console. The SNMP screen will appear (see figure 6.47).
2. Check the *Enable SNMP agent* checkbox and specify the SNMP parameters, as provided by your Internet service provider:

Read-Only/Read-Write Community Names SNMP community strings are passwords used in SNMP messages between the management system and GlobeSurfer 3G. A read-only community allows the manager to monitor GlobeSurfer 3G. A read-write community allows the manager to both monitor and configure GlobeSurfer 3G.

Trusted peer The IP address, or subnet of addresses, that identify which remote management stations are allowed to perform SNMP operations on GlobeSurfer 3G.

SNMP traps Messages sent by GlobeSurfer 3G to a remote management station, in order to notify the manager about the occurrence of important events or serious conditions. GlobeSurfer 3G supports both SNMP version 1 and SNMP version 2c traps.

3. Click *OK* to save the settings.



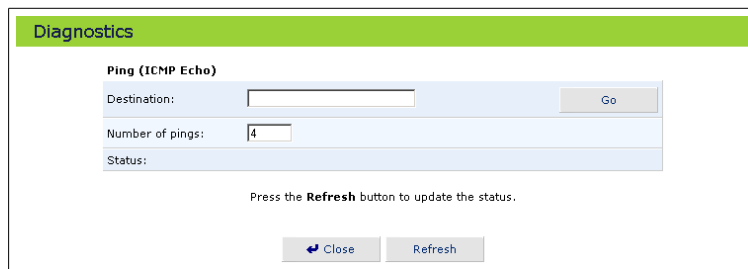
The screenshot shows a configuration window titled "Simple Network Management Protocol". It contains the following elements:

- A green header bar with the title "Simple Network Management Protocol".
- A checkbox labeled "Enable SNMP agent" which is checked.
- Two text input fields: "Read-Only community name:" with the value "public" and "Read-Write community name:" with the value "private".
- A "Trusted peer" section with a dropdown menu currently showing "Any address".
- An "SNMP traps" section with a checkbox labeled "Enabled" which is unchecked.
- At the bottom, three buttons: "OK" (with a green checkmark), "Apply" (with a green arrow), and "Cancel" (with a red X).

Figure 6.47: SNMP Management

6.17 Diagnostics

The Diagnostics screen can assist you in testing network connectivity. This feature will enable you to ping (ICMP echo) an IP address and view statistics such as the number of packets transmitted and received, round trip time and success status.



The screenshot shows a web interface titled "Diagnostics" with a green header. Below the header is a section titled "Ping (ICMP Echo)". This section contains three input fields: "Destination:" with an empty text box and a "Go" button to its right; "Number of pings:" with a text box containing the number "4"; and "Status:" with an empty text box. Below these fields is a text instruction: "Press the **Refresh** button to update the status." At the bottom of the form are two buttons: "Close" with a blue arrow icon and "Refresh" with a circular arrow icon.

Figure 6.48: Advanced Diagnostics

6.17.1 Diagnosing Network Connectivity

To diagnose network connectivity perform the following steps:

1. Click *Diagnostics* on the *Advanced* screen of the management console. The *Diagnostics* screen will appear (see figure 6.48).
2. Enter the IP address to be tested in the *Destination* field.
3. Click the *Go* button in the *Ping* section.
4. After a few seconds, diagnostics statistics will be displayed. If no new information is displayed, click the *Refresh* button.

6.18 Advanced Remote Administration

In its default state, GlobeSurfer 3G blocks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may wish to enable certain services that grant remote users administrative privileges in your network. For example, you may allow yourself to view or change settings while travelling. It may also be necessary to allow your ISP to change settings or help you troubleshoot functionality or communication issues from a remote location.

Remote access is supported by the following services, and you may use the *Remote administration* screen to selectively enable these services if they are needed.

Allow Incoming Access to the Telnet Server
<input type="checkbox"/> Using Primary Telnet Port (23)
<input type="checkbox"/> Using Secondary Telnet Port (8023)
<input type="checkbox"/> Using Secure Telnet over SSL Port (992)
Allow Incoming Access to the Web-Management
<input checked="" type="checkbox"/> Using Primary HTTP Port (80)
<input checked="" type="checkbox"/> Using Secondary HTTP Port (8080)
<input checked="" type="checkbox"/> Using Primary HTTPS Port (443)
<input checked="" type="checkbox"/> Using Secondary HTTPS Port (8443)
Allow SNMP Control and Diagnostic Requests
<input type="checkbox"/> Allow Incoming SNMP Requests
Diagnostic Tools
<input type="checkbox"/> Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)
<input type="checkbox"/> Allow Incoming UDP Traceroute Queries

Figure 6.49: Remote Administration

- To allow remote access to GlobeSurfer 3G services:
 1. Click the *Remote administration* icon on the *Advanced* screen of the management console, or select the *Remote administration* tab on the *Security* screen. The *Remote administration* screen will appear (see figure 6.49).
 2. Select the services that you would like to make available to remote computers on the Internet. These services include:
 - Allow incoming access to the Telnet server** Used to allow command-line access to all system settings and parameters (using a telnet client). While this service is password-protected, it is not considered a secure protocol. If a local server is configured to use port 23 select port 8023 to avoid conflicts.

