

GlobeSurfer® III+

Technical Reference Manual

Copyright © 2012, Option.

All information about Option GlobeSurfer® III+ may change without prior notice. Information published in this reference manual is accurate at the time of publication. Although all security precautions were taken during the creation of this reference manual, Option is not liable toward persons or organizations for losses or damages caused either directly or indirectly due to instructions contained in this reference manual. 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® III+, visit www.option.com

Questions and answers regarding the GlobeSurfer® III+ can be found on our Support website:

<http://www.option.com/en/support/faq/>

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

<http://www.option.com/en/support/support-ticketing-system/>

For registering please go to:

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

March 2012

Table of Contents

1	Introduction to GlobeSurfer® III+	7
1.1	Simple set-up	7
1.2	Instant protection.....	7
1.3	Additional security	7
1.4	Stay in touch	7
1.5	Important note	8
1.6	About This Manual.....	8
2	Setup	8
2.1	Setting up WAN and LAN connections.....	8
2.2	Computer Network Configuration	9
3	The GlobeSurfer® III+ management console	9
3.1	Accessing the GlobeSurfer® III+ Management Console.....	9
3.2	Menu System	10
3.3	Managing Tables	10
3.4	Home.....	11
3.4.1	Overview	11
3.4.2	Map View.....	12
3.4.3	Installation Wizard	12
3.5	Quick Setup	19
3.6	Internet Connection	20

3.6.1	General.....	21
3.6.2	Settings	21
3.6.3	Routing	22
3.6.4	Connection Watchdog.....	24
3.6.5	SMS Control.....	24
3.6.6	Advanced	25
3.7	Local Network.....	26
3.7.1	Overview	26
3.7.2	Device	27
3.7.3	Wireless	28
4	Services.....	30
4.1	Overview	30
4.2	Firewall.....	31
4.2.1	Overview	32
4.2.2	Access Control.....	34
4.2.3	Port Forwarding	44
4.2.4	DMZ Host	47
4.2.5	Port Triggering	49
4.2.6	Website Restrictions	54
4.2.7	NAT.....	57
4.2.8	Connections.....	61
4.2.9	Advanced Filtering.....	62
4.3	VPN/Internet Protocol Security (IPSec).....	74
4.3.1	Internet Protocol Security (IPSec) Settings	75
4.3.2	IPSec Log Settings	76
4.4	Shared Storage / Disk Management	77

4.4.1	Adding normal disk drives.....	78
4.4.2	Adding RAID devices	82
4.5	Shared Printers/Print Server	83
4.5.1	Alternative Method of Configuring the Print Server	86
4.6	Failover	87
4.6.1	Failover Configuration	88
4.6.2	Configuration example.....	92
5	System.....	96
5.1	Overview	96
5.2	System Settings.....	97
5.2.1	Overview/System Settings	97
5.2.2	Date and Time	100
5.3	Users.....	103
5.3.1	User Setting	104
5.3.2	Group setting.....	106
5.4	Network Connection	106
5.4.1	Connection wizard	108
5.5	LAN Bridge	111
5.5.2	LAN Ethernet.....	120
5.5.3	LAN Wireless.....	121
5.5.4	WAN Cellular	128
5.5.5	Configuring your Windows XP clients.....	131
5.6	Monitor	133
5.6.1	Network Connection.....	133
5.6.2	CPU	134
5.6.3	System Log.....	135

5.7	Routing	136
5.7.1	General/Routing.....	136
5.7.2	BGP and OSPF	139
5.7.3	PPPoE Relay.....	140
5.8	Management	140
5.8.1	Universal Plug and Play	141
5.8.2	Simple network Management Protocol (SNMP)	141
5.8.3	Remote Administration	143
5.9	Maintenance	144
5.9.1	About GlobeSurfer III+.....	145
5.9.2	Configuration File	145
5.9.3	Reboot.....	146
5.9.4	Restore Factory Settings.....	147
5.9.5	Firmware Upgrade.....	147
5.9.6	Diagnostics	148
5.10	Objects and Rules	150
5.10.1	Protocols	150
5.10.2	Network Objects	155
5.10.3	Scheduler Rules	157
5.10.4	Certificates.....	160
6	Shortcuts	169
7	Telephone.....	170
7.1	Missed calls.....	171
7.2	Incoming calls.....	171
7.3	Outgoing calls.....	171
7.4	Telephone settings	172

7.5	Call Forwarding	172
7.6	Call Waiting.....	174
7.7	Caller ID.....	174
7.8	SIM Setup.....	175
7.8.1	SIM PIN Change	176
7.8.2	SIM PIN enable.....	176
7.8.3	SIM PIN2 change.....	177
7.8.4	Unlock device	177
8	SMS.....	177
8.1	SMS Create.....	178
8.2	Inbox	179
8.3	Outbox	180
8.4	Sent	180
8.5	Drafts	181
8.6	Templates	181
8.7	Archive	181
8.8	SIM card.....	182
8.9	Settings	182
9	List of Acronyms.....	182
10	Glossary	184

1 Introduction to GlobeSurfer® III+

Within minutes, you can connect to your mobile network and use a wireless connection to the Internet through the mobile network.

GlobeSurfer III+ is compatible with GSM and 3G mobile networks and supports GPRS, EDGE, UMTS, HSDPA and HSUPA technologies. With 'Receive Diversity' on all the high as well as low bands, the signal strength and overall 3G reception is unparalleled.

Tip: To achieve the best possible reception, check the signal strength using the web interface. You may find that placing the unit near a window provides the best reception.

1.1 Simple set-up

GlobeSurfer III+ provides you with a quick installation and set-up that gets you easily and quickly connected to the Internet. You can use any internet browser (e.g. Internet Explorer 7.0 or Firefox 2.5) and most operating systems including Windows, Macintosh and Linux. The 'Quick Setup Wizard' introduces you to the basic settings that need to be configured for use with the mobile network. Once you have configured, you can review and enable customized wireless security settings.

1.2 Instant protection

Your GlobeSurfer III+ supports Network Address Translation (NAT). This network service hides the computers in your network so they cannot be found or directly accessed from outside your network. A firewall is also included which, by default, blocks incoming traffic and allows outgoing traffic.

1.3 Additional security

GlobeSurfer III+ supports both Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA and WPA2) to protect your network data. Security logs keep you aware of potential security risks and intrusion attempts. You can view logs online or via email.

1.4 Stay in touch

You can use GlobeSurfer III+ to send and receive SMS text messages. The LED on the front panel lets you know when a new SMS arrives. If you have installed the "Notifier" software application, then you will also receive a desktop alert indicating the receipt of text messages. The "Notifier" software will also allow you to connect directly to the browser page that handles SMS text messages.

You can use GlobeSurfer III+ to make mobile phone calls. Should you miss a call an LED indicates this. If you have installed the "Notifier" software application, then you will also receive a desktop alert indicating the receipt of telephone calls, as well as missed calls. The "Notifier" software will also allow you to connect directly to the browser page that handles telephone calls.

1.5 Important note

To protect your network from unauthorized access, and to make it more difficult for hackers to analyze your data, please configure the WLAN security settings and enable WEP, WPA or WPA2 encryption on your GlobeSurfer III+.

1.6 About This Manual

This manual describes configuration and operation of GlobeSurfer® III+. It is intended as a complement to the GlobeSurfer® III+ User Guide to provide reference information for the advanced user of the GlobeSurfer® III+. It is assumed that the hardware installation of GlobeSurfer® III+ has been done and you have a device that is able to communicate with the GlobeSurfer® III+ via Ethernet or WLAN when the Reference Manual is read.

This version of the manual is valid for GlobeSurfer® III+.

2 Setup

Connecting your computer or home network to the GlobeSurfer® III+ is a simple procedure, varying slightly depending on your operating system. This chapter will help you to seamlessly integrate GlobeSurfer® III+ with your computer or home network. The Windows default network settings dictate that in most cases the setup procedure described below will be unnecessary. However, if you are having problems 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 setup procedure consists of three configuration stages:

- Setting up WAN and LAN connections
- PC Network Configuration
- GlobeSurfer® III+ Quick Setup

2.1 Setting up WAN and LAN connections

WAN Connection: setting up the WAN connection requires that a SIM card is inserted correctly into the SIM slot of the GlobeSurfer® III+. See the GlobeSurfer® III+ 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 GlobeSurfer® III+. The first time you login to GlobeSurfer® III+ you will have to enter a PIN code if the SIM card has one enabled. The PIN code is received from your ISP, but normally provided separately from the SIM card for security reasons. If your SIM card does not have a PIN code enabled it is recommended for security reasons to set enable it either using a mobile phone or via the GlobeSurfer® III+ web interface.

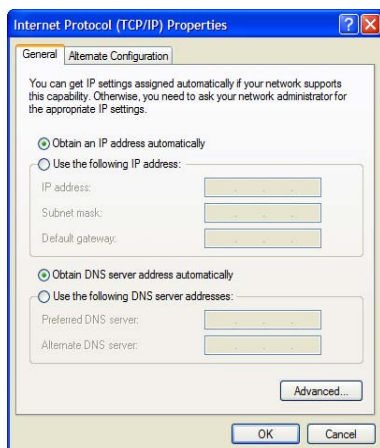
LAN Connection: your computer can connect to the GlobeSurfer® III+ in two ways, either through Ethernet or through the use of WiFi. The simplest type of connection is Ethernet and this is recommended for initial setup purposes. The GlobeSurfer® III+ featuring two such ports. Use an Ethernet cable to connect between an Ethernet port on your GlobeSurfer® III+ and your computer's network card. Please refer to the accompanying User Guide for additional information.

2.2 Computer Network Configuration

GlobeSurfer® III+ provides a DHCP server on its LAN and it is recommended to configure your computer's LAN interface to obtain its IP and DNS server IPs automatically. This configuration principle is true for most operating systems but the steps to do this are specific to each operating system.

Normally your computer's LAN interfaces are setup to use DHCP but if your computer fails to connect to the GlobeSurfer® III+ when you plug in the Ethernet cable check the computer's configuration.

For illustration purposes the following screen displays the TCP/IP Properties dialog box as it appears in Windows XP.



- Access Network Connections from the Control Panel.
- Right-click the Ethernet connection icon and select Properties.
- Under the General tab, select the Internet Protocol (TCP/IP) component, and press the Properties button.
- The Internet Protocol (TCP/IP) properties window will be displayed.
- Select the Obtain an IP address automatically radio button.
- Select the Obtain DNS server address automatically radio button.
- Click OK to save the settings.

3 The GlobeSurfer® III+ management console

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

3.1 Accessing the GlobeSurfer® III+ Management Console

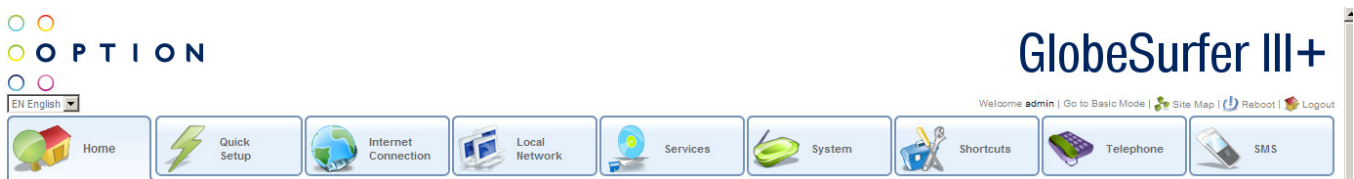
To access the management console:

- Launch a Web-browser on a PC in the LAN or WLAN.
- Type the IP address of the GlobeSurfer® III+ in the address. The default IP address is 192.168.1.1
- Enter your username and password to log on to the web-based management console.

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 re-enter your user name and password before proceeding. This feature helps to prevent unauthorized users from accessing the management console and changing the GlobeSurfer® III+ settings.

3.2 Menu System

The GlobeSurfer® III+ management console screens have been grouped into several subject areas and may be accessed by clicking on the appropriate icon in the top menu.



The subject areas are:

- Home: displays an overview of the status of the Internet Connection, Local Network, Storage, Printers and Services
- Quick Setup: quick access to basic configuration
- Internet Connection: configure internet connections
- Local Network: configure local network, storage and printer settings
- Services: configure Firewall, Print Server, Personal Domain Name, File Server and IPSec settings
- System: configure system settings
- Shortcuts: displays icons to enable quick and easy access to all areas
- Telephone: manage your telephony options
- SMS: manage your SMS messages


3.3 Managing Tables


Tables are used throughout the GlobeSurfer® III+ 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.

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Input						
<input checked="" type="checkbox"/> 0	Any	Any	FTP - TCP Any -> 21	ALG FTP	Active	
<input checked="" type="checkbox"/> 1	Any	Any	IKE - UDP 500 -> 500	ALG IPSec	Active	
<input checked="" type="checkbox"/> 2	Any	Any	SIP - UDP Any -> 5060	ALG SIP	Active	
<input checked="" type="checkbox"/> 3	Any	Any	H.323 Call Signaling - TCP Any -> 1720	ALG H.323 CSL	Active	
New Entry						

In 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.

 Click the Move Down icon to move an entry down.

 Click the Move Up icon to move an entry up.

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

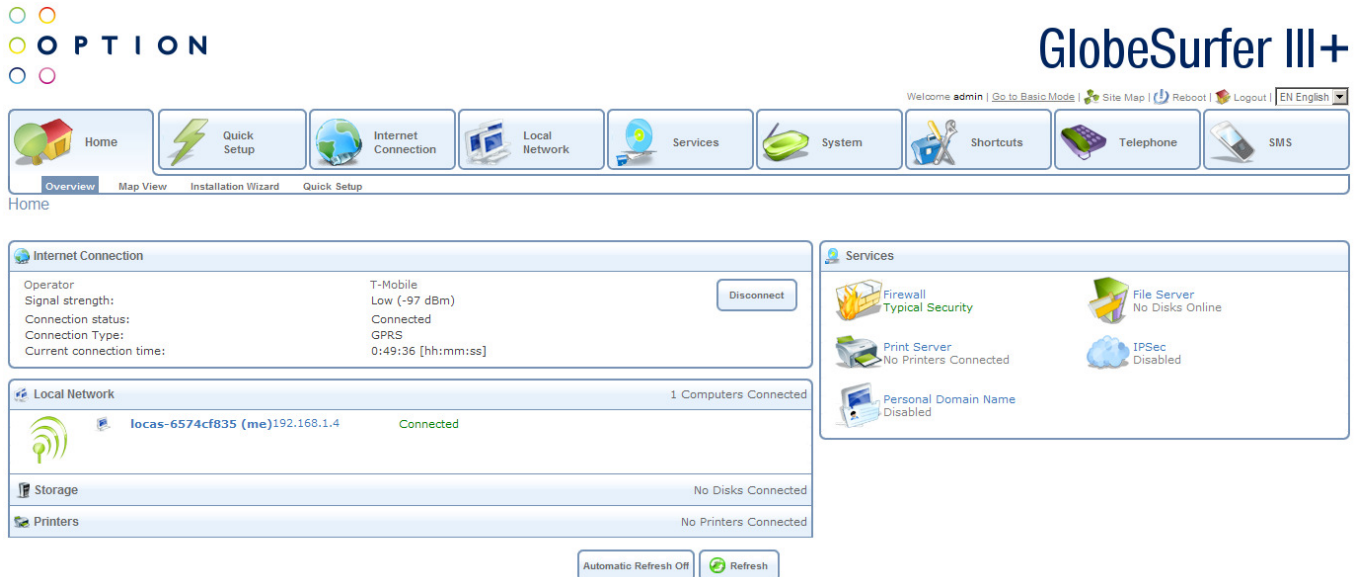
3.4 Home

From this screen you can click on the tabs at the top left hand side to route to the following screens:

- Overview - status of Internet Connection/Local Network/Storage/Printers/Services
- Map View - pictorial overview of all components connected to GlobeSurfer® III+
- Installation Wizard - guides you through the main settings for your GlobeSurfer® III+
- Quick Setup - routes directly to the Quick Setup area to change the main settings

3.4.1 Overview

This screen displays an overview of the status of the Internet Connection, Local Network, Storage, Printers and Services available to you with GlobeSurfer® III+. For details of each component you can easily drill down by clicking on the area.



OPTION

GlobeSurfer III+

Welcome **admin** | [Go to Basic Mode](#) | [Site Map](#) | [Reboot](#) | [Logout](#) | [EN English](#)

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Map View Installation Wizard Quick Setup

Home

Internet Connection

Operator: T-Mobile
Signal strength: Low (-97 dBm)
Connection status: Connected
Connection Type: GPRS
Current connection time: 0:49:36 [hh:mm:ss]

Local Network 1 Computers Connected

locas-6574cf835 (me) 192.168.1.4 Connected

Storage No Disks Connected

Printers No Printers Connected

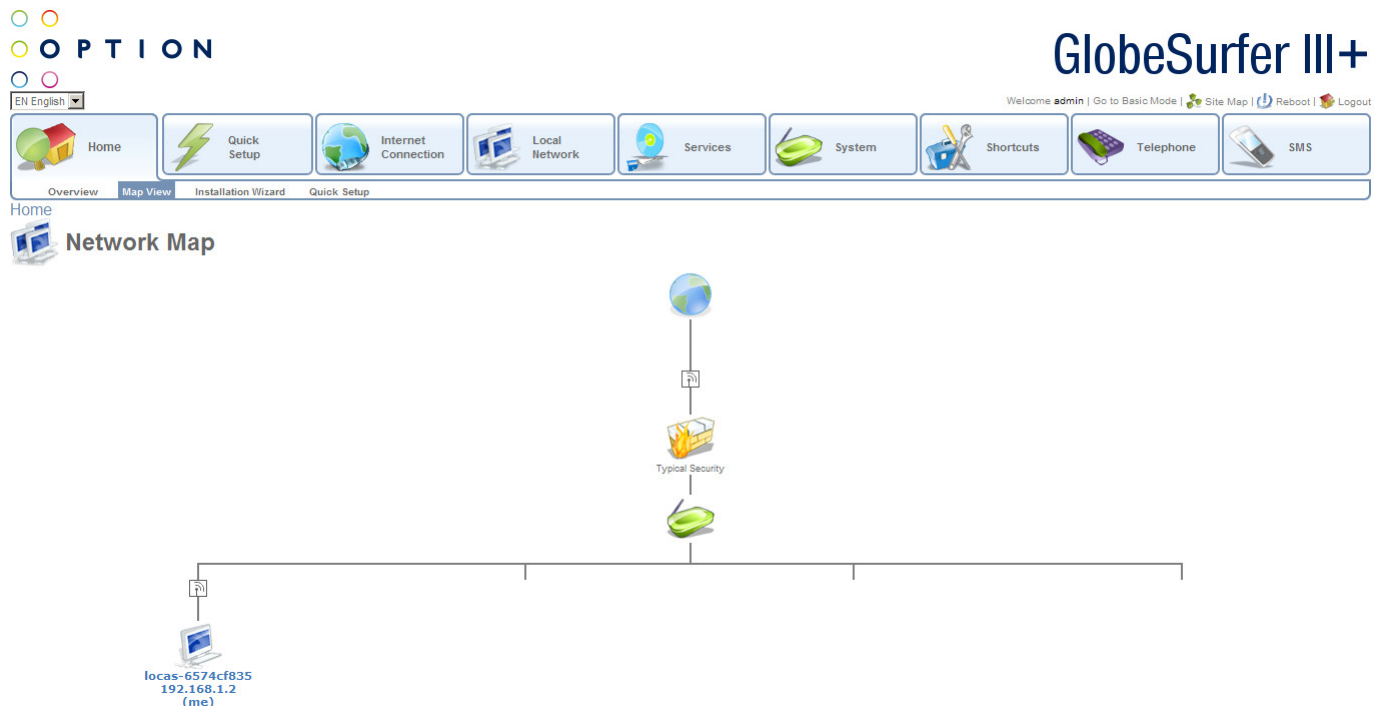
Services

Firewall Typical Security
File Server No Disks Online
Print Server No Printers Connected
IPSec Disabled
Personal Domain Name Disabled

Automatic Refresh Off Refresh

3.4.2 Map View

This screen shows a pictorial overview of all components currently connected to your GlobeSurfer® III+ including the firewall and all networks including wireless networks. For details of each component you can easily drill down by clicking on the component icon.



3.4.3 Installation Wizard

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

Start a web browser on your PC.

Enter the address 192.168.1.1 to display the GlobeSurfer® III+ management console. When first logging on to the management console, the Login screen will appear. Configure your language settings and enter a 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 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® III+ from now on.



GlobeSurfer III+

Language:	EN English
User Name:	
Password (case sensitive):	
<input type="button" value="OK"/>	

After choosing your password and clicking OK you will be forwarded to the Installation Wizard page. Click OK to continue the Installation Wizard.