Allow incoming access to the Web management Used to allow password-protected management console access to all system settings and parameters (using a browser). Both secure (HTTPS) and non-secure (HTTP) access is available. If a local server is configured to use port 80 select port 8080 to avoid conflicts.

Allow SNMP control and diagnostic requests Used to allow access to incoming SNMP requests.

Diagnostic tools Used for troubleshooting and remote system management by you or your Internet Service Provider.

3. Click *OK* to save your changes.

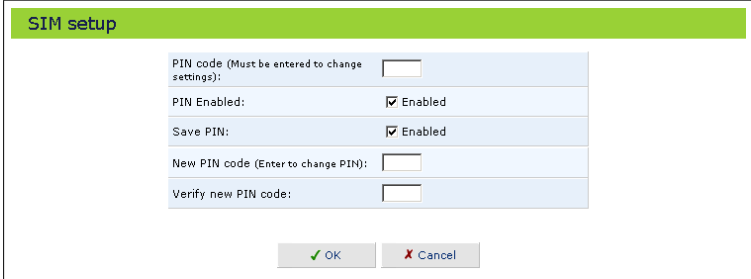
Note: Telnet and Web management may be used to modify settings of the firewall or disable it. The user may also change local IP addresses and other settings, making it difficult or impossible to access the GlobeSurfer 3G from the local network. Therefore, remote access to Telnet or HTTP services **should be blocked** and should only be permitted when absolutely necessary.

Encrypted remote administration is done using a secure SSL connection, that requires an SSL certificate. When accessing GlobeSurfer 3G for the first time using encrypted remote administration, you will be prompted by your browser with a warning regarding certificate authentication. This is due to the fact that GlobeSurfer 3G's SSL certificate is self generated. When encountering this message under these circumstances, ignore it and continue. The self generated certificate is safe, and provides you with a secure SSL connection.

It is also possible to assign a user-defined certificate to GlobeSurfer 3G. To learn about certificates, see Section [6.9](#).

6.19 SIM Setup

The SIM card in the GlobeSurfer 3G requires a PIN code to be entered before it can be used. The PIN code you receive from your ISP can be changed to a PIN code of your own. By default the PIN code is required but it can be stored in the GlobeSurfer 3G after the first use so that you don't have to enter it more than once. These settings can be changed but note that you should disconnect before doing any changes to the SIM setup.



The screenshot shows a 'SIM setup' window with a green header. It contains the following fields and controls:

PIN code (Must be entered to change settings):	<input type="text"/>
PIN Enabled:	<input checked="" type="checkbox"/> Enabled
Save PIN:	<input checked="" type="checkbox"/> Enabled
New PIN code (Enter to change PIN):	<input type="text"/>
Verify new PIN code:	<input type="text"/>

At the bottom, there are two buttons: 'OK' with a green checkmark icon and 'Cancel' with a red X icon.

Figure 6.50: SIM Setup

To change the settings of your SIM card, perform the following:

1. Click *SIM Setup* on the *Advanced* screen of the management console. The SIM Setup screen will appear (see figure 6.50).
2. Enter the PIN code in the first field to be able to change any settings.
3. By default the PIN is enabled. To disable the PIN, de-select the first *Enabled* checkbox.
4. To be forced to enter the PIN code each time the GlobeSurfer 3G is started, de-select the *Enabled* checkbox at *Save PIN*.
5. If you want to change the PIN code, enter a new PIN code in the last two fields.
6. Click *OK* to save your changes.

6.20 Unlock Device

In case the GlobeSurfer 3G is locked to a specific ISP it can be unlocked with a code that you should be able to get from your ISP. Normally there are certain conditions that must be fulfilled to be able to unlock the device.

To unlock the GlobeSurfer 3G:

1. Click *Unlock Device* on the *Advanced* screen of the management console. If the GlobeSurfer 3G really is locked, the *Unlock Device* screen will appear.
2. Enter the unlock code.
3. Click *OK*.

6.21 Restoring Default Settings

You may sometimes wish to restore GlobeSurfer 3G's factory default settings. This may happen, for example, when you wish to build a new network from the beginning, or when you cannot recall changes made to the network and wish to go back to the default configuration.