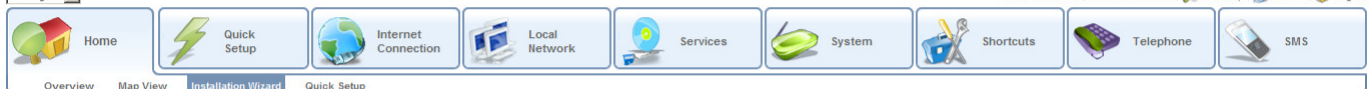
The Installation Wizard helps you to quickly set the most important settings of your GlobeSurfer® III+. If you would like to complete the Installation without using the Wizard just click Cancel. Alternatively, click the Quick Setup icon on the left sidebar, after login in. The following sections describe the various configuration parameters of Installation. Once you have filled the Installation sections as described below, click the OK button to configure your GlobeSurfer® III+.



EN English

GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout



Home

Installation Wizard

Follow the instructions on each page and click 'Next' to continue.

Navigate using '< Back' and 'Next >'. 'Cancel' will exit the wizard.

Click 'Finish' on the Finish page and confirm with 'OK' to accept and save the settings.

Note: Changes will be discarded if you click 'Cancel'.



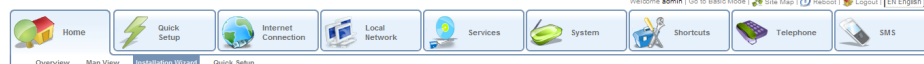
3.4.3.1 Installation Wizard: Language

Select the language and time zone you would like to use on the GlobeSurfer® III+ Management Console and Display.



GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout | EN English



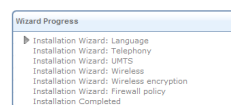
Home

Installation Wizard: Language

Select the language for GlobeSurfer III+.

Note: The current language setting will be restored if you cancel the wizard before clicking 'OK' (after 'Finish').

Language and region settings	
Language:	EN English
Time Zone:	GMT (GMT+02:00)



3.4.3.2 Installation Wizard: Telephony

Select the protocol for your telephone handset. This will adapt the telephone interface of the GlobeSurfer® III+ to work with your handset.

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Map View Installation Wizard Quick Setup

Installation Wizard: Telephony

Select the standard supported by your caller ID box.

Telephony

Caller ID: ETSI DTMF

Back Next Cancel

Wizard Progress

- Installation Wizard: Language
- Installation Wizard: Telephony
- Installation Wizard: UMTS
- Installation Wizard: Wireless encryption
- Installation Wizard: Firewall policy
- Installation Completed

3.4.3.3 Installation Wizard: UMTS

Check or change the following settings on the Installation screen to configure the UMTS connection:

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Map View Installation Wizard Quick Setup

Installation Wizard: UMTS

Configure GlobeSurfer III UMTS settings.

- Access Point Name: Enter the APN provided by your Internet Service Provider, or accept the default.
- UMTS Connect method:
 - Connect Manually: connect to the Internet by clicking 'Connect' on the 'Connection Status' page in the management console or press the 'Connect' button on the GlobeSurfer III unit.
 - Automatically connect upon traffic: GlobeSurfer III will automatically connect when you attempt to send data via the Internet.
 - Always connected: GlobeSurfer III will connect to the internet when possible and will remain connected.
- In case of inactivity, disconnect after(minutes): Set it to zero (0) if you want the UMTS to stay connected. The maximum is 1440 minutes (24hrs). Note: Incoming traffic is treated as inactivity.

UMTS

Access point name: general.t-mobile.uk

UMTS connect method:
☒ Connect Manually
☐ Automatically connect upon traffic
☐ Always connected

In case of inactivity, disconnect after (minutes): 0

Back Next Cancel

Wizard Progress

- Installation Wizard: Language
- Installation Wizard: Telephony
- Installation Wizard: UMTS
- Installation Wizard: Wireless encryption
- Installation Wizard: Firewall policy
- Installation Completed

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

3.4.3.3.1 UMTS connect method:

Connect Manually: connect to the Internet by clicking Connect on the Connection Status page in the management console or press the Connect button on the GlobeSurfer® III+ unit.

Automatically connect upon traffic: GlobeSurfer® III+ will automatically connect when you attempt to send data via the Internet.

Always connected: GlobeSurfer® III+ will connect to the internet when possible and will remain connected.

In case of inactivity, disconnect after (minutes): the default is zero (0), meaning UMTS will stay connected until manually disconnected. The maximum is 1440 minutes (24hrs). Note: For this purpose incoming traffic is not activity.

3.4.3.4 Installation Wizard: Wireless

SSID: the Service Set Identifier: enter a name for your local wireless network (WLAN) (maximum 32 characters).

Note: Setting the SSID to something unique will make it much easier to identify your own wireless network, especially if there are other wireless networks available in the nearby area.

SSID broadcast: if you set the Enabled checkbox to broadcast, then other devices can detect and connect to your WLAN. Clear the checkbox to disable broadcasting and hide the name of your network. This provides minimal security, as other devices have to know the SSID to connect. You can install the WLAN with this feature enabled and then disable it once you have set up GlobeSurfer® III+ and its associated wireless clients.

OPTION

GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Map View **Installation Wizard** Quick Setup

Home

Installation Wizard: Wireless

- SSID: The Service Set Identifier: enter a name for your local wireless network(WLAN) (maximum 32 characters).
- SSID broadcast: If you set the 'Enabled' checkbox to broadcast then other devices can detect and connect to your WLAN. Clear the checkbox to disable broadcasting and hide the name of your network. This provides minimal security as other devices have to know the SSID to connect. You can install the WLAN with this feature enabled and then disable it once you have set up GlobeSurfer III and its associated wireless clients.

Wireless	
Wireless:	<input checked="" type="checkbox"/> Enabled
SSID:	<input type="text" value="SSIDDeborah"/>
SSID Broadcast:	<input checked="" type="checkbox"/> Enabled

Back Next Cancel

Wizard Progress

- Installation Wizard: Language
- Installation Wizard: Telephony
- Installation Wizard: UMTS
- ▶ Installation Wizard: Wireless
- Installation Wizard: Wireless encryption
- Installation Wizard: Firewall policy
- Installation Completed

3.4.3.5 Installation Wizard: Wireless Encryption

In order to prohibit unauthorized access to your GlobeSurfer® III+, make sure to apply sufficient security and encryption on your wireless network.

If WPA2 is supported by your wireless clients it is recommended to apply WPA2 encryption to your wireless network as it offers the highest level of security.

Depending on your choice of security method, the Wireless Encryption page will refresh with relevant configuration choices.

Available choices are:

- None/No encryption: this option is not recommended except during installation of your network.
- WPA: Wi-Fi Protected Access is a 256-bit encryption method with keys that change automatically over time.
- WPA2: a more secure version of WPA with implementation of the 802.11i standard.
- WPA and WPA2: allows both options
- 802.1X WEP: Wireless Equivalent Privacy is a 40-bit or 104-bit encryption method with user configurable fixed keys. 802.1X indicates RADIUS support.
- WEP/Non-802.1X WEP: like 802.1X WEP but without RADIUS support.
- Authentication Only: authentication by physical MAC address.

Configuring WEP: select the desired level (104-bit provides higher security). Enter the Pre-Shared key in hexadecimal (10 or 26 characters), or in plain text (ASCII) format (5 or 13 characters).

If you choose WEP encryption you will be asked to enter an encryption key in either HEX or ASCII format. HEX format requires a hexadecimal key (0-9, a-f) of various length depending on your selection. An ASCII key consists of text as a pass-phrase that will be translated internally by the GlobeSurfer® III+ into a HEX key. Using an ASCII key may be easier to remember than a HEX key, but in some cases there are compatibility issues between different vendors of wireless equipment. Hence, if you are experiencing problems when using an ASCII key try to use HEX keys instead.

ASCII: For best compatibility limit your pass phrase to a mixture of English 26-character alphabet (a-z, A-Z), the numbers (0-9) and simple punctuation (. - <space>).

OPTION

GlobeSurfer III+

Welcome **admin** | Go to Basic Mode | Site Map | Reboot | Logout | EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Map View **Installation Wizard** Quick Setup

Home

Installation Wizard: Wireless encryption

Configure the encryption of the GlobeSurfer III wireless network.

Add encryption to your wireless network to prevent unauthorised traffic monitoring and access:

- No encryption: this option is not recommended except during installation of your network.
- WPA: Wi-Fi Protected Access is a 256-bit encryption method with keys that change automatically over time.
- WPA2: A more secure version of WPA with implementation of the 802.11i standard.
- 802.1X WEP: Wireless Equivalent Privacy is a 40-bit or 104-bit encryption method with user configurable fixed keys. 802.1X indicates RADIUS support.
- Non-802.1X WEP: Like 802.1X WEP but without RADIUS support.
- Authentication only: Authentication by physical MAC address

Note: WPA/WPA2 is recommended as it provides the higher level of security due to the longer key that changes automatically. You must configure your wireless PC clients to use the same encryption type and keys. Otherwise the devices will not understand each other. Enabling wireless encryption has no security effect on wired (Ethernet) connections.

Configuring WEP: Select the desired level (104-bit provides higher security). Enter the Pre-Shared key in hexadecimal (10 or 26 characters), or in plain text (ASCII) format (5 or 13 characters).

Configuring WPA/WPA2: Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters. Note: Not all wireless client equipment supports ASCII-text format. If you are experiencing problems, use the hexadecimal key format since most vendors support it.

Wizard Progress

- Installation Wizard: Language
- Installation Wizard: Telephony
- Installation Wizard: UMTS
- Installation Wizard: Wireless
- ▶ Installation Wizard: Wireless encryption
- Installation Wizard: Firewall policy
- Installation Completed

Security

Security:

Configuring WPA/WPA2: enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.

WPA/WPA2 is strongly recommended as it provides a significantly higher level of security compared to WEP. If possible configure all devices to use WPA2.

You must configure your wireless PC clients to use the same encryption type and keys; otherwise the devices will not understand each other.

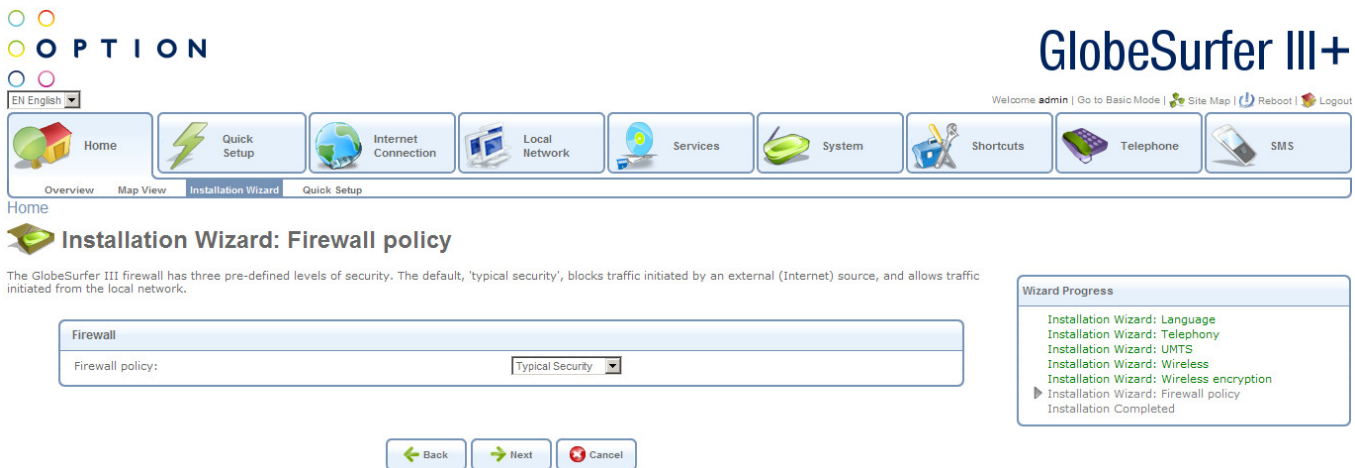
Enabling wireless encryption has no security effect on wired (Ethernet) connections.

3.4.3.6 Installation Wizard: Firewall Policy

The GlobeSurfer® III+ has three different predefined Firewall Policies:

- Minimum Security: lowest level of firewall security allowing both incoming and outgoing traffic.
- Typical Security: offers some firewall security, but is still open for all connections initiated from local clients connected to the GlobeSurfer® III+.
- Maximum Security: highest level of firewall security where only the most commonly used protocols are allowed for local clients trying to connect to the Internet.

It is also possible to add more advanced firewall policies than these three predefined levels.



3.4.3.7 Install Wizard: Finish

The last page of the Installation Wizard shows all the settings made on previous pages. If they all look correct, press the Finish button to apply these settings.

If you want to change any settings, use the Back button to navigate to the appropriate page and modify that setting.

Press the Exit button if you want to quit the Installation Wizard without applying any new changes.



3.5 Quick Setup



GlobeSurfer III+

Welcome **admin** | Goto Basic Mode | Site Map | Reboot | Logout | EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Quick Setup

Language and region settings

Language: EN English
Time Zone: GMT (GMT+00:00)

Telephony

Caller ID: ETSI DTMF

UMTS

Access point name: Internet
UMTS connect method: ☒ Connect, Manually ☐ Automatically connect upon traffic ☐ Always connected
In case of inactivity, disconnect after (minutes): 0

Wireless

Wireless: ☒ Enabled
SSID: GlobeSurferIII+
SSID Broadcast: ☒ Enabled

Security

Security: WPA and WPA2
Authentication Method: Pre-Shared Key
Pre-Shared Key: the quick brown fox
Encryption Algorithm: AES
☐ Group Key Update Interval
☐ Inter Client Privacy
0 Seconds

Firewall

Firewall policy: Typical Security

OK Apply Cancel Installation Wizard

You can use the Quick Setup screen to change the main settings needed to use GlobeSurfer® III+:

3.5.1.1.1 Web interface and display

Language: select the language for GlobeSurfer® III+. The current language setting will be restored if you do not apply the settings.

3.5.1.1.2 Telephony

Caller ID: select the country for the telephone handset interface, options available are:

- ETSI DTMF
- ETSI FSK ring pulse
- ETSI FSK dualtone
- ETSI FSK Line reversal + dualtone
- ETSI FSK during ring
- Bellcore

- Australia

3.5.1.1.3 UMTS

Access point name: as provided by your mobile operator

UMTS connect method: radio button with the following choices:

- Connect Manually: connect to the Internet by clicking Connect on the Connection Status page in the management console or press the Connect button on GlobeSurfer® III+
- Automatically connect upon traffic: GlobeSurfer® III+ will automatically connect when you attempt to send data via the Internet
- Always connected: GlobeSurfer® III+ will stay connected

In case of inactivity, disconnect after (minutes): The default is 10 minutes. Set it to zero (0) if you want the UMTS to stay connected. The maximum is 1440 minutes (24 hours). Incoming traffic is treated as inactivity.

3.5.1.1.4 Wireless

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

- Wireless: click on the Enabled checkbox to enable this function
- SSID: the Service Set Identifier – enter a name for your local wireless network (WLAN)
- SSID Broadcast

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.5.1.1.5 Security

Enable good security selecting by selecting “WPA2” or “WPA and WPA2”. If you select “WPA2” then only devices supporting WPA2 can connect to your GlobeSurfer® III+ and you will have the best WiFi security. Choose a good and easy to remember pre-shared key (passphrase), anything over 8 characters is strong.

3.5.1.1.6 Firewall

Select the level of protection you need. “Typical Security” is sufficient for most circumstances.

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.6 Internet Connection

The WAN Cellular interface connects GlobeSurfer® III+ to the Internet and other networks through GSM or UMTS mobile telecommunications standards. The WAN Cellular Properties screen displays a summary of the connection.

From this screen you can click on the tabs at the top left hand side to route to the following detailed screens:

- General - summary of wireless connection
- Settings - general communications parameters
- Routing - sets static or dynamic routing options
- Advanced - activate firewall for network connection

3.6.1 General

The WAN Cellular connection connects the GlobeSurfer® III+ to the Internet and other networks through the GSM and UMTS mobile telecommunications standards. The WAN Cellular Properties screen displays a summary of the connection properties.

OPTION

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

WAN Cellular Properties

General Settings Routing Advanced

Name:	WAN Cellular	Disconnect
Device Name:	eth1	
Status:	Status working	
Network:	WAN	
Connection Type:	Cellular	
IP Address:	10.35.48.209	
Subnet Mask:	255.255.255.0	
DNS Server:	149.254.192.126	
	149.254.201.126	
Access point name:	general.t-mobile.uk	
Operator:	T-Mobile	
Signal strength:	Low (-93 dBm)	
Connection status:	Connected	
Received bytes:	29.8 [MB]	
Sent bytes:	6.7 [MB]	
Total connection time:	38:39:04 [hh:mm:ss]	
Current connection time:	38:38:33 [hh:mm:ss]	

OK Apply Cancel

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.6.2 Settings

The top part of the configuration window displays general communication parameters. It is not recommended to change the default values in this screen unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

OPTION

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

WAN Cellular Properties

General Settings Routing Advanced

Device Name: eth1
 Status: Status working
 Schedule: Always
 Network: WAN
 Connection Type: Cellular
 MTU: Automatic 1500

Internet Protocol
☐ Override Subnet Mask

DNS Server Obtain DNS Server Address Automatically

UMTS

Access point name: general1-mobile.uk
 Network Authentication: None
 Login User Name (case sensitive):
 Login Password:
 Network type: Automatic
 UMTS connect method:
☒ Connect Manually
☐ Automatically connect upon traffic
☐ Always connected

You can configure the following general connection settings:

MTU: this is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Manual, allows you to enter the largest packet size that will be transmitted. The recommended size is 1500. You should leave this value in the 1200 to 1500 range. To have the gateway select the best MTU for your Internet connection, select Automatic (default setting).

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.6.3 Routing

You can choose to setup your gateway 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.

OPTION

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

WAN Cellular Properties

General Settings **Routing** Advanced

Routing Mode:

Device Metric:

☒ Default Route

☐ Multicast - IGMP Proxy Default

☐ Routing Information Protocol (RIP)

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

OK Apply Cancel

You can configure the following routing settings:

Routing Mode: select one of the following routing modes:

Route: use route mode if you want your GlobeSurfer® III+ to function as a router between two networks. In this mode GlobeSurfer® III+ passes packets between the networks transparently.

NAPT (default): Network Address and Port Translation (NAPT) refers to network address translation (NAT) 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: this is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route: select this checkbox to define this device as the default route out of the local network.

Multicast - IGMP Proxy Default: 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 checkbox to enable this feature.

Routing Information Protocol (RIP): select this checkbox to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination.

Routing Table: allows you to add or modify routes when this device is active. Use the New Route button to add a route or edit existing routes.

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.6.4 Connection Watchdog

When this feature is enabled and the Watchdog timeout duration is set, the GlobeSurfer will do periodic DNS queries to the DNS server to resolve pre-defined websites e.g. www.option.com, www.google.com, www.microsoft.com. If the DNS query does not get resolved, the device will force a reset of the WWAN modem and will try to re-establish the connection.

The screenshot shows the GlobeSurfer III+ web interface. The top navigation bar includes icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. The secondary navigation bar has tabs for Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The 'Settings' tab is selected, and the 'System Settings' page is displayed. The System Settings page contains four sections: Host Information, Installation Wizard, Data Counter, and 3G Connection Watchdog. The 3G Connection Watchdog section is expanded, showing the 'Enabled' checkbox checked and the 'Watchdog timeout' set to 60 seconds. At the bottom of the page are three buttons: OK, Apply, and Cancel.

To enable the Connection Watchdog feature, check the 3G Connection watchdog checkbox and set the frequency of the DNS query by setting the Watchdog timeout duration. A duration of 60 seconds is suggested for this setting.

If the device is already set in Failover mode, this feature will automatically be deactivated.

3.6.5 SMS Control

The GlobeSurfer can be set to receive SMS commands from pre-defined phone numbers to execute certain tasks.

To enable the SMS Control feature, check the SMS Control Center checkbox and define a valid phone number. The phone number has to be in international format with the country prefix preceded by a '+'. e.g. +32475123456 for Belgium where 32 is the country prefix of Belgium.

Multiple phone numbers can be defined for this feature. The phone numbers have to be separated by a comma ','.

SMS commands

SMS commands have to be in simple US characters with no space or other characters before or after the command itself.

REBOOT

The GlobeSurfer will do a power reboot.

CONNECT

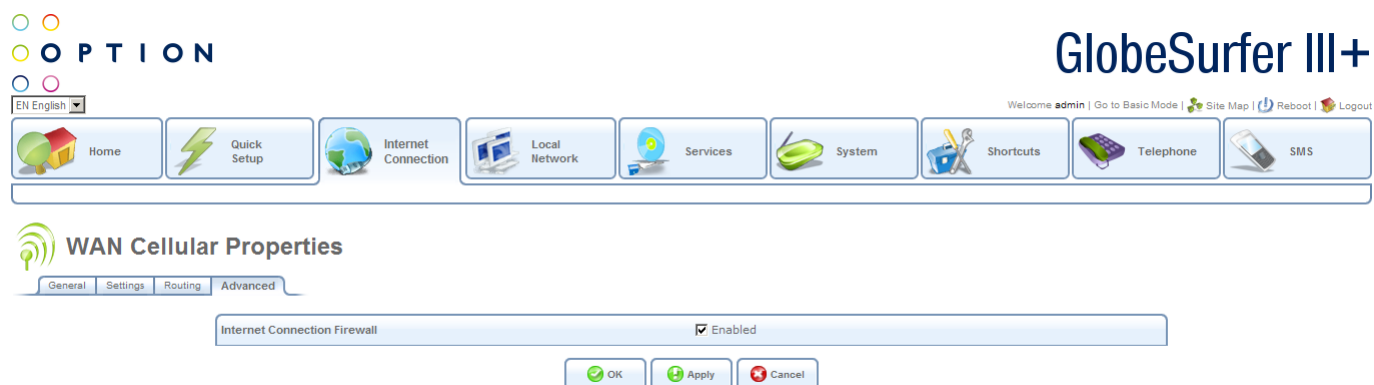
If the device is set at 'Manual Connect' or 'Connect Upon Traffic' and the connection is off, this command will make a connection and change the connection state to 'Connected'.

DISCONNECT

If the device is set at 'Manual Connect' or 'Connect Upon Traffic' and the connection is on, this command will make a disconnection and change the connection state to 'Disconnect'.

3.6.6 Advanced

Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection.



To enable the firewall on this network connection, select the Enabled checkbox.

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.7 Local Network

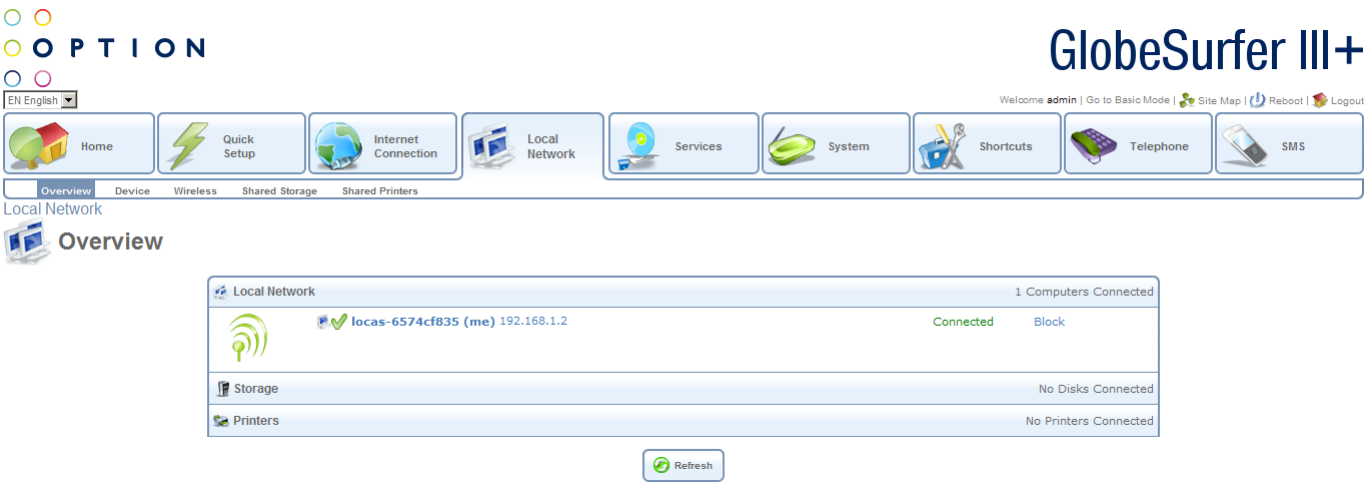
This area provides an overview of and the ability to configure local network, storage and printer settings.

From this screen you can click on the tabs at the top left hand side to route to the following detailed screens:

- Overview - overview of local network, storage and printers
- Device - list of all devices in local network with ability to drill down to see detail
- Wireless - overview of wireless network with ability to drill down to see detail
- Shared Storage - manage your system storage area, disks and RAID devices
- Shared Printers - shows printers attached to the device via the USB connection

3.7.1 Overview

This screen displays an overview of the local network, storage and printers, and provides access to further screens where individual devices, wireless network, shared printers and shared storage can be configured and modified.



The following data is displayed:

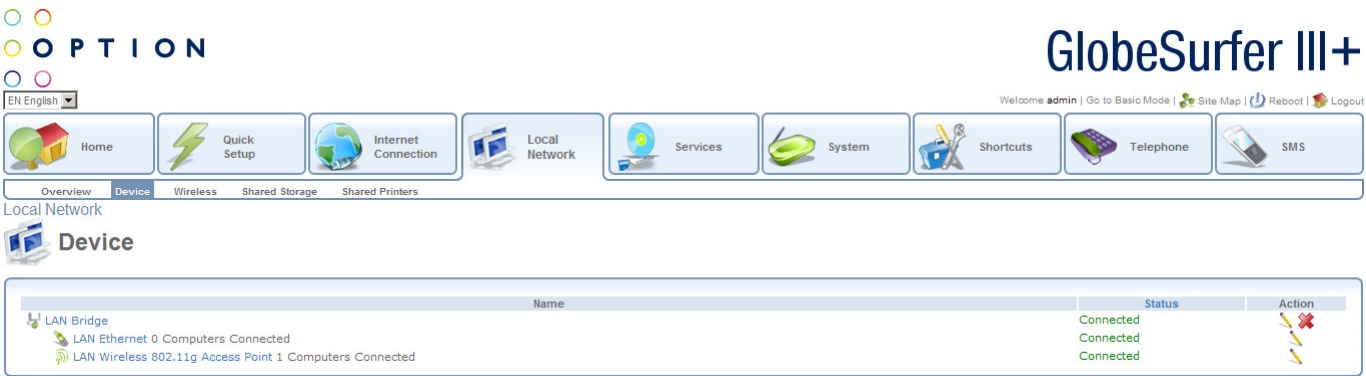
Local Network: the number of computers connected is shown. For each computer the following data appears:

- Type
- Name
- IP address
- Status
- Block status
- Storage: the number of external hard disk drives connected is shown
- Printers: the number of printers connected is shown

Press the Refresh button to refresh the screen.

3.7.2 Device

This screen displays a list of all the devices in the local network along with their status, and provides the ability to modify and delete each entry.



For each device the following data is displayed:

- Name

- Number of computers connected
- Status

Clicking on a LAN Bridge entry routes you to the LAN Bridge Properties screen in the System/Network Connections/General part of the system

Clicking on a LAN Ethernet entry routes you to the LAN Ethernet Properties screen in the System/Network Connections/General part of the system

Clicking on a LAN Wireless 802.11g Access Point entry routes you to the LAN Wireless 802.11g Access Point Properties screen in the System/Network Connections/General part of the system

3.7.3 Wireless

From this screen you can click on the tabs at the top right hand side to route to the detailed screens.

3.7.3.1 General (Wireless)

This screen provides a summary view of the wireless network.

The screenshot shows the 'LAN Wireless 802.11g Access Point Properties' window with the 'General' tab selected. The window has a title bar with 'Local Network' and a 'GlobeSurfer III+' logo. Below the title bar is a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. The main content area displays the following information:

Name:	LAN Wireless 802.11g Access Point
Device Name:	eth0
Status:	Connected
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Download Rate:	54 Mbps
Upload Rate:	54 Mbps
MAC Address:	00:0c:e3:65:fd:77
IP Address Distribution:	Disabled
Encryption:	Disabled
Received bytes:	0.0 [MB]
Sent bytes:	0.0 [MB]
Total connection time:	4:34:04 [hh:mm:ss]
Current connection time:	4:21:02 [hh:mm:ss]

At the bottom of the window are three buttons: OK, Apply, and Cancel.

3.7.3.2 Settings (Wireless)

OPTION

EN English

Home

Quick Setup

Internet Connection

Local Network

Services

System

Shortcuts

Telephone

SMS

Overview | Device | **Wireless** | Shared Storage | Shared Printers

Wireless

LAN Wireless 802.11g Access Point Properties

Overview | Settings | **Advanced**

General | Settings | **Wireless** | Advanced

Device Name:eth0

Status:Connected

Schedule:Always

Network:LAN

Connection Type:Wireless 802.11g Access Point

Physical Address:00:0c:e3:65:f6:ab

MTU:Automatic1500

OK

Apply

Cancel

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.7.3.3 Wireless (Wireless)

OPTION

EN English

Home

Quick Setup

Internet Connection

Local Network

Services

System

Shortcuts

Telephone

SMS

Overview | Device | **Wireless** | Shared Storage | Shared Printers

Wireless

LAN Wireless 802.11g Access Point Properties

Overview | Settings | **Advanced**

General | Settings | **Wireless** | Advanced

Wireless Network (SSID):SSIDDeborah

☒ SSID Broadcast

802.11 Mode:802.11b/g Mixed

Channel:Automatic(FCC)

Network Authentication:Open System Authentication

MAC Filtering Mode:Disable

MAC Filtering Table

New MAC Address	MAC Address	Action

Security

Authentication Method:Web Authentication

Clean Mac List

Wireless QoS (WMM)

☐ Enabled

Transmission Rate:Auto

CTS Protection Mode:None

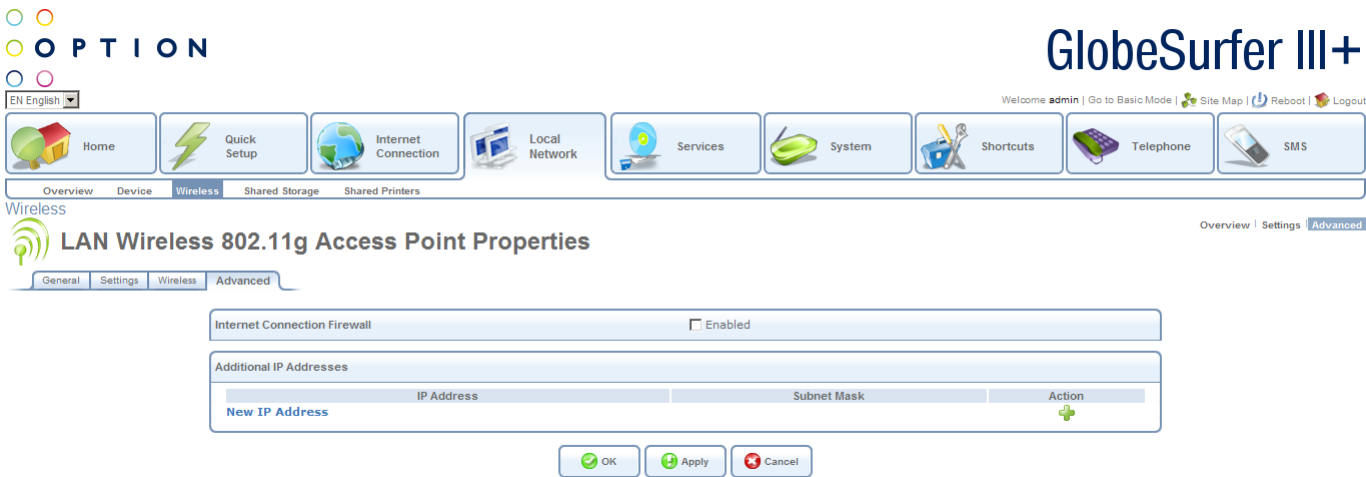
CTS Protection Type:cts-only

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

3.7.3.4 Advanced (Wireless)



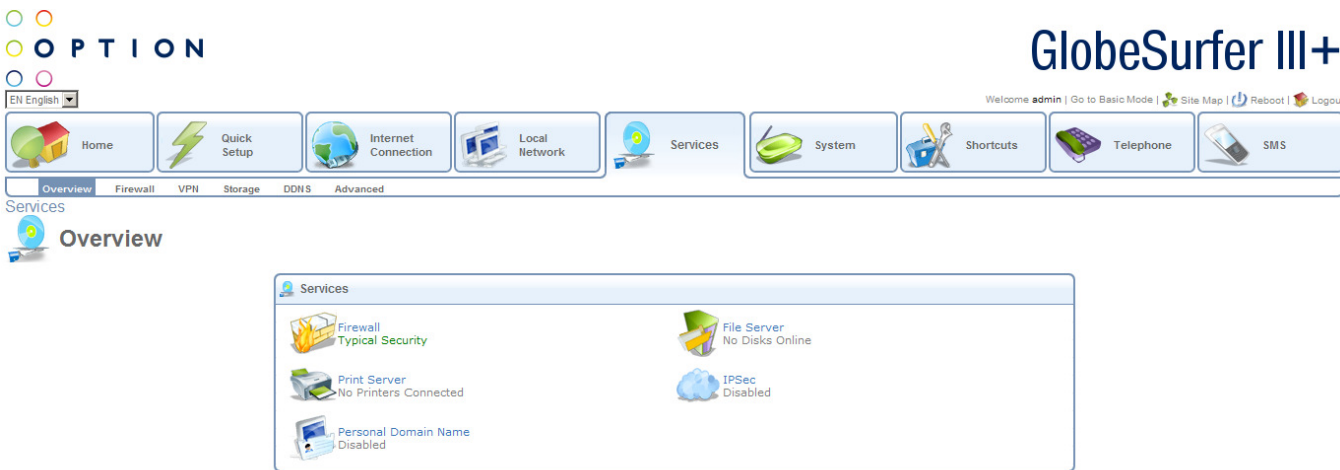
Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

4 Services

4.1 Overview



This screen displays icons/hyperlinks for the various services available:

- Firewall : this hyperlink routes to the Firewall Overview screen
- File Server : this hyperlink routes to the File Server Overview screen
- Print Server : this hyperlink routes to the Print Server Overview screen
- IPSec : this hyperlink routes to the IPSec Overview screen

- Personal Domain Name : this hyperlink routes to the Personal Domain Name Overview screen

Each service also shows a summary description of the status of the service.

4.2 Firewall

The GlobeSurfer® III+ 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 to be protected from the security threats of the Internet.

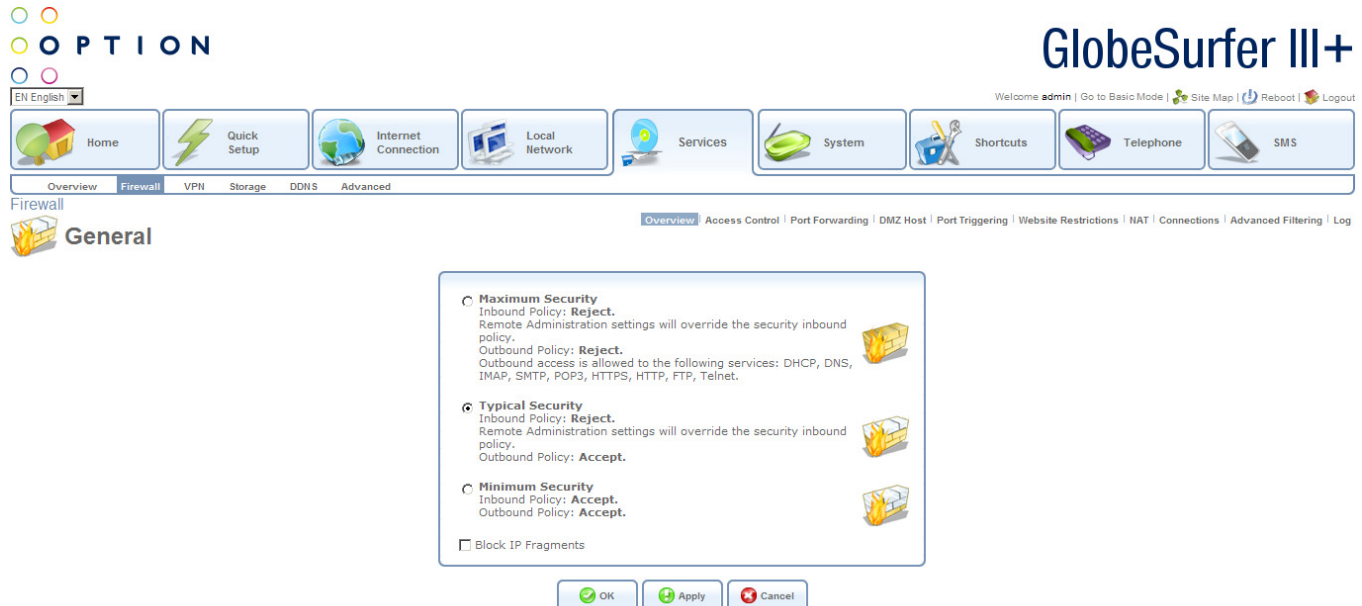
The firewall, the cornerstone of the GlobeSurfer® III+'s security services, has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security.

The GlobeSurfer® III+'s 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 videoconferencing.

The GlobeSurfer® III+'s 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 Overview screen allows you to quickly choose the security level for the firewall.
- The Access Control screen can be used to restrict access from the local network to the Internet.
- The Port Forwarding screen can be used to enable access from the Internet to specified services provided by computers in the local network and special Internet applications.
- The DMZ Host screen allows you to configure a LAN host to receive all traffic arriving at your GlobeSurfer® III+, which does not belong to a known session.
- The Port Triggering screen allows you to define port triggering entries, to dynamically open the firewall for some protocols or ports.
- The Website Restrictions screen allows you to block LAN access to a certain host or Web site on the Internet.
- The NAT (Network Address Translation) screen allows you to hide the computers in your network so they cannot be found or directly accessed from outside your network.
- The Connections screen allows you to view all the active connections on the system.
- The Advanced Filtering screen allows you to implicitly control the firewall setting and rules.
- The Log screen allows you to view and configure the firewall Log.

4.2.1 Overview



Use the Overview screen to quickly configure the gateway's basic security settings.

The firewall regulates the flow of data between the home network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through GlobeSurfer® III+) or rejected (barred from passing through GlobeSurfer® III+) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing home 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 home network and what types of services available in the home 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 home 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® III+ the firewall will identify the request type and origin, HTTP and a specific PC in your home 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. 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 home 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® III+: Minimum, Typical and Maximum. The table below summarizes the behavior of GlobeSurfer® III+ 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	Blocked: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	Limited: By default, only commonly-used services, such as Web browsing and e-mail, are permitted *
Typical Security	Blocked: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	Blocked: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens
Minimum Security	Unrestricted: Permits full access from Internet to home network; all connection attempts permitted.	Blocked: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens

* These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP₃ and SMTP. The list of allowed services at 'Maximum Security' mode can be edited in the Access Control page. 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 behavior, these applications will not be blocked outbound, even at Maximum Security Level.

Choose from the among the three pre-defined security levels described in the table above:

- **Maximum Security:** if this option is chosen, remote administration settings will override the security inbound policy and outbound access is allowed to the following services: DHCP, DNS, IMAP, POP₃, HTTPS, FTP and Telnet.
- **Typical Security:** this is the default option where remote administration settings will override the security inbound policy.

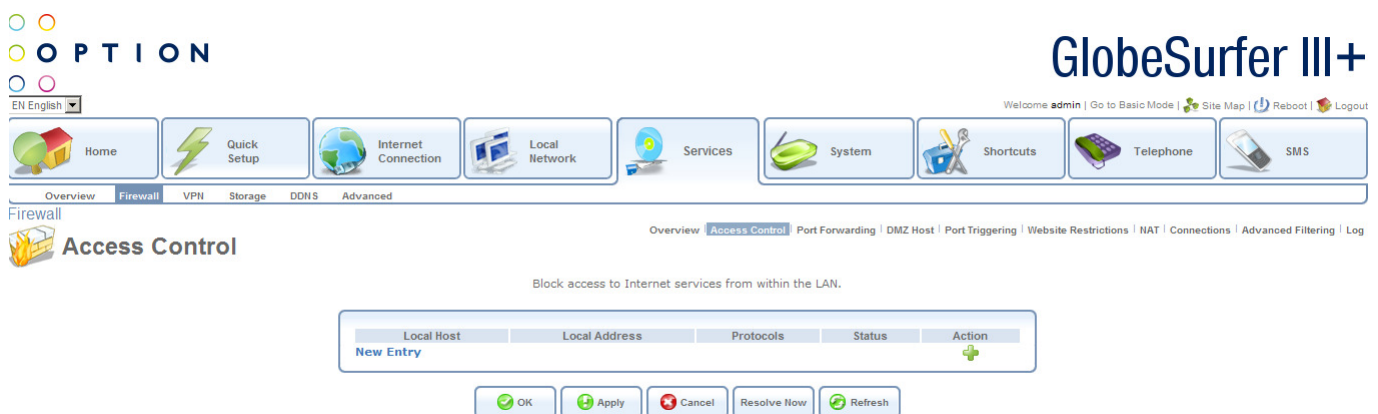
- Minimum security: this setting should not be used except for short periods of time under as it provides little protection from outside attack.
- Fragments: click this checkbox in order to protect your home network from a common type of hacker attack that could make use of fragmented data packets to sabotage your home 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 home network in order to make use of these select services.)