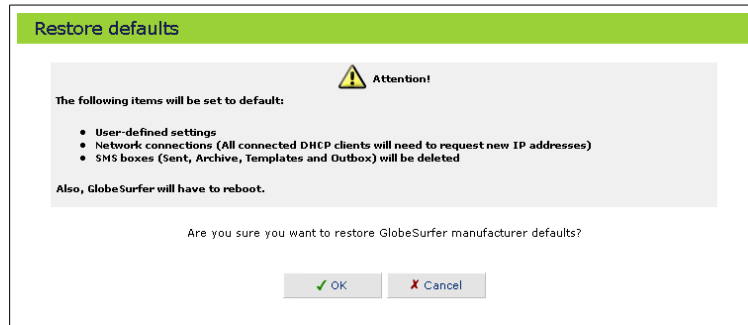


Figure 6.51: Restore Defaults

To restore default settings:

1. Click *Restore defaults* on the *Advanced* screen of the management console. The *Restore defaults* screen will be displayed (see figure 6.51).
2. Click *OK* to restore GlobeSurfer 3G's factory default settings.

Note: All web-based management settings and parameters, not only those in the *Advanced* section, will be restored to their default values. This includes the administrator password; a user-specified password will no longer be valid.

6.22 Restart

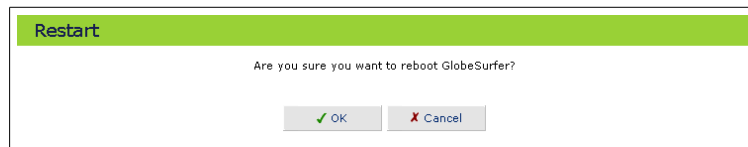


Figure 6.52: Restart

To restart the GlobeSurfer 3G:

1. Click *Restart* on the *Advanced* screen of the management console. The *Restart* screen will be displayed (see figure 6.52).
2. Click *OK* to restart the GlobeSurfer 3G. This may take up to one minute.

To reenter the management console after restarting the GlobeSurfer 3G, click the browser's *Refresh* button.

6.23 Technical Information

To view technical information regarding GlobeSurfer 3G:

1. Click *Technical information* on the *Advanced* screen of the management console. The *Technical information* screen will appear.

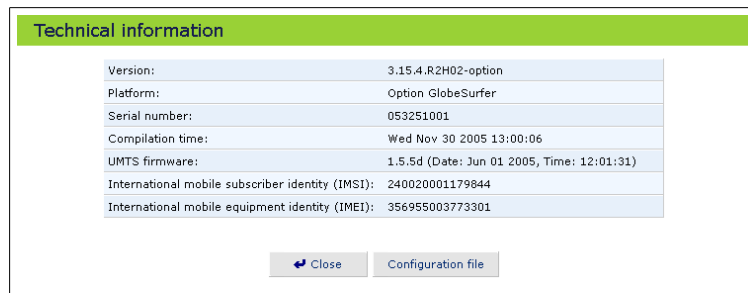


Figure 6.53: Technical Information

2. Click *Configuration file* to view the contents of GlobeSurfer 3G's configuration file.

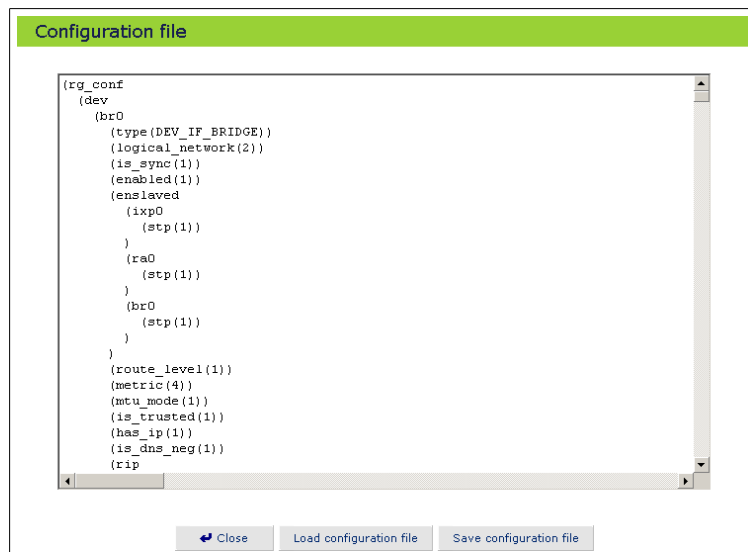


Figure 6.54: Configuration File

3. Click *Save configuration file* to save a copy of the configuration file.
4. Click *Load configuration file* to load a configuration file and restart GlobeSurfer 3G.

7

System Monitoring

The *System monitoring* screen (see figure 7.1) displays important system information, including:

- Key network device parameters
- Network traffic statistics
- The system log
- The amount of time that has passed since the system was last started

To display the *System monitoring* screen:

1. Click *System monitoring* in the left sidebar. The screen consists of four tabs with the first summarizing the monitored connection data (see figure 7.1).
2. Click the *Refresh* button to update the display, or click the *Automatic refresh on* button to constantly update the displayed parameters.

7.1 Monitoring Connections

The *Connections* tab shows a table summarizing data of the monitored connections.

Name	LAN Bridge	LAN Ethernet	VPN IPSec Properties	WAN UMTS
Device name	br0	ixp0	ra0	ppp100
Status	Connected	Connected (no IP address assigned)	Connected (no IP address assigned)	Not connected
Network	LAN	LAN	LAN	WAN
Underlying device	LAN Ethernet VPN IPSec Properties			
Connection type	Bridge	Ethernet	Wireless	UMTS
MAC address	00:09:8c:00:0a:74	00:09:8c:00:0a:74	00:14:a5:06:12:40	
IP address	192.168.1.1			
Subnet mask	255.255.255.0			
DHCP	DHCP server	Disabled	Disabled	
Username				
Encryption			Disabled	

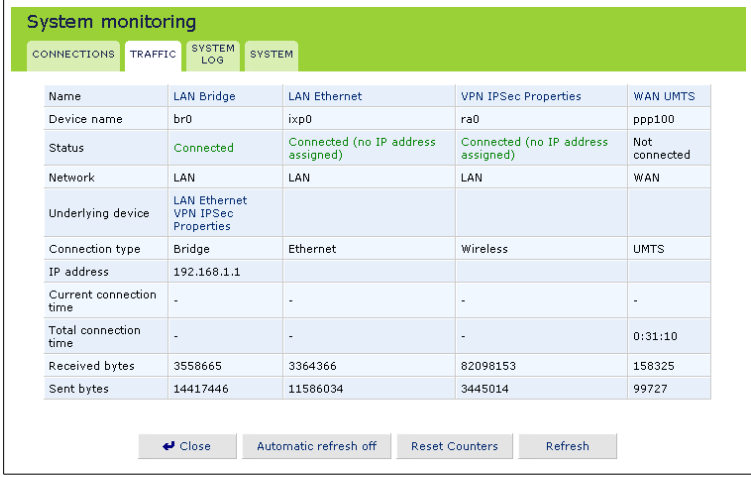
Close Automatic refresh off Refresh

Figure 7.1: Monitoring Connections

7.2 Traffic Statistics

GlobeSurfer 3G is constantly monitoring traffic within the local network and between the local network and the Internet.

Select the *Traffic* tab to display up-to-the-second statistical information about data received from and transmitted to the Internet (WAN) and about data received from and transmitted to computers in the local network (LAN).



The screenshot shows a 'System monitoring' window with a 'TRAFFIC' tab selected. It displays a table of network connections and their associated statistics.

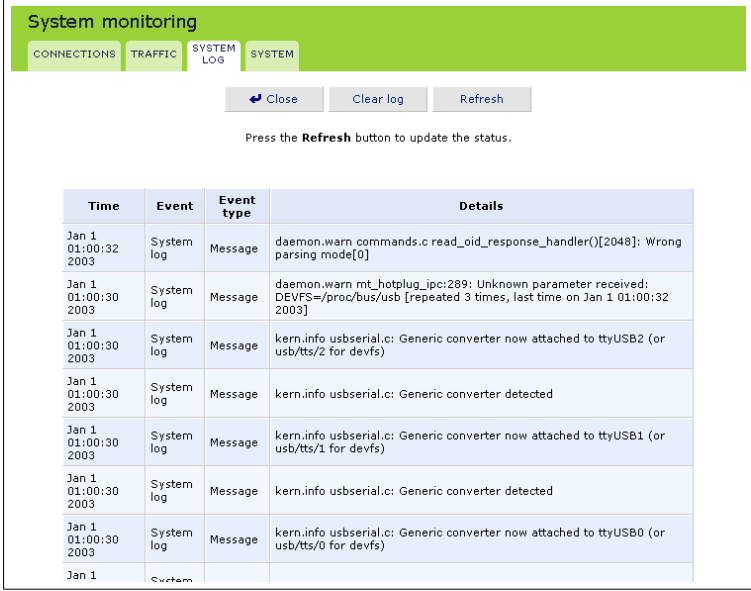
Name	LAN Bridge	LAN Ethernet	VPN IPSec Properties	WAN UMTS
Device name	br0	ixp0	ra0	ppp100
Status	Connected	Connected (no IP address assigned)	Connected (no IP address assigned)	Not connected
Network	LAN	LAN	LAN	WAN
Underlying device	LAN Ethernet VPN IPSec Properties			
Connection type	Bridge	Ethernet	Wireless	UMTS
IP address	192.168.1.1			
Current connection time	-	-	-	-
Total connection time	-	-	-	0:31:10
Received bytes	3558665	3364366	82098153	158325
Sent bytes	14417446	11586034	3445014	99727

At the bottom of the window, there are four buttons: 'Close', 'Automatic refresh off', 'Reset Counters', and 'Refresh'.