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

4.2.2 Access Control



You may want to block specific computers within the home 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 home network out to the Internet, and thus may block traffic flowing in both directions. It can also be used for allowing specific services when maximum security is configured. In the e-mail example given above, you may prevent computers in the home network from receiving e-mail by blocking their outgoing requests to POP3 servers on the Internet.

There are numerous services you should consider blocking, such as popular game and file sharing servers. For example, if you want to make sure that your employees do not put your business at risk from illegally traded copyright files, you may want to block several popular P2P and file sharing applications.

This screen offers the facility to block access to Internet services from within the LAN. Entries can be added, edited or deleted.

The following fields are displayed:

- Local Host: identifier
- Local Address: computer to apply the access control rule to
- Protocols: type of protocol
- Status: shows the status of the access control rule

Action: options for adding new entries or editing or deleting existing ones

Click on New Entry - this routes to the Add Access Control Rule screen

Click on the edit icon - this routes to the Edit Access Control Rule screen

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

Press the Resolve Now button to check the screen.

Press the Refresh button to refresh the screen.

4.2.2.1 Add Access Control Rule

The screenshot displays the 'Add Access Control Rule' configuration page in the GlobeSurfer III+ web interface. The top navigation bar includes icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. The sub-navigation bar shows tabs for Overview, Firewall, VPN, Storage, DDNS, and Advanced, with 'Firewall' being the active tab. The 'Access Control' sub-tab is selected. The main form contains the following fields:

- Address:** A dropdown menu currently set to 'Any'.
- Protocol:** A dropdown menu currently set to 'Any'.
- Reply an HTML Page to the Blocked Client:** A checkbox that is checked.
- Schedule:** A dropdown menu currently set to 'Always'.

At the bottom of the form are two buttons: 'OK' (with a green checkmark icon) and 'Cancel' (with a red X icon).

This screen allows the entry of new access control rules. The following fields should be entered:

Address: specify the computer or group of computers to apply the access control rule to: options available are:

- Any
- User Defined – this routes to the Edit Network Object screen
- Specific computer address in your LAN

Protocol: type of protocol that will be used: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Service

Show Basic Services – if this option is chosen a reduced list of options is displayed including:

- FTP - File Transfer
- HTTP – Web Server
- HTTPS – Secured Web Server
- IMAP – Messaging Server
- L2TP – Layer 2 Tunneling Protocol
- Ping – ICMP Echo Request
- POP3 – Incoming Mail
- SMTP – Outgoing Mail
- SNMP – Simple Network Management Protocol
- Telnet – Remote Connection
- TFTP – Trivial File Transfer Protocol
- Traceroute – Route Tracking Utility
- Show All Services – a more comprehensive list of services is displayed
- Reply an HTML Page to the Blocked Client: click this checkbox to send an HTML page to the client when access is blocked – this is checked by default
- Schedule: define the time period during which this rule will take effect:
 - Always – access is always controlled
 - User defined – this routes to the Edit Scheduler Rule screen

Press the OK button to apply changes and go back to the Access Control screen.

Press the Cancel button to reject changes and go back to the Access Control screen.

4.2.2.2 Edit Access Control Rule

This screen allows the editing of existing access control rules. The following fields should be entered:

Address: specify the computer or group of computers to apply the access control rule to: options available are:

- Any
- User Defined – this routes to the Edit Network Object screen
- Specific computer address in your LAN

Protocol: type of protocol that will be used: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Service screen
- Show Basic Services – if this option is chosen a reduced list of options is displayed including:
 - FTP - File Transfer
 - HTTP – Web Server
 - HTTPS – Secured Web Server
 - IMAP – Messaging Server
 - L2TP – Layer 2 Tunneling Protocol
 - Ping – ICMP Echo Request
 - POP3 – Incoming Mail
 - SMTP – Outgoing Mail
 - SNMP – Simple Network Management Protocol
 - Telnet – Remote Connection
 - TFTP – Trivial File Transfer Protocol
 - Traceroute – Route Tracking Utility
- Show All Services – a more comprehensive list of services is displayed

- Reply an HTML Page to the Blocked Client: click this checkbox to send an HTML page to the client when access is blocked – this is checked by default
- Schedule: define the time period during which this rule will take effect:
- Always – access is always controlled
- User defined – this routes to the Edit Scheduler Rule screen

Press the OK button to apply changes and go back to the Access Control screen.

Press the Cancel button to reject changes and go back to the Access Control screen.

4.2.2.3 Edit Network Object

OPTION

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall

Overview Access Control Port Forwarding DMZ Host Port Triggering Website Restrictions NAT Connections Advanced Filtering Log

Edit Network Object

Network Object

Description: Network Object

Items

Item	Action
New Entry	+

OK Cancel

This screen allows the editing of network objects. The following fields should be entered:

- Description: type the description of the object

Click on New Entry - this routes to the Edit Item screen

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.2.4 Edit Item

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall

Overview Access Control Port Forwarding DMZ Host Port Triggering Website Restrictions NAT Connections Advanced Filtering Log

Edit Item

Network Object Type: IP Address

IP Address: 0 0 0 0

OK Cancel

This screen allows the editing of network object types. The following fields should be entered:

Network Object Type: choose from the drop down list:

- IP Address, then enter
- IP address
- IP Subnet, then enter
- Subnet IP Address
- Subnet Mask
- IP Range, then enter
- From IP Address
- To IP Address
- MAC Address, then enter
- MAC Address
- MAC Mask
- Host Name, then enter
- Host Name

DHCP Option, then choose from the drop down list:

- Vendor Class ID
- Client ID
- User Class ID

Then enter the appropriate ID.

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.2.5 Edit Service

Service Name:

Protocol	Server Ports	Action
New Server Ports		+

OK Cancel

This screen allows the editing of services. The following fields should be entered:

- Service Name: type the name of the service

Click on New Server Ports - this routes to the Edit Service Server Ports screen

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.2.6 Edit Service Server Ports

Protocol:

Protocol Number:

OK Cancel

This screen allows the editing of service server ports. The following fields should be entered:

Protocol: choose from the drop down list:

- TCP, then enter
- Source Ports, then choose from the drop down list:

- Any
- Single, then enter port number
- Range, then enter range values

Destination Ports, then choose from the drop down list:

- Any
- Single, then enter port number
- Range, then enter range values
- UDP,

then enter Source Ports then choose from the drop down list:

- Any
- Single, then enter port number
- Range, then enter range values

Destination Ports, then choose from the drop down list:

- Any
- Single, then enter port number
- Range, then enter range values
- ICMP, then enter

ICMP Message by choosing from the drop down list:

- Echo Reply
- Network Unreachable
- Host Unreachable
- Protocol Unreachable
- Port Unreachable
- Destination Network Unknown
- Destination Host Unknown
- Redirect for Network
- Redirect for Host
- Echo Request
- Other
- GRE
- ESP
- AH
- Other, then enter
- Protocol Number

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.2.7 Edit Scheduler Rule

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall

Overview Access Control Port Forwarding DMZ Host Port Triggering Website Restrictions NAT Connections Advanced Filtering Log

Edit Scheduler Rule

Name: Scheduler Rule

Rule Activity Settings

☒ Rule will be Active at the Scheduled Time

☐ Rule will be Inactive at the Scheduled Time

Time Segments	Action
New Time Segment Entry	+

OK Cancel

This screen allows the editing of scheduler rules. The following fields should be entered:

Name: type the name of the scheduler rule and click on New Time Segment Entry

Rule Activity settings: choose from the following radio buttons

Rule will be Active at the Scheduled Time

Rule will be Inactive at the Scheduled Time

Click on New Time Segment Entry - this routes to the Edit Time Segment screen

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.2.8 Edit Time Segment

OPTION

GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DNS Advanced

Firewall Edit Time Segment

Overview Access Control Port Forwarding DMZ Host Port Triggering Website Restrictions NAT Connections Advanced Filtering Log

Days of Week

☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday
☐ Sunday

Hours Range

Start Time	End Time	Action
New Hours Range Entry		

OK Cancel

This screen allows the editing of time segments. The following fields should be entered:

- Days of Week: check the days of the week when the rule should apply

Click on New Hours Range Entry - this routes to the Edit Hour Range screen

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.2.9 Edit Hour Range

OPTION

GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DNS Advanced

Firewall Edit Hour Range

Overview Access Control Port Forwarding DMZ Host Port Triggering Website Restrictions NAT Connections Advanced Filtering Log

Start Time: 00 : 00

End Time: 00 : 00

OK Cancel

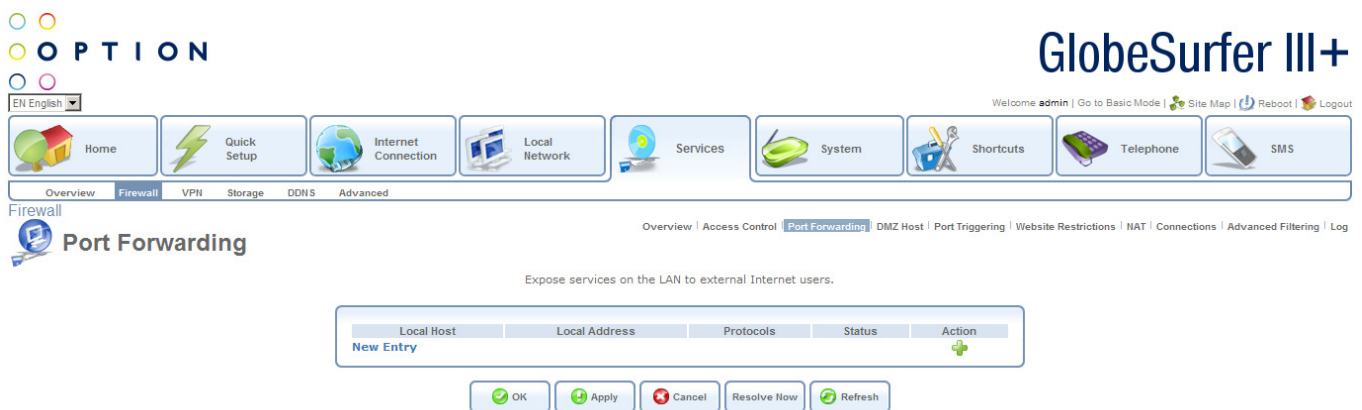
This screen allows the entry of the hours during the day when the rules will apply. The following fields should be entered:

- Start Time in hours and minutes
- End Time in hours and minutes

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.3 Port Forwarding



In its default state, GlobeSurfer® III+ 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 home network. The Port Forwarding feature supports both of these functionalities. If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as “Local Servers”.

The Port Forwarding screen lets you define the applications that require special handling by GlobeSurfer® III+. All you have to do is select the application's protocol and the local IP address of the computer that will be using or providing the service. If required, you may add new protocols in addition to the most common ones provided by GlobeSurfer® III+.

For example, if you wanted to use a File Transfer Protocol (FTP) application on one of your PCs, you would simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at GlobeSurfer® III+ from the Internet will henceforth be forwarded to the specified computer.

Similarly, if you want to grant Internet users access to servers inside your home 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 home network you must select HTTP from the list of protocols and enter the local IP address or host name of the computer that will host the Web server. When an Internet user

points her browser to the external IP address of GlobeSurfer® III+, the gateway will forward the incoming HTTP request to the computer that is hosting the Web server.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. Let's 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® III+ via HTTP. To accomplish this, do the following:

- Define a port forwarding rule for the HTTP service, with the PC's IP or host name.
- Specify 8080 in the 'Forward to Port' field.

All incoming HTTP traffic will now be forwarded to the PC running the Web server on port 8080. When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP - the port used by the gateway's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

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 home 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® III+ is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network.

Note: The ALG is automatically assigned based on the destination port.

This screen offers the facility to expose services on the LAN to external Internet users. Entries can be added, edited or deleted.

The following fields are displayed:

- Local Host: identifier
- Local Address: IP address or host name of computer providing the service
- Protocols: type of protocol
- Status: shows the status of the port forwarding rule
- Action: options for adding new entries or editing or deleting existing ones

Click on New Entry - this routes to the Add Port Forwarding Rule screen

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

Press the Resolve Now button to check the screen.

Press the Refresh button to refresh the screen.

4.2.3.1 Add Port Forwarding Rule

The screenshot shows the 'Add Port Forwarding Rule' screen in the GlobeSurfer III+ web interface. The top navigation bar includes icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Firewall, VPN, Storage, DDNS, and Advanced. The 'Firewall' tab is selected, and the 'Add Port Forwarding Rule' screen is displayed. The screen has two input fields: 'Local Host' with an 'Add...' button and 'Protocol' with a dropdown menu set to 'Any'. At the bottom are 'OK', 'Cancel', and 'Advanced >>' buttons.

This screen allows the entry of new port forwarding rules. The following fields should be entered:

Local Host: 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): options available are:

- User Defined – this routes to the Edit Item screen
- A specific address
- Protocol: type of protocol: choose from the drop down list:
- Any
- User Defined – this routes to the Edit Service screen

Show Basic Services – if this option is chosen a reduced list of options is displayed including:

- FTP - File Transfer
- HTTP – Web Server
- HTTPS – Secured Web Server
- IMAP – Messaging Server
- L2TP – Layer 2 Tunneling Protocol
- Ping – ICMP Echo Request
- POP3 – Incoming Mail
- SMTP – Outgoing Mail
- SNMP – Simple Network Management Protocol
- Telnet – Remote Connection
- TFTP – Trivial File Transfer Protocol
- Traceroute – Route Tracking Utility
- Show All Services – a more comprehensive list of services is displayed

Press the OK button to apply changes and go back to the Port Forwarding screen.

Press the Cancel button to reject changes and go back to the Port Forwarding screen.

Press the Advanced button to go to the Home screen.

4.2.3.2 Edit Item

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall

Edit Item

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

Network Object Type: IP Address

IP Address: 0.0.0.0

OK Cancel

This screen allows the editing of network object types. The following fields should be entered:

Network Object Type: choose from the drop down list:

- IP Address, then enter
- IP address
- Host Name, then enter
- Host Name

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.4 DMZ Host

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall

DMZ Host

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

Allow a single LAN computer to be fully exposed to the Internet.

DMZ Host IP Address: 192.168.1.0

OK Apply Cancel

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 Port Forwarding 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 home 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 home network, such as a Web-server, is fielded by GlobeSurfer® III+. GlobeSurfer® III+ will forward this request to the DMZ host (if one is designated) unless the service is being provided by another PC in the home network (assigned in Port Forwarding), in which case that PC will receive the request instead.

This screen offers the facility to allow a single LAN computer to be fully exposed to the Internet.

The following fields should be entered:

- **DMZ Host IP Address:** click on the checkbox and 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.

You can 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, and click OK.

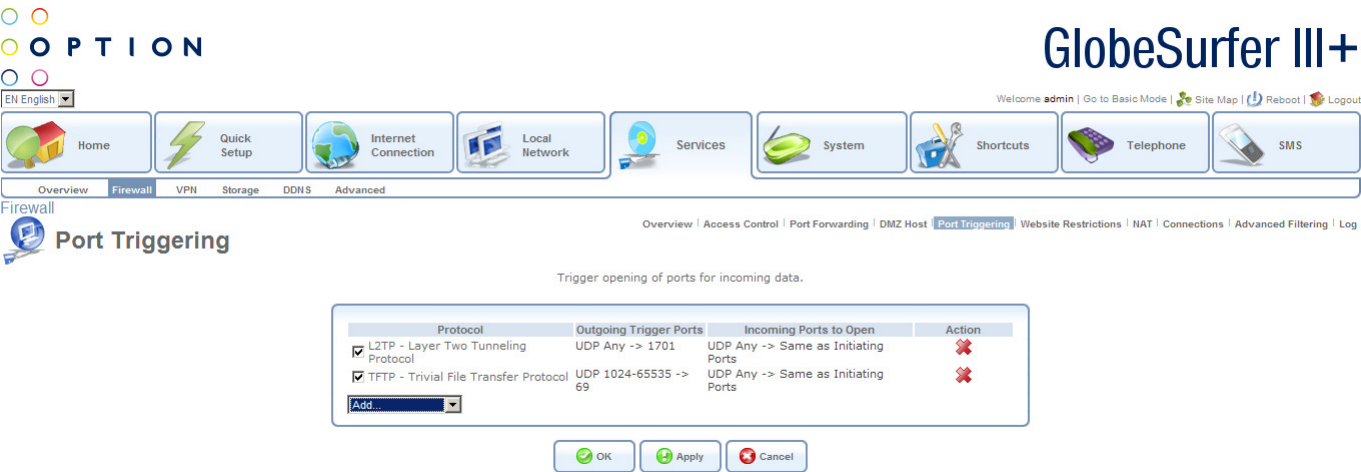
To reinstate it at a later time, simply reselect the check box.

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

4.2.5 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® III+'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.

This screen offers the facility to trigger the opening of ports for incoming data. Entries can be added, edited or deleted.

The following fields are displayed:

- Protocol: the protocol for this entry
- Outgoing Trigger Ports: shows the range of trigger ports for this protocol
- Incoming Ports to Open: shows the ports to be opened when triggered
- Action: options for adding new entries or editing or deleting existing ones

To add a trigger, choose from the drop down list:

- User Defined – this routes to the Edit Port Triggering Rule screen
- Show Basic Services – if this option is chosen a reduced list of options is displayed
- Show All Services – a more comprehensive list services is displayed including
- L2TP – Layer 2 Tunneling Protocol
- TFTP – Trivial File Transfer Protocol
- AIM Talk
- DialPad.com
- ICQ
- RealAudio on Port 7070

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

You can disable a port triggering rule without having to remove it from the Port Triggering screen.

To temporarily disable a rule, clear the check box next to the service name.

To reinstate it at a later time, simply reselect the check box.

To remove a rule, click the Remove action icon for the service. The service will be permanently removed.

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.

4.2.5.1 Edit Port Triggering Rule

Service Name:

Outgoing Trigger Ports

Protocol	Server Ports	Action
New Trigger Ports		

Incoming Ports to Open

Protocol	Opened Ports	Action
New Opened Ports		

This screen allows the editing of port triggering rules. The following fields should be entered:

- Service Name: type the name of the service

Click on New Trigger Ports - this routes to the Edit Service Server Ports screen

Click on New Opened Ports - this routes to the Edit Service Opened Ports screen

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.5.2 Edit Service Opened Ports

The screenshot shows the GlobeSurfer III+ web interface. At the top, there's a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Firewall (selected), VPN, Storage, DDNS, and Advanced. The main title 'Edit Service Opened Ports' is displayed. The form contains three dropdown menus: 'Protocol' (set to TCP), 'Source Ports' (set to Any), and 'Destination Ports' (set to Any). At the bottom, there are 'OK' and 'Cancel' buttons.