Figure 7.2: Traffic Statistics

7.3 System Log

Select the *System log* tab to display a list of the most recent activity that has taken place on GlobeSurfer 3G.



System monitoring

CONNECTIONS TRAFFIC SYSTEM LOG SYSTEM

Close Clear log Refresh

Press the **Refresh** button to update the status.

Time	Event	Event type	Details
Jan 1 01:00:32 2003	System log	Message	daemon.warn commands.c read_oid_response_handler()[2048]: Wrong parsing mode[0]
Jan 1 01:00:30 2003	System log	Message	daemon.warn mt_hotplug_ipc:289: Unknown parameter received: DEVFS=/proc/bus/usb [repeated 3 times, last time on Jan 1 01:00:32 2003]
Jan 1 01:00:30 2003	System log	Message	kern.info usbserial.c: Generic converter now attached to ttyUSB2 (or usb/tts/2 for devfs)
Jan 1 01:00:30 2003	System log	Message	kern.info usbserial.c: Generic converter detected
Jan 1 01:00:30 2003	System log	Message	kern.info usbserial.c: Generic converter now attached to ttyUSB1 (or usb/tts/1 for devfs)
Jan 1 01:00:30 2003	System log	Message	kern.info usbserial.c: Generic converter detected
Jan 1 01:00:30 2003	System log	Message	kern.info usbserial.c: Generic converter now attached to ttyUSB0 (or usb/tts/0 for devfs)
Jan 1	System		

Figure 7.3: System Log

7.4 System Up Time

Select the *System* tab to display the amount of time that has passed since the system was last started.

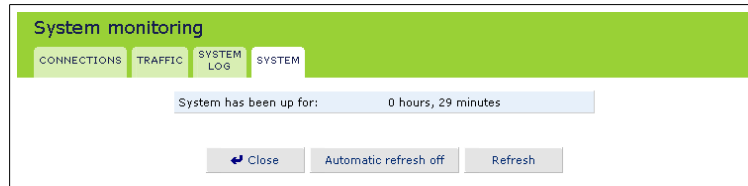


Figure 7.4: System Up Time



Glossary

PAP Password Authentication Protocol, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP.

CHAP Challenge Handshake Authentication Protocol, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. The sender and peer must share a predefined secret.

Authentication The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Encryption The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

MPPE Microsoft Point to Point Encryption (MPPE) is a means of representing Point to Point Protocol (PPP) packets in an encrypted form.

Broadcast Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients.

Multicast To transmit a single message to a select group of recipients. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks.

-
- PPTP** Point-to-Point Tunneling Protocol, a technology for creating Virtual Private Networks (VPNs). Because the Internet is essentially an open network, the Point-to-Point Tunneling Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.
- PPTP** IP Security, a set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).
- VPN** A Virtual Private Network (VPN) is a private Network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling Protocol and security procedures.
- 100Base-T** Also known as "Fast Ethernet", an Ethernet cable standard with a data transfer rate of up to 100 Mbps.
- 10Base-T** An older Ethernet cable standard with a data transfer rate of up to 10 Mbps.
- 802.11, 802.11b** A family of IEEE (Institute of Electrical and Electronics Engineers)-defined specifications for wireless networks. Includes the 802.11b standard, which supports high-speed (up to 11 Mbps) wireless data transmission.
- 802.3** The IEEE (Institute of Electrical and Electronics Engineers - defined specification that describes the characteristics of Ethernet (wired) connections.
- Access point** A device that exchanges data between computers on a network. An access point typically does not have any Firewall or NAT capabilities.
- Ad hoc network** A solely wireless computer-to-computer network. Unlike an infrastructure network, an ad hoc network does not include a gateway router.
- Adapter** Also known as a *Network Interface Card* (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.
- Administrator** A person responsible for planning, configuring, and managing the day-to-day operation of a computer network. The duties of an administrator include installing new workstations and other devices, adding and removing individuals from the list of authorized users, archiving files, overseeing password protection and other security measures, monitoring usage of shared resources, and handling malfunctioning equipment.
- Bandwidth** The amount of information, or size of file, that can be sent through a network connection at one time. A connection with more bandwidth can transfer information more quickly.
- Bridge** A device that forwards packets of information from one segment of a network to another. A bridge forwards only those packets necessary for communication between the segments.
- Broadband connection** A high-speed connection, typically 256 Kbps or faster. Broadband services include cable modems and DSL.