This screen allows the editing of service opened ports. The following fields should be entered:

Protocol: choose from the drop down list:

- TCP, then enter
- Source Ports, then choose from the drop down list:
- Any
- Single, then enter port number
- Range, then enter range values

Destination Ports then choose from the drop down list:

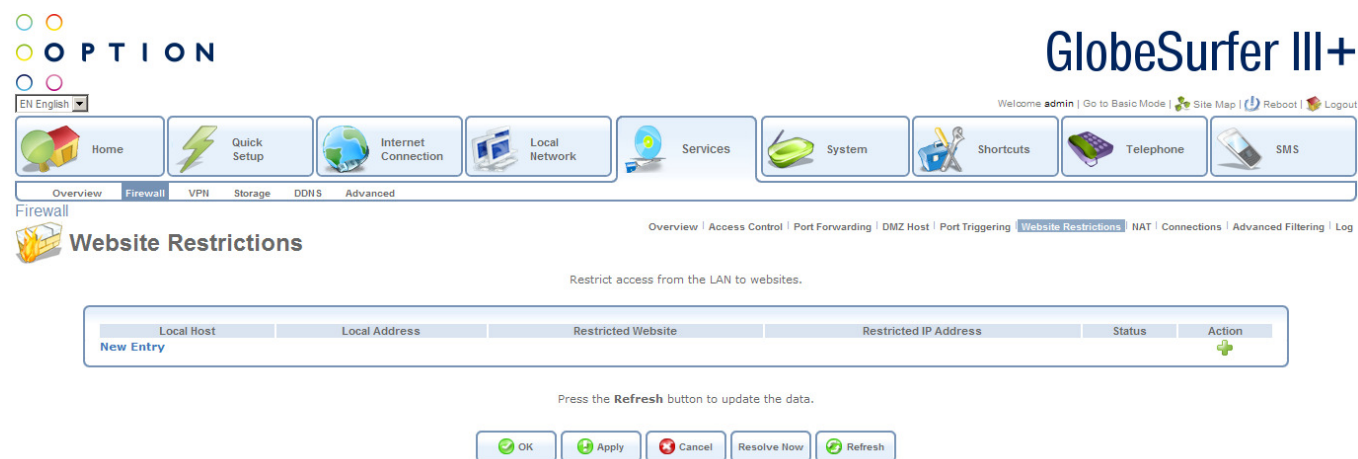
- Any
- Single, then enter port number
- Range, then enter range values
- Same as Initiating Ports
- UDP, then enter
- Source Ports, then choose from the drop down list:
- Any
- Single, then enter port number
- Range, then enter range values
- Destination Ports, then choose from the drop down list:
- Any
- Single, then enter port number
- Range, then enter range values
- Same as Initiating Ports
- ICMP, then enter
- ICMP Message by choosing from the drop down list:

- Echo Reply
- Network Unreachable
- Host Unreachable
- Protocol Unreachable
- Port Unreachable
- Destination Network Unknown
- Destination Host Unknown
- Redirect for Network
- Redirect for Host
- Echo Request
- Other
- GRE
- ESP
- AH
- Other, then enter
- Protocol Number

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.6 Website Restrictions



You may configure GlobeSurfer® III+ to block specific Internet websites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied to a comprehensive and automatically updated table of sites to which access is not recommended.

This screen offers the facility to restrict access from the LAN to websites. Entries can be added, edited or deleted.

The following fields are displayed:

- Local Host: the host for which restrictions are shown
- Local Address: shows the address for this entry
- Restricted Website: the website name to be restricted
- Restricted IP Address: the IP address to be restricted
- Status: shows the status of the website restriction
- Action: options for adding new entries or editing or deleting existing ones

Click on New Entry - this routes to the Restricted Website screen

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

Press the Resolve Now button to try to locate the site and resolve the URL into one or more IP addresses.

Press the Refresh button to refresh the screen.

You may edit the website restriction by modifying its entry under the Local Host column. To modify an entry click the Edit action icon for the restriction. Modify the website address, group or schedule as necessary.

To ensure that all current IP addresses corresponding to the restricted websites are blocked, click the Resolve Now button. GlobeSurfer® III+ will check each of the restricted website addresses and ensure that all IP addresses at which this website can be found are included in the IP addresses column.

You can disable a restriction in order to make a website available again without having to remove it from the Website Restrictions screen. This may be useful if you wish to make the website available only temporarily and expect that you will want to block it again in the future.

To temporarily disable a rule, clear the check box next to the service name.

To reinstate it at a later time, simply reselect the check box.

To remove a rule, click the Remove action icon for the service. The service will be permanently removed.

4.2.6.1 Restricted Website

Enter the website you wish to restrict:

Restricted Website:

Local Host:

Schedule:

This screen allows the entry of websites to be restricted. The following fields should be entered:

Restricted Website: enter the website address (IP address or URL) that you would like to make inaccessible from your home network (all web pages within the site will also be blocked and if the website address has multiple IP addresses, GlobeSurfer® III+ will resolve all additional addresses and automatically add them to the restrictions table)

Local Host: specify the computer or group of computers for which you would like to apply the website restriction: options available are:

- Any
- User Defined – this routes to the Edit Network Object screen
- A specific computer address in your LAN
- Schedule: choose when the website is to be restricted, by default the rule will always be active:
- Always – access is always controlled
- User defined – this routes to the Edit Scheduler Rule screen

Press the OK button to apply changes and go back to the Restricted Website screen.

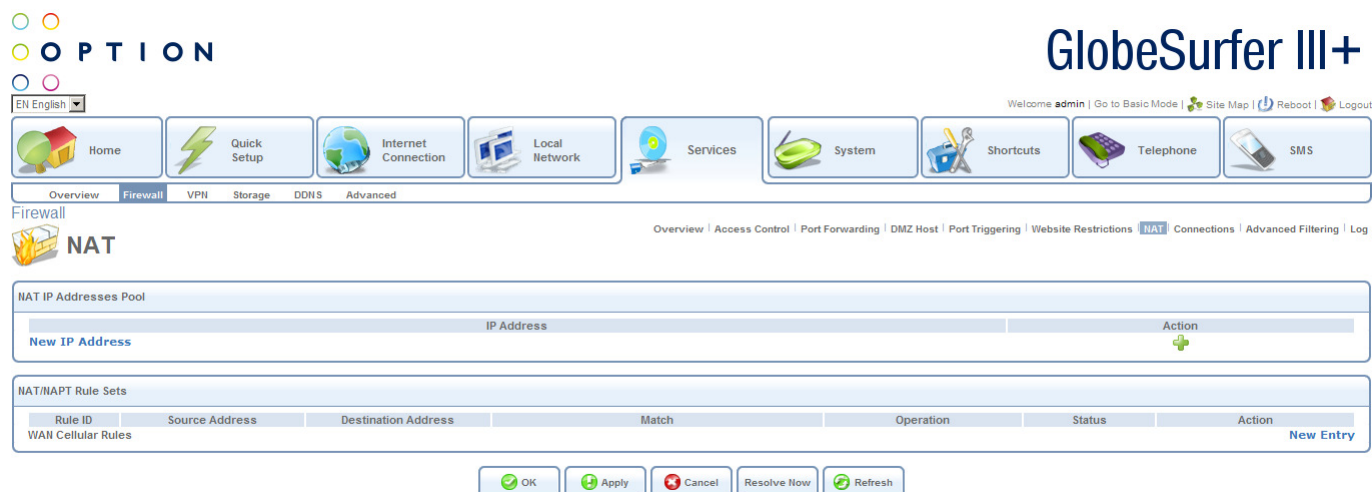
Press the Cancel button to reject changes and go back to the Restricted Website screen.

“Resolving” will appear in the Status column while the site is being located (the URL is resolved into one or more IP addresses). If the site is successfully located then “Resolved” will appear in the status bar, otherwise “Hostname Resolution Failed” will appear. In case GlobeSurfer® III+ fails to locate the website, do the following:

Use a web browser to verify that the website is available. If it is, then you probably entered the website address incorrectly.

If the website is not available, return to the “Website Restrictions” screen at a later time and click the Resolve Now button to verify that the website can be found and blocked by GlobeSurfer® III+.

4.2.7 NAT



The NAT (Network Address Translation) screen allows you to hide the computers in your network so they cannot be found or directly accessed from outside your network.

This screen offers the facility to translate network addresses. Entries can be added, edited or deleted.

The following fields are displayed:

- NAT (Network Address Translation) IP Addresses Pool
- IP address: the IP address to be translated
- Action: options for adding new entries or editing or deleting existing ones
- Click on New IP Address - this routes to the Edit Item screen
- NAT/NAPT Rule Sets
- Rule ID: the rule identifier
- Source Address: IP address of source
- Destination Address: IP address of source
- Match: the condition that must exist for the rule to apply
- Operation: protocol in use
- Status: shows the status of the rule set
- Action: options for adding new entries or editing or deleting existing ones

Click on New Entry - this routes to the Add NAT/NAPT Rule screen

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

Press the Resolve Now button to check the screen.

Press the Refresh button to refresh the screen.

4.2.7.1 Edit Item

The screenshot shows the 'Edit Item' configuration page for the Firewall section. The interface includes a top navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Firewall (selected), VPN, Storage, DDNS, and Advanced. The main content area is titled 'Edit Item' and contains a form with the following fields:

- Network Object Type:** A dropdown menu currently set to 'IP Address'.
- IP Address:** A text input field with a placeholder '0.0.0.0'.

At the bottom of the form are two buttons: 'OK' (green checkmark) and 'Cancel' (red X).

This screen allows the editing of network object types. The following fields should be entered:

Network Object Type: choose from the drop down list:

- IP Address, then enter
- IP address
- IP Subnet, then enter
- Subnet IP Address
- Subnet Mask
- IP Range, then enter
- From IP Address
- To IP Address

DHCP Option, then choose from the drop down list:

- Vendor Class ID
- Client ID
- User Class ID

then enter the appropriate ID

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

4.2.7.2 Add NAT/NAPT Rule

The screenshot shows the GlobeSurfer III+ web interface. At the top, there's a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Firewall, VPN, Storage, DDNS, and Advanced. The 'Firewall' tab is selected, and the 'Add NAT/NAPT Rule' screen is displayed. The screen is divided into several sections: 'Matching' (Source Address, Destination Address, Protocol), 'Operation' (NAT, Source IP translation rule), 'NAT Addresses' (Add...), 'Logging' (Log Packets Matched by This Rule), and 'Schedule' (Always). At the bottom, there are 'OK' and 'Cancel' buttons.

Option

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT Connections | Advanced Filtering | Log

Add NAT/NAPT Rule

Matching

Source Address Any

Destination Address Any

Protocol Any

Operation

NAT Source IP translation rule

NAT Addresses Add...

Logging

☐ Log Packets Matched by This Rule

Schedule Always

OK Cancel

This screen allows the entry of new NAT (Network Address Translation) /NAPT rules. The following fields should be entered:

Matching

Source Address: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Network Object screen
- A specific address

Destination Address: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Network Object screen
- A specific address

Protocol: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Service screen
- Show Basic Services – if this option is chosen a reduced list of options is displayed including:

- FTP - File Transfer
- HTTP – Web Server
- HTTPS – Secured Web Server
- IMAP – Messaging Server
- L2TP – Layer 2 Tunneling Protocol
- Ping – ICMP Echo Request
- POP3 – Incoming Mail
- SMTP – Outgoing Mail
- SNMP – Simple Network Management Protocol
- Telnet – Remote Connection
- TFTP – Trivial File Transfer Protocol
- Traceroute – Route Tracking Utility
- Show All Services – a more comprehensive list of services is displayed
- Operation: choose from the drop down list:
- NAT – Source IP translation rule
- NAT Addresses: choose from the drop down list:
- User Defined – this routes to the Edit Network Object screen
- NATP – Source IP and port translation rule
- NATP Address: choose from the drop down list:
- User Defined – this routes to the Edit Item screen
- NATP Ports: Choose from the drop down list:
- Single, then enter port number
- Range, then enter range values
- Logging
- Log Packets Matched by This Rule: click this checkbox to log packets matched by this rule

Schedule: choose when the rule is to be followed:

- Always – access is always controlled
- User defined – this routes to the Edit Scheduler Rule screen

Press the OK button to apply changes and go back to the NAT screen.

Press the Cancel button to reject changes and go back to the NAT screen.

4.2.8 Connections

OPTION

EN English

Home

Quick Setup

Internet Connection

Local Network

Services

System

Shortcuts

Telephone

SMS

Overview

Firewall

VPN

Storage

DDNS

Advanced

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Connections

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

Active Connections: 9

Approximate Max. Connections: 66862

Connection List

Number	Protocol	LAN IP:Port	GlobeSurfer IP:Port	WAN IP:Port	Direction	Action
1	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
2	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
3	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
4	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
5	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
6	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
7	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
8	UDP	10.34.113.121:1024	10.34.113.121:1024	149.254.192.126:53	Outgoing	
9	UDP	192.168.1.2:1948	10.34.113.121:1948	212.58.250.75:443	Outgoing	

Close

Refresh

Advanced >>

This screen shows all connections currently active.

The following fields are displayed:

- Active Connections: number of active connections
- Approximate Max. Connections: maximum number of possible connections (approximate)

For each active connection the following fields are displayed:

- Number: number of connection in sequential order
- Protocol: protocol used
- LAN IP Port: IP address of LAN
- GlobeSurfer® III+ IP Port: IP address of GlobeSurfer® III+
- WAN IP Port: IP address of WAN
- Direction: Outgoing/incoming
- Action: options for deleting connections

Press the Close button to go back to the previous screen.

Press the Refresh button to refresh the screen.

Press the Advanced button to go to the Home screen.

4.2.9 Advanced Filtering

OPTION

EN English

Home

Quick Setup

Internet Connection

Local Network

Services

System

Shortcuts

Telephone

SMS

Overview

Firewall

VPN

Storage

DDNS

Advanced

GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Firewall

Advanced Filtering

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

Input Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
WAN Cellular Rules						New Entry
Final Rules						New Entry

Output Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
WAN Cellular Rules						New Entry
Final Rules						New Entry

ALG Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Input						
<input checked="" type="checkbox"/> 0	Any	Any	FTP - TCP Any -> 21	ALG FTP	Active	
<input checked="" type="checkbox"/> 1	Any	Any	IKE - UDP 500 -> 500	ALG IPSec	Active	
<input checked="" type="checkbox"/> 2	Any	Any	SIP - UDP Any -> 5060	ALG SIP	Active	
<input checked="" type="checkbox"/> 3	Any	Any	H.323 Call Signaling - TCP Any -> 1720	ALG H.323 CSL	Active	
New Entry						
Output						
<input checked="" type="checkbox"/> 0	Any	Any	FTP - TCP Any -> 21	ALG FTP	Active	
<input checked="" type="checkbox"/> 1	Any	Any	DNS ALG - UDP Any -> 53	ALG DNS Protection	Active	
<input checked="" type="checkbox"/> 2	Any	Any	DHCP ALG - UDP 67-68 -> 67	ALG DHCP	Active	

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.

The screen is divided into three sections, one for Input Rule Sets, one for Output Rule Sets and one for ALG (Application Level Gateway) Rule Sets. The Input Rule Sets and Output Rule Sets sections are comprised of subsets, which can be grouped into three main subjects:

- Initial rules - rules defined here will be applied first, on all gateway devices.
- Network devices rules - rules can be defined per each gateway device.
- Final rules - rules defined here will be applied last, on all gateway devices.

Note: The order of the firewall rules' appearance in the Advanced Filtering screen represents the sequence by which they will be applied.

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

This screen displays advanced filtering rules. Entries can be added, edited, deleted, moved up or moved down.

The following fields are displayed:

- Input Rule Sets for configuring inbound traffic
- Rule ID: the rule identifier
- Source Address: source address of the packets sent to or received from the network object
- Destination Address: destination address of the packets sent to or received from the network object – this address can be configured in the same manner as the source address
- Match: the condition that must exist for the rule to apply
- Operation: action the rule will take
- Status: shows the status of the rule set
- Action: options for adding new entries or editing, deleting, moving up or moving down existing ones

Click on New Entry - this routes to the Add Advanced Filter screen

Output Rule Sets for configuring outbound traffic:

- Rule ID: the rule identifier
- Source Address: source address of the packets sent to or received from the network object
- Destination Address: destination address of the packets sent to or received from the network object – this address can be configured in the same manner as the source address
- Match: the condition that must exist for the rule to apply
- Operation: action the rule will take
- Status: shows the status of the rule set
- Action: options for adding new entries or editing, deleting, moving up or moving down existing ones

Click on New Entry - this routes to the Add Advanced Filter screen

ALG Rule Sets:

- Rule ID: the rule identifier
- Source Address: source address of the packets sent to or received from the network object
- Destination Address: destination address of the packets sent to or received from the network object – this address can be configured in the same manner as the source address
- Match: the condition that must exist for the rule to apply
- Operation: protocol in use
- Status: shows the status of the rule set
- Action: options for adding new entries or editing, deleting, moving up or moving down existing ones

Click on New Entry - this routes to the Add ALG Rule screen

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

Press the Resolve Now button to check the screen.

Press the Refresh button to refresh the screen.

4.2.9.1 Add Advanced Filter

The screenshot shows the GlobeSurfer III+ web interface. At the top, there's a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Firewall, VPN, Storage, DDNS, and Advanced. The 'Firewall' tab is selected, and the 'Add Advanced Filter' screen is displayed. The screen is divided into several sections: 'Matching' with fields for Source Address, Destination Address, Protocol, and a checkbox for Length; 'Operation' with a dropdown menu set to 'Drop' and the text 'Drop packets'; 'Logging' with a checkbox for 'Log Packets Matched by This Rule'; and 'Schedule' with a dropdown menu set to 'Always'. At the bottom, there are 'OK' and 'Cancel' buttons.

Matching

Source Address: Any

Destination Address: Any

Protocol: Any

☐ Length

Operation

Drop Drop packets

Logging

☐ Log Packets Matched by This Rule

Schedule

Always

OK Cancel

This screen allows the entry of advanced filtering rules. The following fields should be entered:

Matching – to apply a rule, a matching must be made between IP addresses and a traffic protocol must be defined:

Source Address: source address of the packets sent to or received from the network object: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Network Object screen
- A specific address

Destination Address: destination address of the packets sent to or received from the network object – this address can be configured in the same manner as the source address: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Network Object screen
- A specific address

Protocol: traffic protocol: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Service screen

- Show Basic Services – if this option is chosen a reduced list of options is displayed including:
- FTP - File Transfer
- HTTP – Web Server
- HTTPS – Secured Web Server
- IMAP – Messaging Server
- L2TP – Layer 2 Tunneling Protocol
- Ping – ICMP Echo Request
- POP3 – Incoming Mail
- SMTP – Outgoing Mail
- SNMP – Simple Network Management Protocol
- Telnet – Remote Connection
- TFTP – Trivial File Transfer Protocol
- Traceroute – Route Tracking Utility
- Show All Services – a more comprehensive list of services is displayed
- Length: click this checkbox to enter packet or data length, then choose from the drop down list:
- Packet Length, then enter range in bytes
- Data Length, then enter range in bytes

Operation: define what action the rule will take, by selecting one of the following from the drop down list:

- 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 an ICMP error or a TCP reset to the origination peer.
- Accept Connection – 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 be useful when creating rules that allow broadcasting.
- Logging
- Log Packets Matched by This Rule: click this checkbox to log the first packet from a connection that was matched by this rule
- Schedule: choose when the rule is to be followed:
- Always – access is always controlled
- User defined – this routes to the Edit Scheduler Rule screen

Press the OK button to apply changes and go back to the Advanced Filtering screen.

Press the Cancel button to reject changes and go back to the Advanced Filtering screen.

4.2.9.2 Add ALG Rule

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DNS Advanced

Firewall

Add ALG Rule

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

Matching

Source Address Any

Destination Address Any

Protocol Any

Operation

ALG Select...

Logging

☐ Log Packets Matched by This Rule

Schedule Always

OK Cancel

This screen allows the entry of ALG (Application Level Gateway) rules. The following fields should be entered:

Matching - to apply a rule, a matching must be made between IP addresses and a traffic protocol must be defined:

- Source Address: source address of the packets sent to or received from the network object: choose from the drop down list:
- Any
- User Defined – this routes to the Edit Network Object screen
- A specific address

Destination Address: destination address of the packets sent to or received from the network object – this address can be configured in the same manner as the source address: choose from the drop down list:

- Any
- User Defined – this routes to the Edit Network Object screen
- A specific address
- Protocol: traffic protocol: choose from the drop down list:
- Any
- User Defined – this routes to the Edit Service screen

Show Basic Services – if this option is chosen a reduced list of options is displayed including:

- FTP - File Transfer
- HTTP – Web Server
- HTTPS – Secured Web Server
- IMAP – Messaging Server
- L2TP – Layer 2 Tunneling Protocol
- Ping – ICMP Echo Request
- POP3 – Incoming Mail
- SMTP – Outgoing Mail
- SNMP – Simple Network Management Protocol
- Telnet – Remote Connection
- TFTP – Trivial File Transfer Protocol
- Traceroute – Route Tracking Utility
- Show All Services – a more comprehensive list of services is displayed
- Operation: choose from the drop down list:
 - FTP
 - H.323 CSL
 - SIP
 - IPSec
 - Logging

Log Packets Matched by This Rule: click this checkbox to log the first packet from a connection that was matched by this rule

Schedule: choose when the rule is to be followed:

- Always – access is always controlled
- User defined – this routes to the Edit Scheduler Rule screen

Press the OK button to apply changes and go back to the Advanced Filtering screen.

Press the Cancel button to reject changes and go back to the Advanced Filtering screen.

4.2.9.3 Log

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logo

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall Log

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering

Close Clear Log Download Log Settings Refresh

Press the Refresh button to update the data.