-
- Broadband modem** A device that enables a broadband connection to access the Internet. The two most common types of broadband modems are cable modems, which rely on cable television infrastructure, and DSL modems, which rely on telephone lines operating at DSL speeds.
- Bus** A set of hardware lines used for data transfer among the components of a computer system. A bus essentially allows different parts of the system to share data. For example, a bus connects the disk-drive controller, memory, and input/output ports to the microprocessor.
- Cable modem** A device that enables a broadband connection to access the Internet. Cable modems rely on cable television infrastructure, in other words, the data travels on the same lines as you cable television.
- CAT 5 cable** Abbreviation for *Category 5 cable*. A type of Ethernet cable that has a maximum data rate of 100 Mbps.
- Channel** A path or link through which information passes between two devices.
- Client** Any computer or program that connects to, or requests the services of, another computer or program on a network. For a local area network or the Internet, a client is a computer that uses shared network resources provided by a server.
- Client/server network** A network of two or more computers that rely on a central server to mediate the connections or provide additional system resources. This dependence on a server differentiating a client/server network from a peer-to-peer network.
- Computer name** A name that uniquely identifies a computer on the network so that all its shared resources can be accessed by other computers on the network. One computer name cannot be the same as any other computer or domain name on the network.
- Crossover cable** A type of cable that facilitates network communications. A crossover cable is a cable that is used to interconnect two computers by "crossing over" (reversing) their respective pin contacts.
- DHCP** Acronym for *Dynamic Host Configuration Protocol*. A TCP/IP protocol that automatically assigns temporary IP addresses to computers on a local area network (LAN). GlobeSurfer 3G supports the use of DHCP. You can use DHCP to share one Internet connection with multiple computers on a network.
- Dial-up connection** An Internet connection of limited duration that uses a public telephone network rather than a dedicated circuit or some other type of private network.
- DMZ** Acronym for *demilitarized zone*. A collection of devices and subnets placed between a private network and the Internet to help protect the private network from unauthorized Internet users.
- DNS** Acronym for *Domain Name System*. A data query service chiefly used on the Internet for translating host names into Internet addresses. The DNS database maps DNS domain names to IP addresses, so that users can locate computers and services through user-friendly names.

Domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

Domain name An address of a network connection that identifies the owner of that address in a hierarchical format: server.organization.type. For example, www.whitehouse.gov identifies the Web server at the White House, which is part of the U.S. government.

Drive An area of storage that is formatted with a file system and has a drive letter. The storage can be a floppy disk (which is often represented by drive A), a hard disk (usually drive C), a CD-ROM (usually drive D), or another type of disk. You can view the contents of a drive by clicking the drive's icon in Windows Explorer or My Computer. Drive C (also known as the hard disk), contains the computer's operating system and the programs that have been installed on the computer. It also has the capacity to store many of the files and folders that you create.

Driver Within a networking context, a device that mediates communication between a computer and a network adapter installed on that computer.

DSL Acronym for *Digital Subscriber Line*. A constant, high-speed digital connection to the Internet that uses standard copper telephone wires.

DSL modem A device that enables a broadband connection to access the Internet. DSL modems rely on telephone lines that operate at DSL speeds.

Duplex A mode of connection. Full-duplex transmission allows for the simultaneous transfer of information between the sender and the receiver. Half-duplex transmission allows for the transfer of information in only one direction at a time.

Dynamic IP address The IP address assigned (using the DHCP protocol) to a device that requires it. A dynamic IP address can also be assigned to a gateway or router by an ISP.

Edge computer The computer on a network that connects the network to the Internet. Other devices on the network connect to this computer. The computer running the most current, reliable operating system is the best choice to designate as the edge computer.

Ethernet A networking standard that uses cables to provide network access. Ethernet is the most widely-installed technology to connect computers together.

Ethernet cable A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. there is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second.

Firewall A security system that helps protect a network from external threats, such as hacker attacks, originating outside the network. A hardware Firewall is a connection routing device that has specific data checking settings and that helps protect all of the devices connected to it.

Firmware Software information stored in nonvolatile memory on a device.

Flash memory A type of memory that does not lose data when power is removed from it. Flash memory is commonly used as a supplement to or replacement for hard disks in portable computers. In this context, flash memory either is built in to the unit or, more commonly, is available as a PC Card that can be plugged in to a PCMCIA slot.

FTP Acronym for *File Transfer Protocol*. The standard Internet protocol for downloading, or transferring, files from one computer to another.

Gateway A device that acts as a central point for networked devices, receives transmitted messages, and forwards them. GlobeSurfer 3G can link many computers on a single network, and can share an encrypted Internet connection with wired and wireless devices.

Gateway address The IP address you use when you make a connection outside your immediate network.

Hexadecimal A numbering system that uses 16 rather than 10 as the base for representing numbers. It is therefore referred to as a base-16 numbering system. The hexadecimal system uses the digits 0 through 9 and the letters A through F (uppercase or lowercase) to represent the decimal numbers 0 through 15. For example, the hexadecimal letter D represents the decimal number 13. One hexadecimal digit is equivalent to 4 bits, and 1 byte can be expressed by two hexadecimal digits.