Time	Event	Event-Type	Details
Jul 28 15:17:08 2008	WBM Login	User authentication success	Username: admin [repeated 5 times, last time on Jul 28 19:58:34 2008]
Jul 28 12:43:36 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:43:35 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:43:34 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:43:34 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:43:34 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:43:34 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:43:33 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:43:33 2008	Firewall Setup	Firewall internal	No IP for NAT - connections may fail [repeated 2 times, last time on Jul 28 12:43:33 2008]
Jul 28 12:43:33 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:42:47 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:42:47 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:42:45 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:42:45 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:42:43 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:42:43 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:42:40 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:42:40 2008	Firewall Setup	Firewall internal	Starting firewall configuration
Jul 28 12:37:01 2008	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jul 28 12:37:01 2008	Firewall Setup	Firewall internal	Starting firewall configuration

The Security Log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate through an administrative interface (Web-based management or Telnet terminal), firewall configuration and system start-up.

The following fields are displayed:

- Time: the date and 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: a textual description of the event:

- Blocked: the packet was blocked – the message is colored red
- Accepted: the packet was accepted – the message is colored green
- Details: more details about the packet or the event, such as protocol, IP addresses, ports, etc.

Press the Close button to go back to the Home screen.

Press the Clear Log button to delete all entries in the log and stay on this screen.

Press the Download Log button to download the log into a Microsoft Excel spreadsheet.

Press the Settings button to go to the Log Settings screen

Press the Refresh button to refresh the screen.

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

- Firewall internal - an accompanying explanation from the firewall internal mechanism will be added in case this event-type is recorded.
- Firewall status changed - the firewall changed status from up to down or the other way around, as specified in the event type description.
- STP packet - an STP packet has been accepted/rejected.
- Illegal packet options - the options field in the packet's header is either illegal or forbidden.
- Fragmented packet - a fragment has been rejected.
- WinNuke protection - a WinNuke attack has been blocked.
- ICMP replay - an ICMP replay message has been blocked.
- ICMP redirect protection - an ICMP redirected message has been blocked.
- Packet invalid in connection - a packet has been blocked, being on an invalid connection.
- ICMP protection - a broadcast ICMP message has been blocked.
- Broadcast/Multicast protection - a packet with a broadcast/multicast source IP has been blocked.
- Spoofing protection - a packet from the WAN with a source IP of the LAN has been blocked.
- DMZ network packet - a packet from a demilitarized zone network has been blocked.
- Trusted device - a packet from a trusted device has been accepted.
- Default policy - a packet has been accepted/blocked according to the default policy.
- Remote administration - a packet designated for GlobeSurfer® III+™ II management has been accepted or blocked.
- Access control - a packet has been accepted or blocked according to an access control rule.
- Parental control - a packet has been blocked according to a parental control rule.
- NAT out failed - NAT failed for this packet.
- DHCP request - GlobeSurfer® III+™ II sent a DHCP request (depends on the distribution).
- DHCP response - GlobeSurfer® III+™ II received a DHCP response (depends on the distribution).
- DHCP relay agent - a DHCP relay packet has been received (depends on the distribution).
- IGMP packet - an IGMP packet has been accepted.
- Multicast IGMP connection - a multicast packet has been accepted.
- RIP packet - a RIP packet has been accepted.
- PPTP connection - a packet inquiring whether GlobeSurfer® III+™ II is ready to receive a PPTP connection has been accepted.
- Kerberos key management 1293 - security related, for future use.
- Kerberos 88 - for future use.
- AUTH:113 request - an outbound packet for AUTHprotocol has been accepted (for maximum security level).
- Packet-Cable - for future use.

- IPV6 over IPV4 - an IPV6 over IPV4 packet has been accepted.
- ARP - an ARP packet has been accepted.
- PPP Discover - a PPP discover packet has been accepted.
- PPP Session - a PPP session packet has been accepted.
- 802.1Q - a 802.1Q (VLAN) packet has been accepted.
- Outbound Auth1X - an outbound Auth1X packet has been accepted.
- IP Version 6 - an IPV6 packet has been accepted.
- GlobeSurfer® III+ initiated traffic - all traffic that GlobeSurfer® III+ initiates is recorded.
- Maximum security enabled service - a packet has been accepted because it belongs to a permitted service in the maximum security level.
- SynCookies Protection - a SynCookies packet has been blocked.
- ICMP Flood Protection - a packet has been blocked, stopping an ICMP flood.
- UDP Flood Protection - a packet has been blocked, stopping a UDP flood.
- Service - a packet has been accepted because of a certain service, as specified in the event type.
- Advanced Filter Rule - a packet has been accepted or blocked because of an advanced filter rule.
- Fragmented packet, header too small - a packet has been blocked because after the defragmentation, the header was too small.
- Fragmented packet, header too big - a packet has been blocked because after the defragmentation, the header was too big.
- Fragmented packet, drop all - not used.
- Fragmented packet, bad align - a packet has been blocked because after the defragmentation, the packet was badly aligned.
- Fragmented packet, packet too big - a packet has been blocked because after the defragmentation, the packet was too big.
- Fragmented packet, packet exceeds - a packet has been blocked because defragmentation found more fragments than allowed.
- Fragmented packet, no memory - a fragmented packet has been blocked because there was no memory for fragments.
- Fragmented packet, overlapped - a packet has been blocked because after the defragmentation, there were overlapping fragments.
- Defragmentation failed - the fragment has been stored in memory and blocked until all fragments arrived and defragmentation could be performed.
- Connection opened - usually a debug message regarding a connection.
- Wildcard connection opened - usually a debug message regarding a connection.
- Wildcard connection hooked - usually debug message regarding connection.
- Connection closed - usually a debug message regarding a connection.
- Echo/Chargen/Quote/Snork protection - a packet has been blocked, protecting from Echo/Chargen/Quote/Snork.
- First packet in connection is not a SYN packet - a packet has been blocked because of a TCP connection that had started without a SYN packet.
- Error: No memory - a message notifying that a new connection has not been established because of lack of memory.

- NAT Error : Connection pool is full - a message notifying that a connection has not been created because the connection pool is full.
- NAT Error: No free NAT IP - a message notifying that there is no free NAT IP, therefore NAT has failed.
- NAT Error: Conflict Mapping already exists - a message notifying that there is a conflict since the NAT mapping already exists, therefore NAT has failed.
- Malformed packet: Failed parsing - a packet has been blocked because it is malformed.
- Passive attack on ftp-server: Client attempted to open Server ports - a packet has been blocked because of an unauthorized attempt to open a server port.
- FTP port request to 3rd party is forbidden (Possible bounce attack) - a packet has been blocked because of an unauthorized FTP port request.
- Firewall Rules were changed - the firewall rule set has been modified.
- User authentication - a message during login time, including both successful and failed authentication.
- First packet is Invalid - First packet in connection failed to pass firewall or NAT

4.2.9.4 Log Settings

OPTION

GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Firewall Log Settings

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

Accepted Events

☐ Accepted Incoming Connections

☐ Accepted Outgoing Connections

Blocked Events

☐ All Blocked Connection Attempts

☐ WinNuke

☐ Defragmentation Error

☐ Blocked Fragments

☐ Syn Flood

☐ Echo Chargen

☐ Multicast/Broadcast

☐ Spoofed Connection

☐ Packet Illegal Options

☐ UDP Flood

☐ ICMP Replay

☐ ICMP Redirect

☐ ICMP Multicast

☐ ICMP Flood

Other Events

☐ Remote Administration Attempts

☐ Connection States

Log Buffer

This screen allows you to select the types of activities for which you would like to have a log message generated:

The following checkboxes can be clicked:

- Accepted Events

- Accepted Incoming Connections - write a log message for each successful attempt to establish an inbound connection to the home network.
- Accepted Outgoing Connections - write a log message for each successful attempt to establish an outgoing connection to the public network.
- Blocked Events
 - All Blocked Connection Attempts - write a log message for each blocked attempt to establish an inbound connection to the home 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 "All Blocked Connection Attempts" check-box is checked.
 - Winnuke
 - Defragmentation Error
 - Blocked Fragments
 - Syn Flood
 - Echo Chargen
 - Multicast/Broadcast
 - Spoofed Connection
 - Packet Illegal Options
 - UDP Flood
 - ICMP Replay
 - ICMP Redirect
 - ICMP Multicast
 - ICMP Flood
 - Other Events
- Remote Administration Attempt - write a log message for each remote-administration connection attempt, whether successful or not.
- Connection States - provide 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).
- Log Buffer

Prevent Log Overrun - select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.

Press the OK button to apply changes and go back to the Log screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Log screen.

4.3 VPN/Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec)

Block Unauthorized IP ☒ Enabled

Maximum Number of Authentication Failures:

Block Period (in seconds):

Anti-Replay Protection ☒ Enabled

Connections

Name	Status	Action

OK Apply Cancel Settings Log Settings

This screen allows the entry of Internet Protocol Security (IPSec) data. The following fields should be entered:

- Block Unauthorized IP
- Enabled: click this checkbox to block unauthorized attempts, and then enter
- Maximum Number of Authentication Failures: number allowed before blocking
- Block Period: time in seconds
- Anti-Replay Protection
- Enabled: click this checkbox to provide anti-replay protection
- Connections: for each connection the following fields are displayed:
 - Name: description of connection
 - Status: status of connection
 - Action: options for adding new entries or editing or deleting existing ones

Press the OK button to apply changes and go back to the Overview screen.

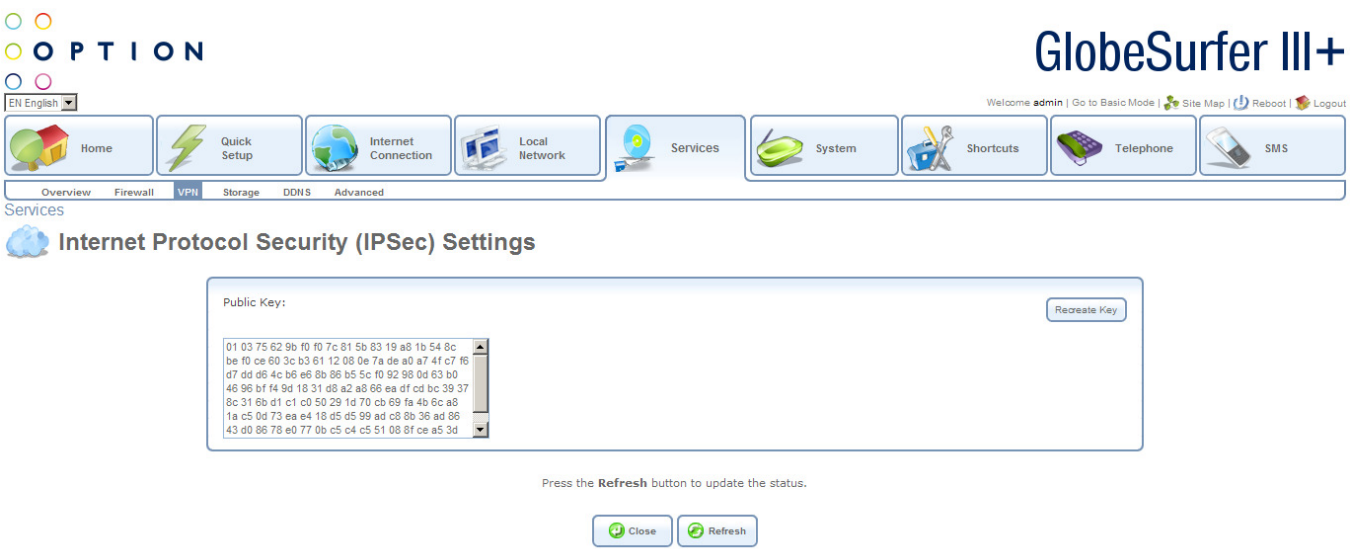
Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

Press the Settings button to go to the Internet Protocol Security (IPSec) Settings screen.

Press the Log Settings button to refresh the screen.

4.3.1 Internet Protocol Security (IPSec) Settings



This screen displays the IPSec public key and allows it to be recreated.

Press the Recreate Key button to recreate the IPSec public key.

Press the Close button to go back to the VPN/Internet Protocol Security (IPSec) screen.

Press the Refresh button to refresh the screen.

4.3.2 IPSec Log Settings

OPTION

GlobeSurfer III+

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Firewall VPN Storage DDNS Advanced

Services

IPSec Log Settings

Enabling all of the IPSec log options may reduce GlobeSurfer's performance.

IKE Log Settings

- ☐ Message's Raw Bytes
- ☐ Message's Encryption and Decryption
- ☐ Message's Input Structure
- ☐ Message's Output Structure
- ☐ Verbose Automatic Keying
- ☐ Verbose IKE IPSec Interaction
- ☐ Verbose Private Keys
- ☐ Verbose Dead Peer Detection
- ☐ Verbose NAT Traversal Negotiation
- ☐ Verbose IKE Reject Packets
- ☐ Print All IKE Messages Ignoring Rate Limit

IPSec Log Settings

- ☐ Tunneling Code
- ☐ Tunneling Transmit Code

This screen allows the customization of the IPSec log, by allowing the user to choose what data is recorded. It is important to note the enabling many of these options may reduce GlobeSurfer® III+'s performance.

The following checkboxes can be clicked:

- IKE Log Settings
- Message's Raw Bytes
- Message's Encryption and Decryption
- Message's Input Structure
- Message's Output Structure
- Verbose Automatic Keying
- Verbose IKE IPSec Interaction
- Verbose Private Keys
- Verbose Dead Peer Detection
- Verbose NAT Traversal Negotiation
- Verbose IKE Reject Packets
- Print All IKE Messages Ignoring Rate Limit
- IPSec Log Settings
- Tunneling Code
- Tunneling Transmit Code

- User-Space Communication Code
- Transform Selection and Manipulation Code
- Internal Route Table Manipulation Code
- Secure Association Table Manipulation Code
- Radij Tree Manipulation Code
- Encryption Transforms Code
- Authentication Transforms Code
- Receive Code
- IP Compression Transforms Code
- Even More Verbose Output
- Verbose Rejected Packets
- Print All IPSec Messages Ignoring Rate Limit

Press the OK button to apply changes and go back to the VPN/Internet Protocol Security (IPSec) screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the VPN/Internet Protocol Security (IPSec) screen.

4.4 Shared Storage / Disk Management

GlobeSurfer III includes a file server function that allows external hard disk drives to be attached to the device via the USB port. Once the external disk drive is connected, it can be shared by all computers on the LAN.

Note: The external hard disk drives must be formatted as “FAT” (File Allocation Table) format in order to read and write to the disk. NTFS (New Technology File System) format is supported for ‘read’ only and will not enable you to write to the disk. It is possible to re-format your external hard drive in FAT32 format through the GlobeSurfer if you require read/write functionality.

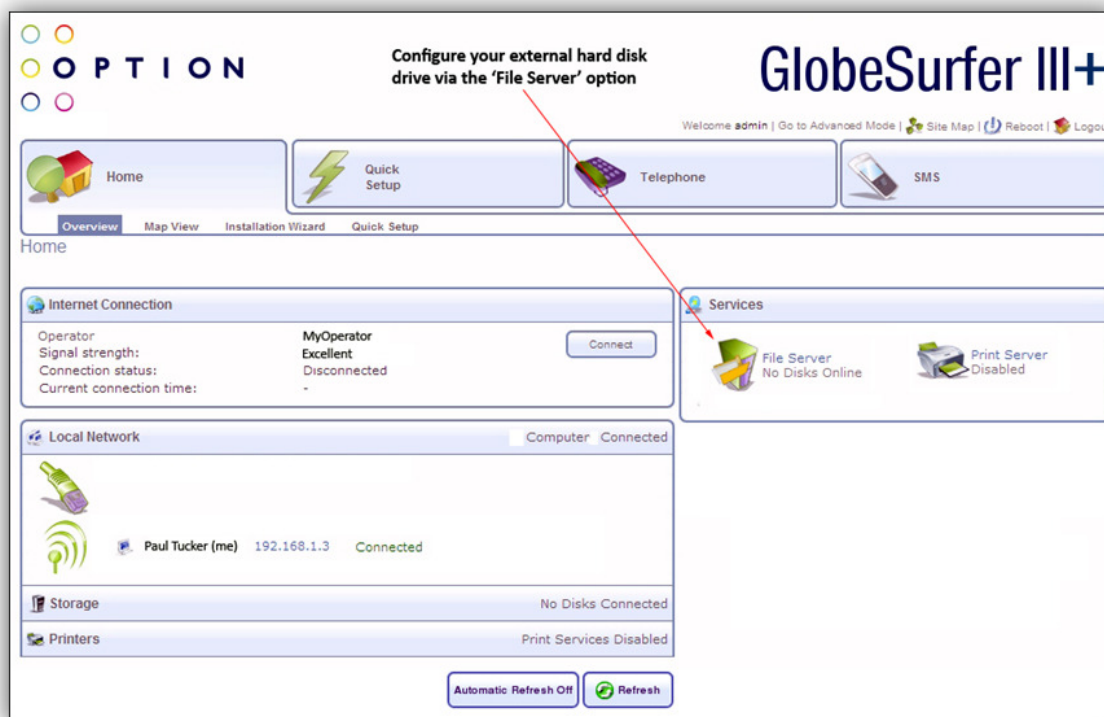
Note: The GlobeSurfer can deliver up to approx. 700 mA of current over the USB connection. Any disk drive having power consumption more than 700 mA has to be powered externally. External hard drives that require power from the GlobeSurfer over the USB connection should be connected while the device is turned off. Otherwise the connection will cause a sudden power surge and may cause the GlobeSurfer to malfunction. USB ‘memory stick’ type of device can be connected to the GlobeSurfer at any point without turning the power off.

To add an external hard disk drive to the GlobeSurfer III device, and use it over the LAN, follow the steps listed below.

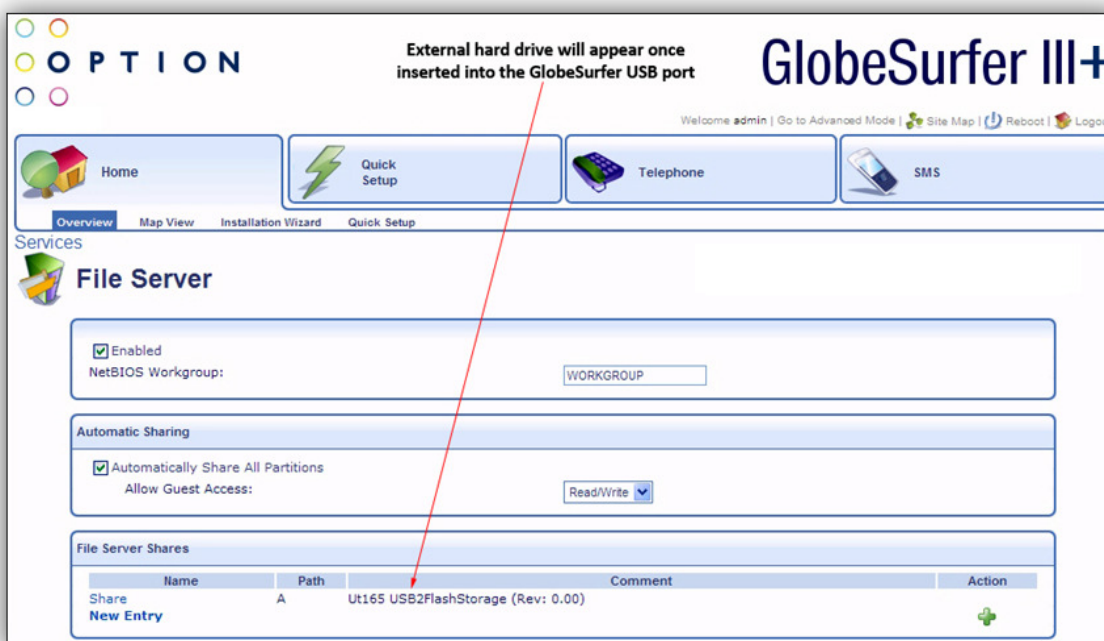
- 1) Power **OFF** the GlobeSurfer III if the external hard drive draws its power from the device it is being connected to.
- 2) Power on and connect the external hard disk drive to the GlobeSurfer USB port, and then turn on the GlobeSurfer III.

- 3) Log in to the GlobeSurfer Management Console.
- 4) Select the “File Server” icon from the Basic or Advanced Home Screen.

4.4.1 Adding normal disk drives

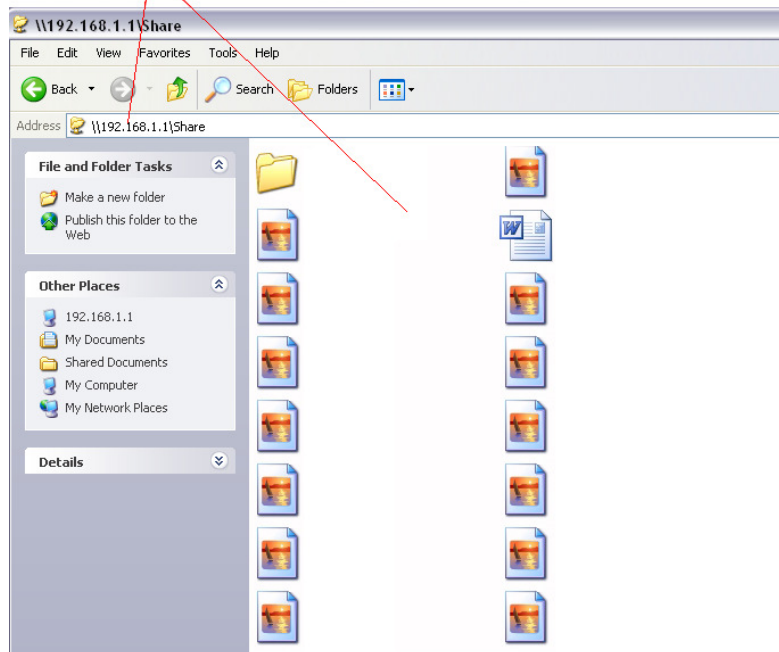


Once you insert your external hard drive to the USB port on the GlobeSurfer III, the browser will refresh to show the presence of the external device.



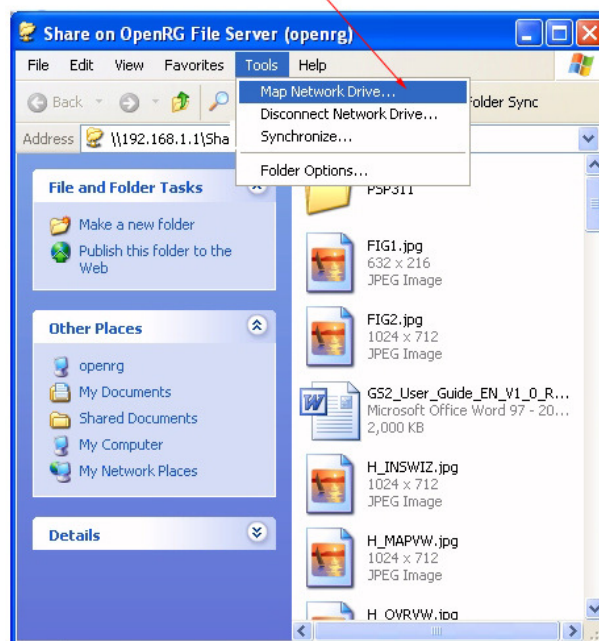
Open Windows Explorer and type in Address : <\\192.168.1.1\\share> or <\\GlobeSurferIII\\Share>. A new client windows will open showing the content of your external drive.

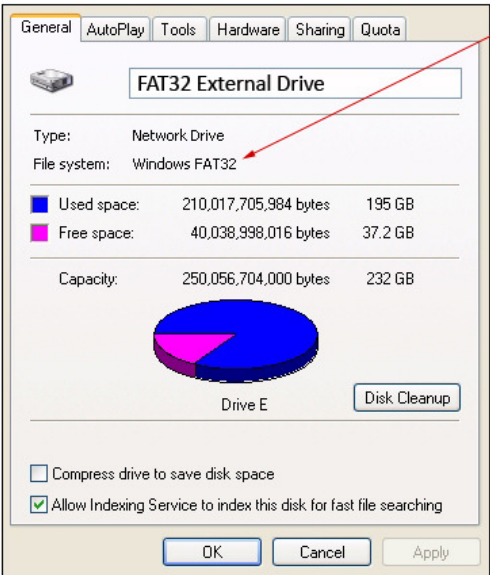
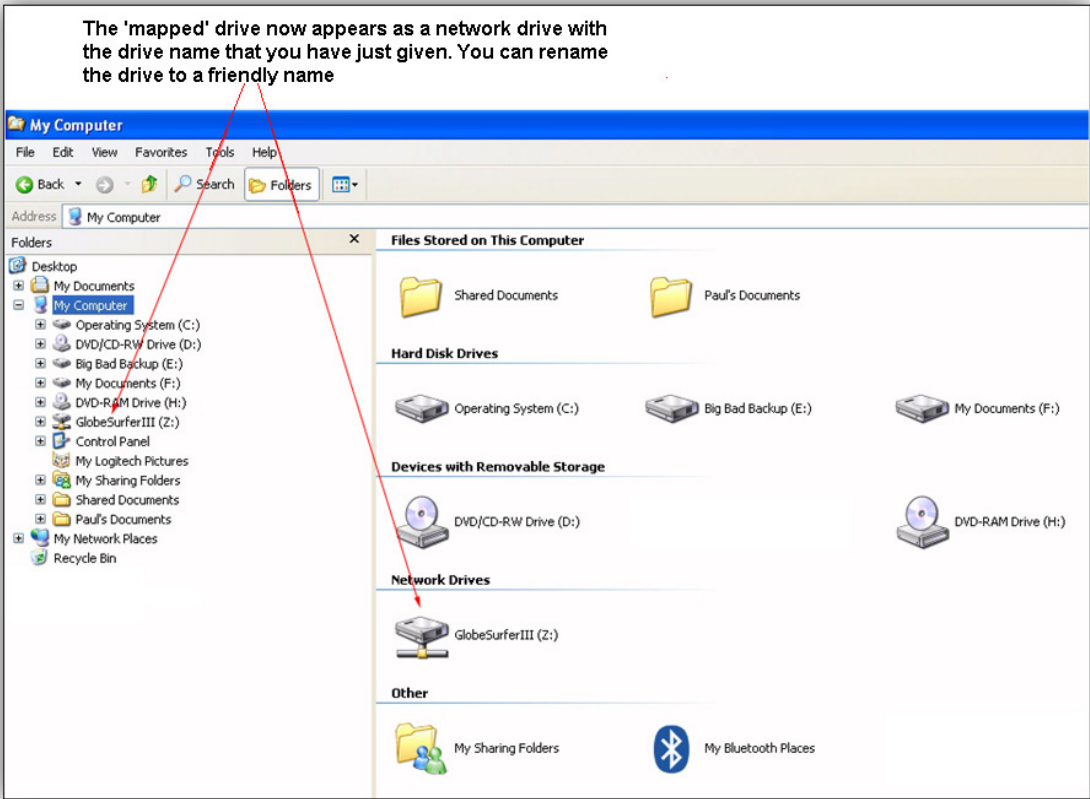
The external hard drive will open a new client window showing the contents of the external hard drive.



In order to configure your external hard drive device so that it is available every time you insert it into the GlobeSurfer III, select “Map Network Drive” from the Tools menu and assign a drive label (such as ‘G:’).

To configure your external drive so it appears on your desktop every time it is attached, select 'Map Network Drive' from the Tools menu and assign a drive label (eg 'G:')





Only FAT16 or FAT32 drives are currently 'Read' and 'Write' supported.

NTFS formatted drives are visible in 'Read' mode only.

It is possible to re-format an NTFS external drive as FAT32 by right-clicking on the disk image and selecting 'Format'.

Supported Devices:

- Memory Stick Storage Devices.

- USB Based FAT32 formatted Hard Disk Drives (any devices consuming more than 700 mA should be powered independently to avoid excessive power drain on the GlobeSurfer)

4.4.2 Adding RAID devices

This screen enables you to add a RAID device.

The screenshot shows the GlobeSurfer III+ web interface. At the top, there's a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Device, Wireless, Shared Storage, and Shared Printers. The main content area is titled "RAID Properties" and contains a form for configuring RAID. The form has two fields: "RAID Level:" with a dropdown menu set to "RAID0" and "Mount Point:" with a text input field. Below the form are "Next" and "Cancel" buttons. A message above the form says: "Please choose RAID level, RAID devices and mount point name for the created device."

The following data can be entered:

RAID level: choose one of the following options from the drop down list:

- RAID₀
- RAID₁
- RAID₅

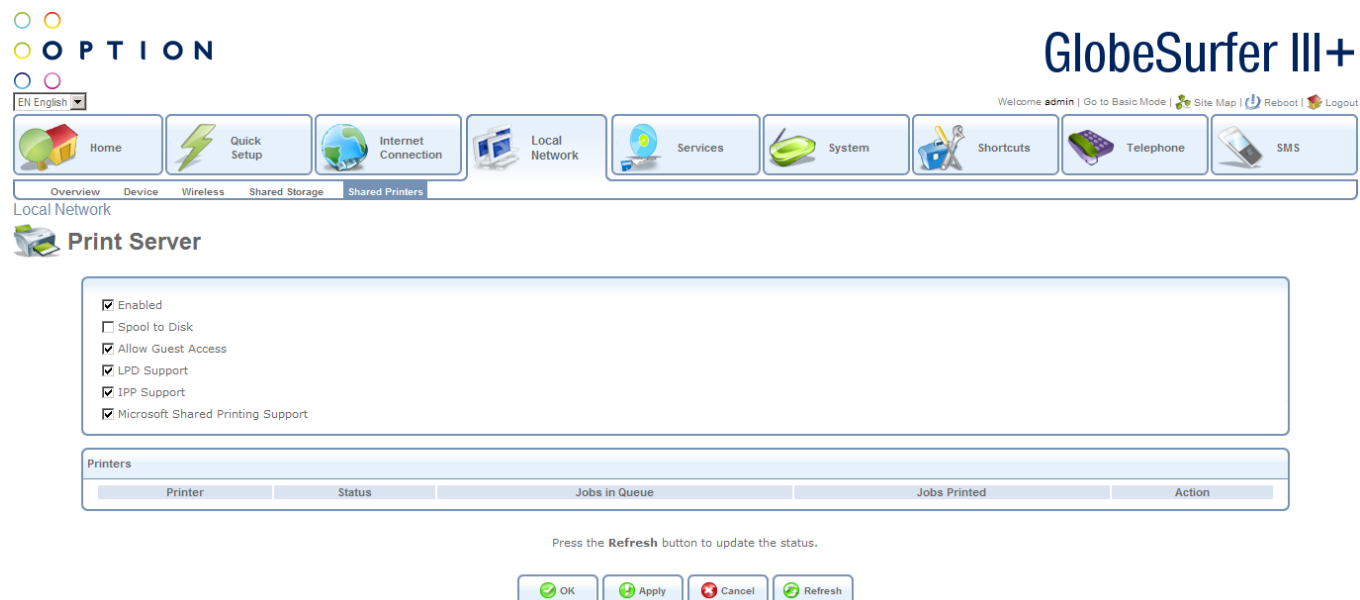
Mount Enabled: add a mount point name for the created device

Press the Next button to apply changes and add another device.

Press the Cancel button to reject changes and go back to the previous screen.

4.5 Shared Printers/Print Server

GlobeSurfer® III+ includes a print server that allows printers attached to the device via the USB connection to be shared by all computers on the LAN.



On this screen you can see information about your printer, as well as view a list of print jobs (when prints are in the queue).

The following checkboxes can be modified:

- Enabled
- Spool to Disk
- Allow Guest Access
- LPD Support
- IPP Support
- Microsoft Shared Printing Support

For each print job, the following data is displayed:

- Printer
- Status
- Jobs in Queue
- Jobs Printed
- Action
- Storage: the number of external hard disk drives connected is shown
- Printers: the number of printers connected is shown

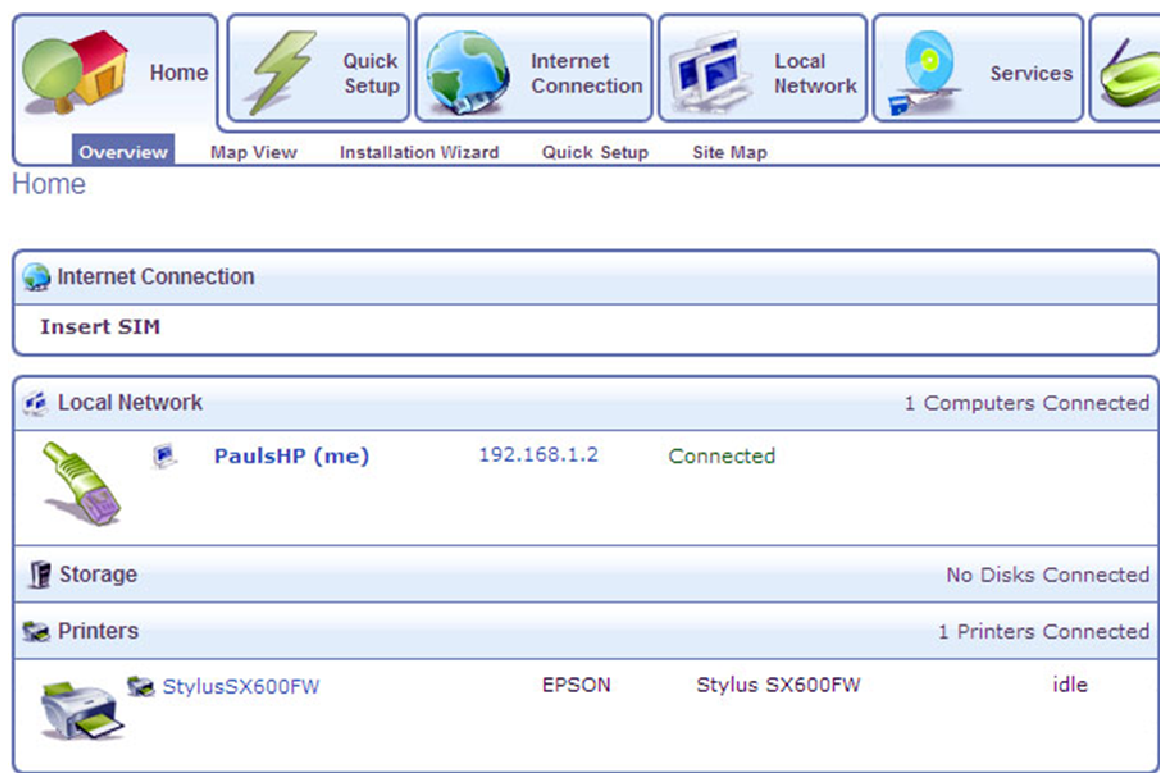
Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

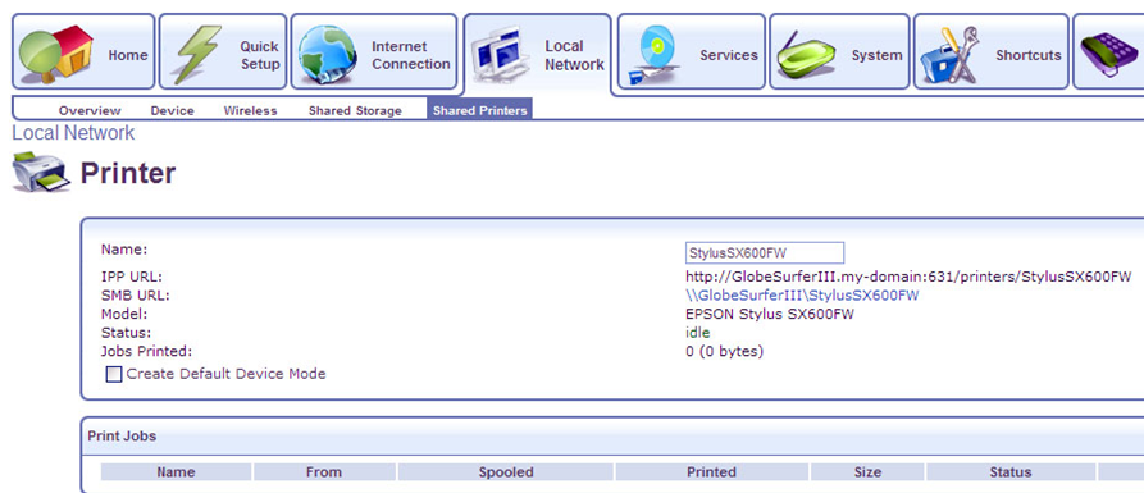
Press the Cancel button to reject changes and go back to the previous screen.

Press the Refresh button to refresh the screen.

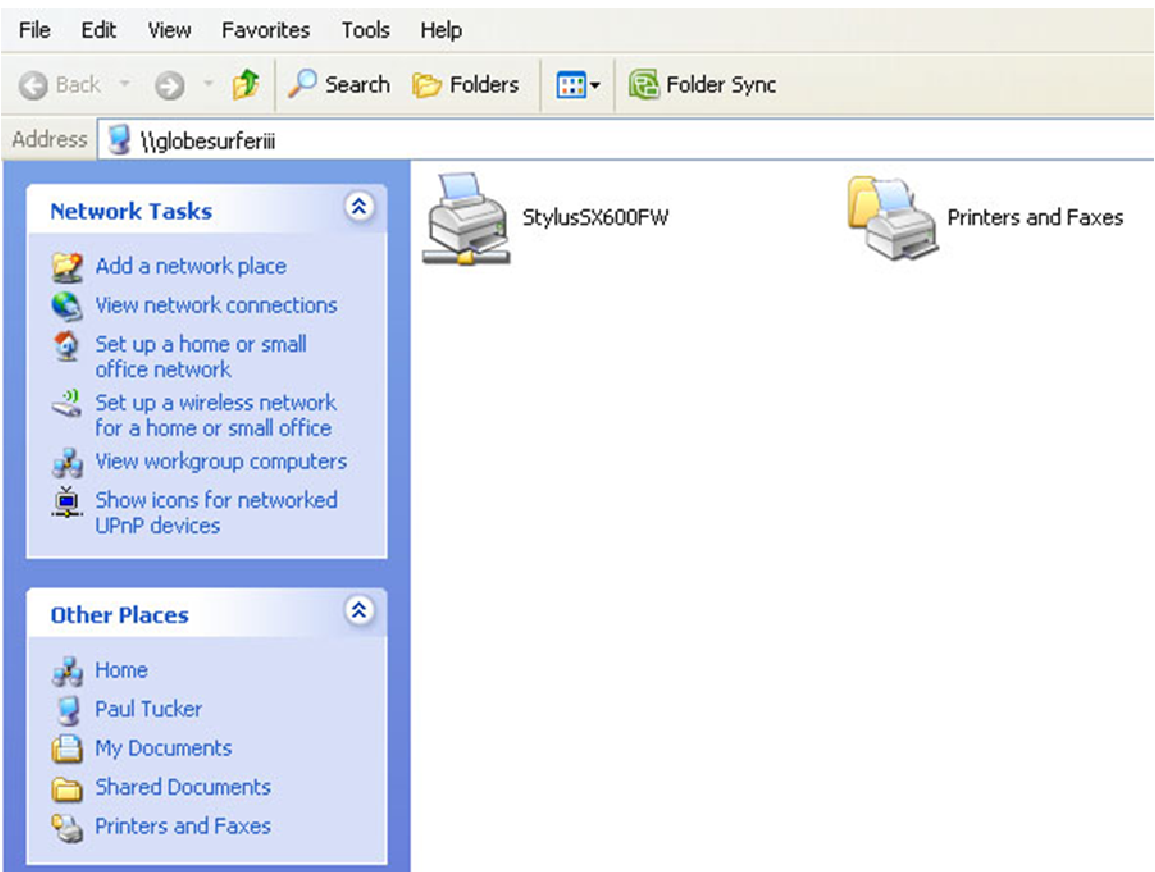
NOTE: Only printers supporting Windows IPP (International Printer Protocols) are supported. This accounts for the vast majority of printers available today, but in some extreme cases, this protocol is not supported, in which case, it is likely the printer will not be recognized.



The auto-detecting nature of the GlobeSurfer GUI will refresh to show the printer connected, along with a link (in blue) to the printer device. By pressing on the blue printer link (as seen above), the following screen is presented:



The user can rename the printer here, and can find the URLs necessary to ‘mount’ the printer onto the users desktop for printing. By clicking on the SMB URL, the following screen appears:



The printer is now installed and ready to be used by network (Wi-Fi or Ethernet) connected users.

4.5.1 Alternative Method of Configuring the Print Server

Normally the method indicated above will be sufficient to enable the configuration of your printer, however in some cases a more granular approach may be necessary.

In the event the above fails to locate or enable your printer, please try the method outlined below.

To use the print server on the Option GlobeSurfer, you need to accomplish the following tasks:

- Install the printer drivers on the computer
- Connect the Printer to you Option GlobeSurfer
- Add a network printer on your Windows based PC

4.5.1.1 Install the Printer Drivers

Printers using the USB port come with a software installation CD for installing the printer drivers and applications. The drivers for the printer must be installed on the computer first to prepare it to use the printer when it's connected to the GlobeSurfer. Refer to the printer's documentation on how to install the drivers.