HomePNA An industry standard that ensures that through existing telephone lines and a registered jack, computer users on a home network can share resources (such as an Internet connection, files, and printers) without interfering with regular telephone service. HomePNA currently offers data transmission speeds of up to 10 Mbps.

HomeRF An industry standard that combines 802.11b and portable phone standards for home networking. It uses frequency hopping (switching of radio frequencies within a given bandwidth to reduce the risk of unauthorized signal interception). HomeRF offers data transmission speeds of up to 1.6 Mbps at distances of up to 150 feet.

Host name The DNS name of a device on a network, used to simplify the process of locating computers on a network.

Hub A device that has multiple ports and that serves as a central connection point for communication lines from all devices on a network. When data arrives at one port, it is copied to the other ports.

IEEE Acronym for *Institute of Electrical and Electronics Engineers*. A society of engineering and electronics professionals that develops standards for the electrical, electronics, computer engineering, and science-related industries. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters I-E-E-E.

Infrastructure network A network configuration in which wireless devices connect to a wireless access point (such as GlobeSurfer 3G) instead of connecting to each other directly.

Internet domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

Intranet A network within an organization that uses Internet technologies (such a Web browser for viewing information) and protocols (such as TCP/IP), but is available only to certain people, such as employees of a company. Also called a private network. Some intranets offer access to the Internet, but such connections are directed through a Firewall.

IP Acronym for *Internet Protocol*. The protocol within TCP/IP that is used to send data between computers over the Internet. More specifically, this protocol governs the routing of data messages, which are transmitted in smaller components called packets.

IP address Acronym for *Internet Protocol* address. IP is the protocol within TCP/IP that is used to send data between computers over the Internet. An IP address is an assigned number used to identify a computer that is connected to a network through TCP/IP. An IP address consists of four numbers (each of which can be no greater than 255) separated by periods, such as 192.168.1.1.

ISO/OSI reference model Abbreviation for "International Organization for Standardization Open Systems Interconnection" reference model. An architecture that standardizes levels of service and types of interaction for computers that exchange information through a communications network. The ISO/OSI reference model separates computer-to-computer communications into seven protocol layers, or levels; each builds on and relies on the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the program level. It is a fundamental blueprint designed to help guide the creation of hardware and software for networks.

ISP Acronym for *Internet Service Provider*. A company that provides individuals or companies access to the Internet.

Kbps Abbreviation of *kilobits per second*. Data transfer speed, as through a modem or on a network, measured in multiples of 1,000 bits per second.

LAN Acronym for *Local Area Network*. A group of computers and other devices dispersed over a relatively limited area (for example, a building) and connected by a communications link that enables any device to interact with any other on the network.

MAC address Abbreviation for *Media Access Control* address. The address that is used for communication between network adapters on the same subnet. Each network adapter is manufactured with its own unique MAC address.

MAC layer Abbreviation for *Media Access Control* layer. The lower of two sub layers that make up the data-link layer in the ISO/OSI reference model. The MAC layer manages access to the physical network, so a protocol like Ethernet works at this layer.

mapping A process that allows one computer to communicate with a resource located on another computer on the network. For example, if you want to access a folder that resides on another computer, you “map to” that folder, as long as the computer that holds the folder has been configured to share it.

Mbps Abbreviation of *megabits per second*. A unit of bandwidth measurement that defines the speed at which information can be transferred through a network or Ethernet cable. One megabyte is roughly equivalent to eight megabits.

Modem A device that transmits and receives information between computers.

NAT Acronym for *Network Address Translation*. The process of converting between IP addresses used within a private network and Internet IP addresses. NAT enables all of the computers on a network to share one IP address.

Network A collection of two or more computers that are connected to each other through wired or wireless means. These computers can share access to the Internet and the use of files, printers, and other equipment.

Network adapter Also known as a *Network Interface Card* (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.

Network name The single name of a grouping of computers that are linked together to form a network.

Network printer A printer that is not connected directly to a computer, but is instead connected directly to a network through a wired or wireless connection.

Packet A unit of information transmitted as a whole from one device to another on a network.

PC Card A peripheral device that adds memory, mass storage, modem capability, or other networking services to portable computers.

PCI Acronym for *Peripheral Component Interconnect*. A specific bus type designed to be used with devices that have high bandwidth requirements.

PCI card A card designed to fit into a PCI expansion slot in a personal computer. PCI cards provide additional functionality; for example, two types of PCI cards are video adapters and network interface cards. See PCI.

PCI expansion slot A connection socket designed to accommodate PCI cards.

PCMCIA Acronym for *Personal Computer Memory Card International Association*. A nonprofit organization of manufacturers and vendors formed to promote a common technical standard for PC Card-based peripherals and the slot designed to hold them, primarily on portable computers and intelligent electronic devices.

Peer-to-peer network A network of two or more computers that communicate without using a central server. This lack of reliance on a server differentiates a peer-to-peer network from a client/server network.

-
- PING** A protocol for testing whether a particular computer is connected to the Internet by sending a packet to the computer's IP address and waiting for a response.
- Plug and Play** A set of specifications that allows a computer to automatically detect and configure various peripheral devices, such as monitors, modems, and printers.
- Port** A physical connection through which data is transferred between a computer and other devices (such as a monitor, modem, or printer), a network, or another computer. Also, a software channel for network communications.
- PPPoE** Acronym for *Point-to-Point Protocol over Ethernet*. A specification for connecting users on an Ethernet network to the Internet by using a broadband connection (typically through a DSL modem).
- Profile** A computer-based record that contains an individual network's software settings and identification information.
- Protocol** A set of rules that computers use to communicate with each other over a network.
- Resource** Any type of hardware (such as a modem or printer) or software (such as an application, file, or game) that users can share on a network.
- Restore factory defaults** The term used to describe the process of erasing the current settings of your device to restore factory settings. You accomplish this by pressing the Reset button and holding it for five or more seconds. Note that this is different from just resetting the device.
- RJ-45 connector** An attachment found on the ends of all Ethernet cables that connects Ethernet (wired) cables to other devices and computers
- Server** A computer that provides shared resources, such as storage space or processing power, to network users.
- Shared folder** A folder (on a computer) that has been made available for other people to use on a network.
- Shared printer** A printer (connected to a computer) that has been made available for other people to use on a network.
- Sharing** To make the resources associated with one computer available to users of other computers on a network.
- SNTP** Acronym for *Simple Network Time Protocol*. A protocol that enables client computers to synchronize their clocks with a time server over the Internet.
- SSID** Acronym for *Service Set Identifier*, also known as a "wireless network name." An SSID value uniquely identifies your network and is case sensitive.
- Static IP address** A permanent Internet address of a computer (assigned by an ISP).
- Straight-through cable** A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. There is twisted pair, and coax Ethernet cables. Each of these allow data to travel at

10Mbit per second. Unlike the Crossover cable, straight-through cable has the same order of pin contacts on each end-plug of the cable.

Subnet A distinct network that forms part of a larger computer network. Subnets are connected through routers and can use a shared network address to connect to the Internet.

Subnet mask Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. Similar in form to an IP address and typically provided by an ISP. An example of a subnet mask value is 255.255.0.0.

Switch A central device that functions similarly to a hub, forwarding packets to specific ports rather than broadcasting every packet to every port. A switch is more efficient when used on a high-volume network.

Switched network A communications network that uses switching to establish a connection between parties.

Switching A communications method that uses temporary rather than permanent connections to establish a link or to route information between two parties. In computer networks, message switching and packet switching allow any two parties to exchange information. Messages are routed (switched) through intermediary stations that together serve to connect the sender and the receiver.

TCP/IP Acronym for *Transmission Control Protocol/Internet Protocol*. A networking protocol that allows computers to communicate across interconnected networks and the Internet. Every computer on the Internet communicates by using TCP/IP.

Throughput The data transfer rate of a network, measured as the number of kilobytes per second transmitted.

USB Acronym for *universal serial bus*. USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.

USB adapter A device that connects to a USB port.

USB connector The plug end of the USB cable that is connected to a USB port. It is about half an inch wide, rectangular and somewhat flat.

USB port A rectangular slot in a computer into which a USB connector is inserted.

UTP Acronym for *unshielded twisted pair*. A cable that contains one or more twisted pairs of wires without additional shielding. It's more flexible and takes less space than a shielded twisted pair (STP) cable, but has less bandwidth.

Virtual server One of multiple Web sites running on the same server, each with a unique domain name and IP address.

WAN Acronym for *Wide Area Network*. A geographically widespread network that might include many linked local area networks.

Wi-Fi A term commonly used to mean the wireless 802.11b standard.

Wireless Refers to technology that connects computers without the use of wires and cables. Wireless devices use radio transmission to connect computers on a network to one another. Radio signals can be transmitted through walls, ceilings, and floors, so you can connect computers that are in different rooms in the house without physically attaching them to one another.

Wireless access point A device that exchanges data between wireless computers or between wireless computers and wired computers on a network.

Wireless network name The single name of a grouping of computers that are linked together to form a network.

Wireless security A wireless network encryption mechanism that helps to protect data transmitted over wireless networks.

WLAN Acronym for *Wireless Local Area Network*. A network that exclusively relies on wireless technology for device connections.