4.5.1.2 Connecting the Printer

Turn OFF the GlobeSurfer.

Connect the Printer to the USB port and switch ON the router and printer.

4.5.1.3 Add a Network Printer

4.5.1.3.1 For Windows XP

- Before you continue, ensure that you've installed the printer drivers on this computer and the printer is attached to the GlobeSurfer.
- Click on the Start Button > Control Panel > Printers and Other Hardware > Printers and Faxes.
- Click on the File Menu > Add Printer.
- Click on Next on the Add Printer Wizard page.
- Choose Local Printer attached to this computer and click Next, on the Local or Network Printer page.
- Choose Create a new port and on the drop down box choose Standard TCP/IP Port then click Next.
- Click Next button on Welcome to the Add Standard TCP/IP Printer Port Wizard.
- Enter your GlobeSurfer's Default Gateway IP address 192.168.1.1 then click Next.
- Under Additional Port Information Required choose Custom then click Next
- Once the computer detects the printer on the Print Server, it will ask for the printer manufacturer and model, a list of printers will be shown, select the your printer from the list and click OK.
- Choose Keep existing driver (recommended) then click Next until you reach Completing the Add Printer Wizard.
- Click Finish to complete the installation.

4.5.1.4 *Printing a Test Page after Installation*

Open the Printers and Faxes page from Control Panel.

Right click on the new printer and click on Properties.

Click on the Print Test Page button on the Printer properties page, the test page will be printed on the network printer.

For Windows Vista

- Click on the Start Button> Control Panel.
- Click Printer under the Hardware and Sound category.
- Click on Add a Printer.
- Click on Add a local printer then click Next.
- Select Create a new port, on the drop down box choose Standard TCP/IP port then click Next.
- Enter the Default Gateway IP address of your GlobeSurfer 192.168.1.1 then click Next.
- Under Additional Port Information Required window, select Custom then click Next.
- Once the computer detects the printer on the Print Server, it will ask for the printer manufacturer and model, a list of printers will be shown, select the your printer from the list and click OK.
- Select Use the driver that is currently installed then click Next.
- To print a test page click on Print a test page on the confirmation screen, click Finish to complete the installation.
- If Printing was unsuccessful right click on the Printer's icon then select Properties.
- Under printer's Properties click Port Tab and tick the IP address (192.198.1.1) that was set on previous settings then click Apply

4.6 Failover

The GlobeSurfer can be configured to backup a fixed DSL line in converting one of the Ethernet port as WAN input. GlobeSurfer samples the DSL connection at a fixed interval. When it finds the DSL line going down, it will switch automatically to WWAN.

GlobeSurfer will continue to sample the fixed DSL line. When the connection comes back, it will switch back internet connect to the DSL line.

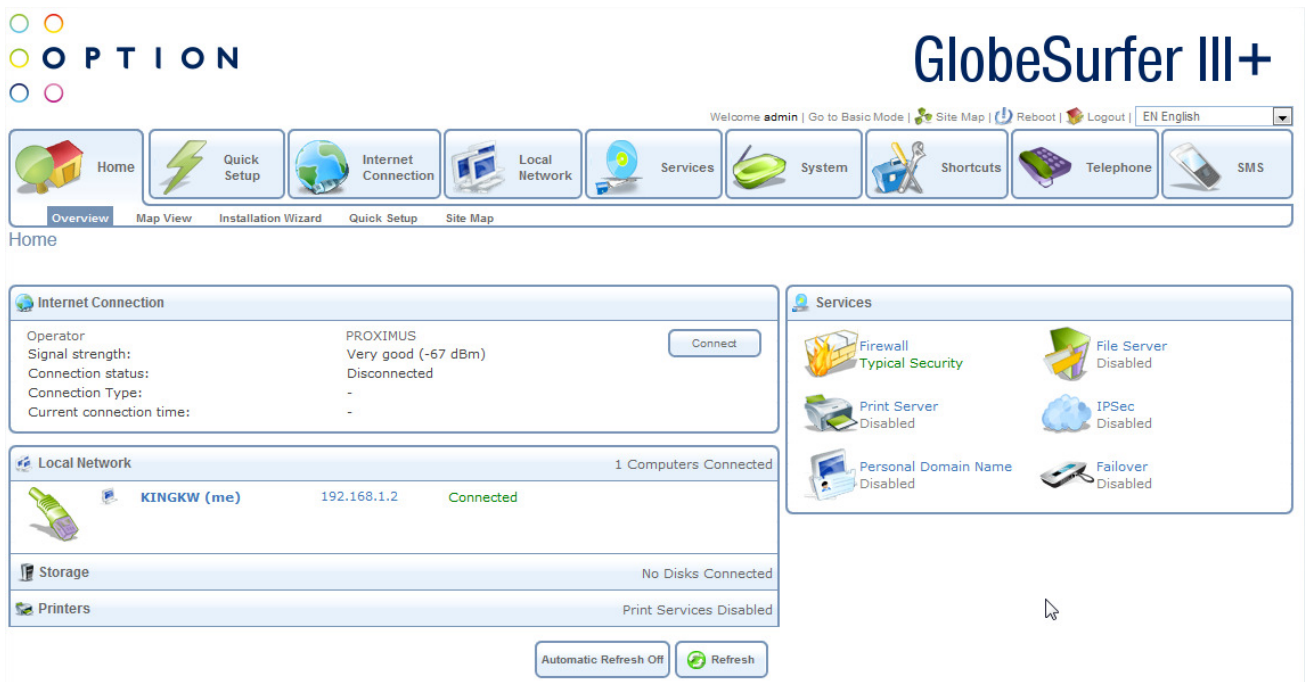


LAN Ethernet and WAN Ethernet interfaces on the GlobeSurfer

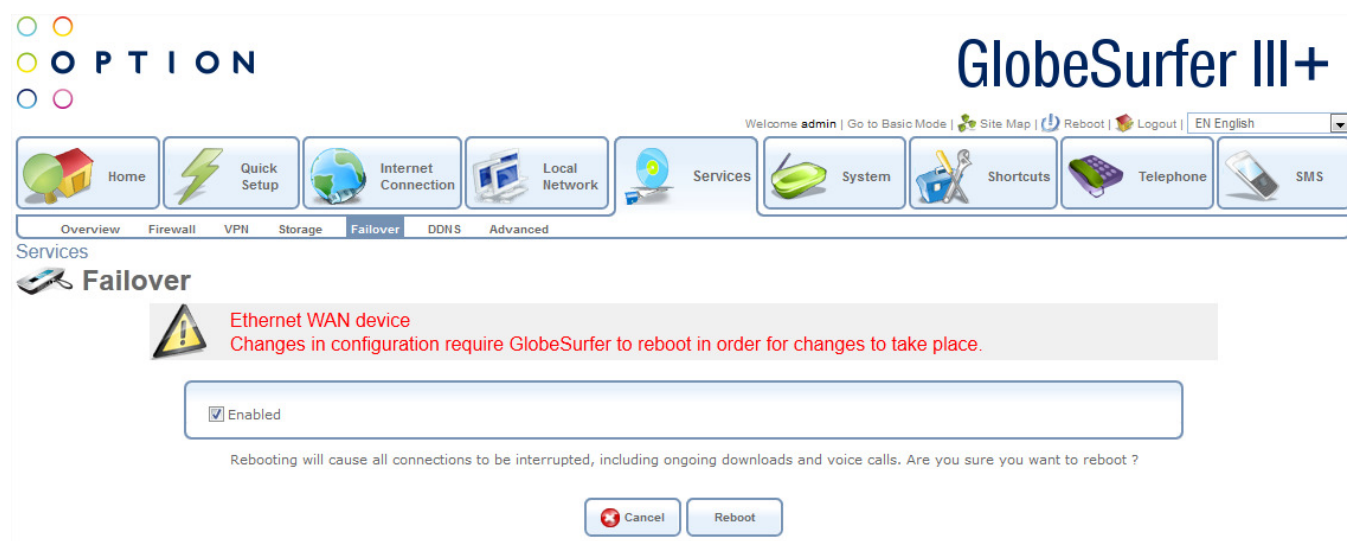
4.6.1 Failover Configuration

Follow the next steps to activate the failover functionality on the GlobeSurfer:

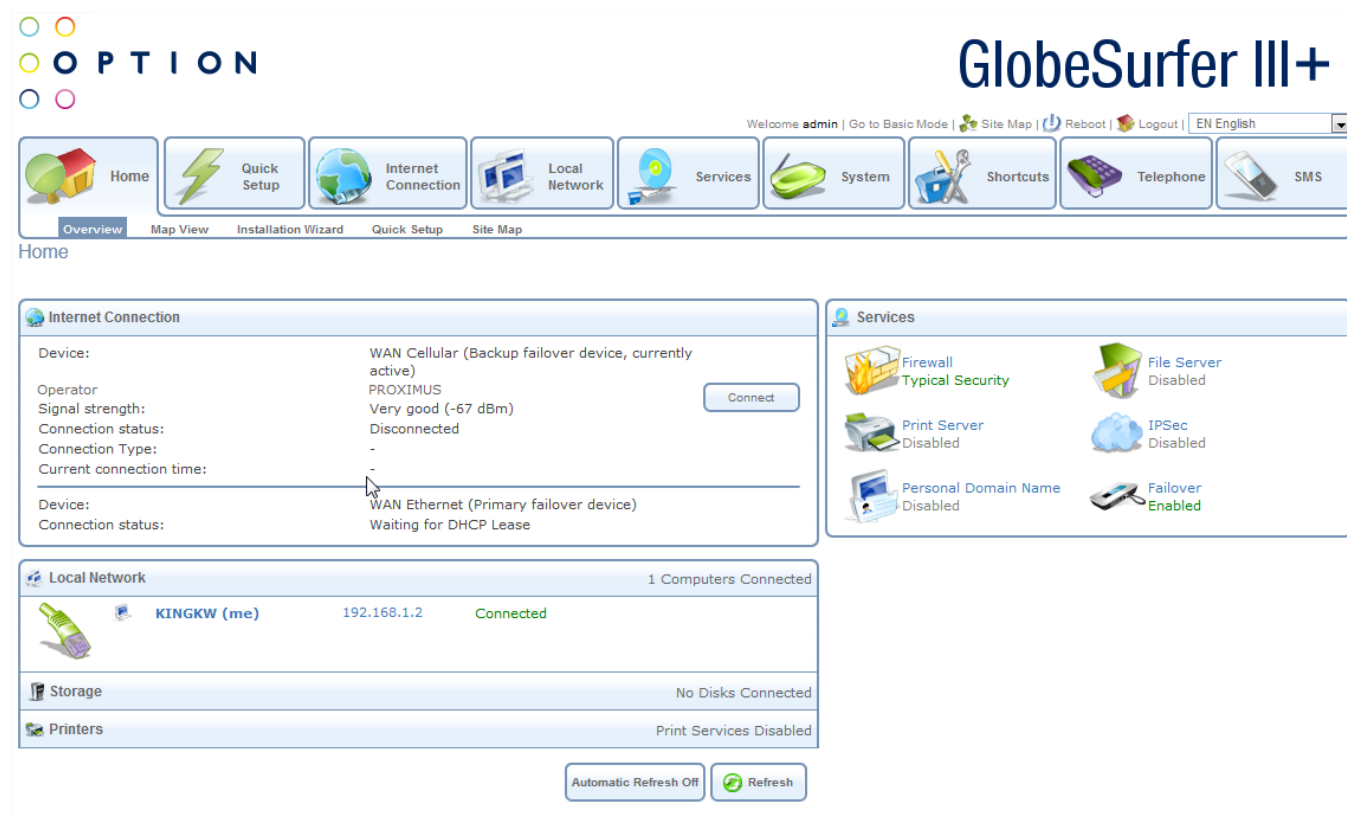
- Go to Advance Mode



- Click on the Failover Link located on the “Services” section, the GUI will prompt you to the Failover configuration page.



- To enable the Failover functionality, check the “Enabled” check box.
- Click on the Reboot button to reboot the device.



After the reboot, the Home page of the GUI is going to show information about the new failover functionality.



The Network connections page (Under System>Network Connections) also shows a new device called “WAN Ethernet” which is one of the two physical Ethernet interfaces on the GlobeSurfer.

Services

Failover

☒ Enabled

Active device:

Primary device:

Backup device:

Active device metric:

Standby device metric:

WAN Cellular

WAN Ethernet

WAN Cellular

10

20

DNS

DNS query time:

30

Seconds

DNS request timeout:

10

Seconds

Host Names

Host Name	Action
www.option.com	

[New Entry](#)

Constraints

Constraint check time:

30

Seconds

Number of connections:

0

Throughput:

0

Kbps

Constraint times

Start Time	End Time	Action

OK

Apply

Cancel

The Failover configuration page has change after the reboot of the GlobeSurfer and now it shows the different configuration parameters that are available for the Failover.

On the Failover page we can distinguish five different sections:

1. General section: In which you can find:

- The enabled check box: to activate or deactivate the failover functionality.
- The Active device: shows the device that is currently in use.
- Primary device: is the first device to use. By default this device will be the WAN Ethernet, but it can be changed.
- Secondary device: is the device to go when the first device fails. By default this device will be the WAN Cellular, but it can be change.
- Active device metric: this metric is applied to the “Active device” to force the device to send all the data through that interface. This value always has to be lower than the “Standby device metric”. The default value is 10.
- Standby device metric: this metric is applied to the Non-Active device and always has to be bigger than the “Active device metric” to ensure that all the packages are send through the
- “Active device”. The default value is 20.

2. DNS section: In which you can find:

- DNS query time: at this interval the GlobeSurfer will send DNS request out to check the “Active device” connection to internet. The default value is 30 seconds.
- DNS request timeout: as it can take few seconds before the GlobeSurfer gets an answer from the DNS server, this parameter set how patient the GlobeSurfer is before it decides that there is no connection through the “Active device”. The default value is 10 seconds.

3. Host Names section: this is the list of hosts to resolve with the DNS request. The GlobeSurfer will attempt to resolve each host on the list each “DNS query time” until the end of the list or until a host can be resolved. If at least one of the hosts can be resolved, the connection is assumed to be OK. The user can add or remove host from this list, be aware that the list has to have at least one host.

4. Constraints section: In which you can find:

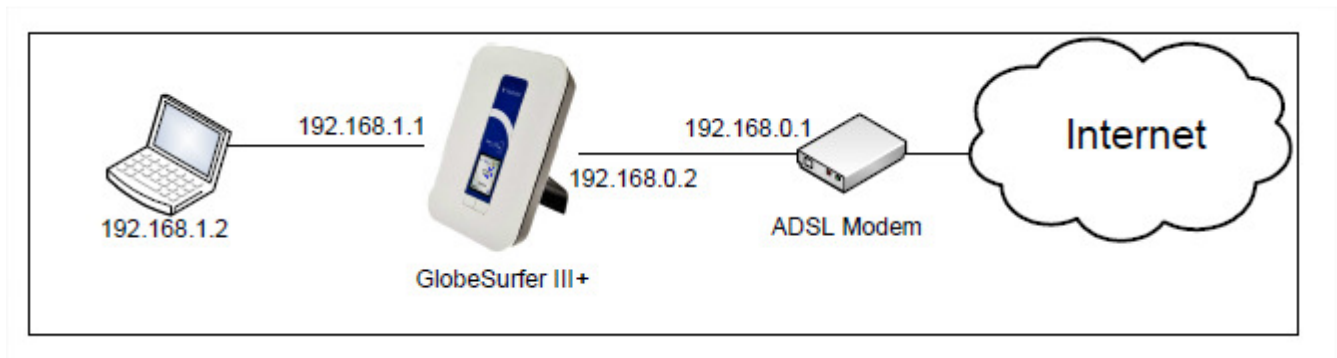
- Constraints check time: at this interval, the GlobeSurfer will see if it is OK to switch back to the “Primary device” if it is currently using the “Secondary device”. The default value is 30 seconds.
- Number of connections: if at a “Constraint time check” interval, the number of ongoing TCP connections is greater than this value, no attempt will be made to switch back to the primary
- device. The default value is 0 which means that the number of connections doesn’t matter for the failover.
- Throughput: if at a “Constraint time check” interval, the current throughput is greater than this value, no attempt will be made to switch back to the primary device. The default value is 0 which means that the throughput doesn’t matter for the failover.

5. Constraint times section: a list of time periods in which it is ok to switch back from the “Secondary device” to the “Primary device”.

4.6.2 Configuration example

The following example will cover the configuration of the failover functionality together with a possible configuration for the WAN cellular interface.

The following Network diagram shows the network configuration that will be used on this example.



Network Diagram

In this example the ADSL Modem was already configured to be connected to the internet and with its LAN connection as follows:

IP Address: 192.168.0.1

Network mask: 255.255.255.252 (Only two devices on the network)

The first step is enabling the Failover functionality described here above.

Use the default configuration of the Failover, no changes have to be done on the Failover configuration page.

By default the IP address of the WAN Ethernet is set to DHCP but in our case we will use a static IP address due to the configuration of the ADSL modem. To change this just go to System>Network Connections, click on WAN Ethernet and under Settings change the Internet Protocol to “Use the Following IP address”.

The screenshot shows the 'WAN Ethernet Properties' window with the following settings:

- Device Name:** bcm0.2
- Status:** Failed Connectivity Check
- Schedule:** Always
- Network:** WAN
- Connection Type:** Ethernet
- Physical Address:** 30 16 b2 5e 0e 71
- MTU:** Automatic 1500
- Internet Protocol:** Use the Following IP Address

192	168	0	2
255	255	255	252
192	168	0	1
- DNS Server:** Use the Following DNS Server Addresses

192	168	0	1
0	0	0	0
- IP Address Distribution:** Disabled

Buttons at the bottom: OK, Apply, Cancel.

WAN Ethernet Properties page

Go to quick setup and change the UMTS connection to “Automatically connect upon traffic” and the inactivity timer to one.

The screenshot shows the 'Quick Setup' page with the following settings:

- Language and region settings:**
 - Language: EN English
 - Time Zone: Europe/Brussels (GMT+01:00)
- Telephony:**
 - Caller ID: ETSI DTMF
- UMTS:**
 - Access point name: internet.proximus.be
 - UMTS connect method:
 - ☐ Connect, Manually
 - ☒ Automatically connect upon traffic
 - ☐ Always connected
 - In case of inactivity, disconnect after (minutes): 0
- Wireless:** (Section header)

Quick Setup

Note: Using this UMTS configuration, the GS3 will be disconnected from the 3G network unless we lose connection through the WAN Ethernet port, this connection will remain until there is a gap of one minute without traffic on the 3G interface. This is only a possibility for the configuration; each of the three UMTS types of connection should work with their own specifications.

The GlobeSurfer is now ready to be connected to the ADSL Modem. Remember that there is a specific Ethernet port for the WAN Ethernet. After connecting the GlobeSurfer to the ADSL router you should be

able to see on the Home page and on the Failover page that the “Active device” changes to WAN Ethernet instead of WAN Cellular.

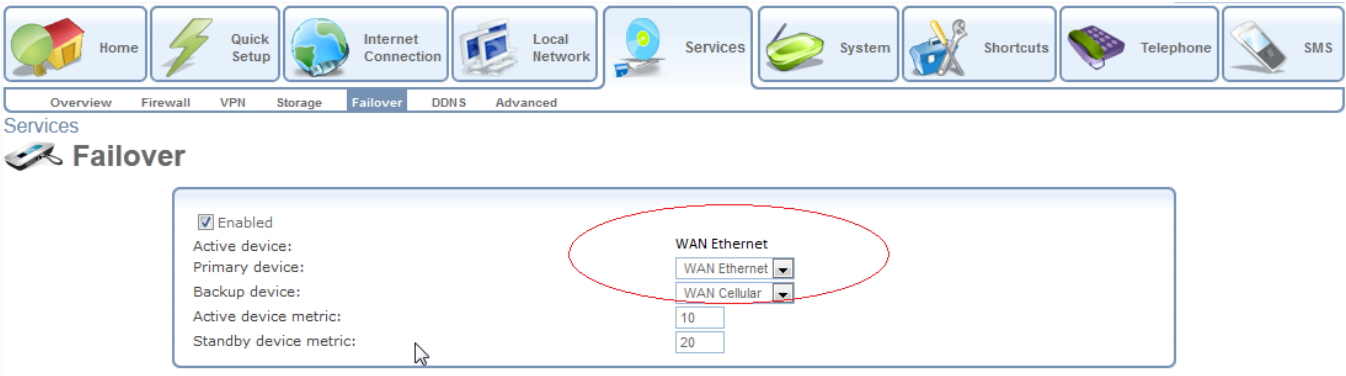
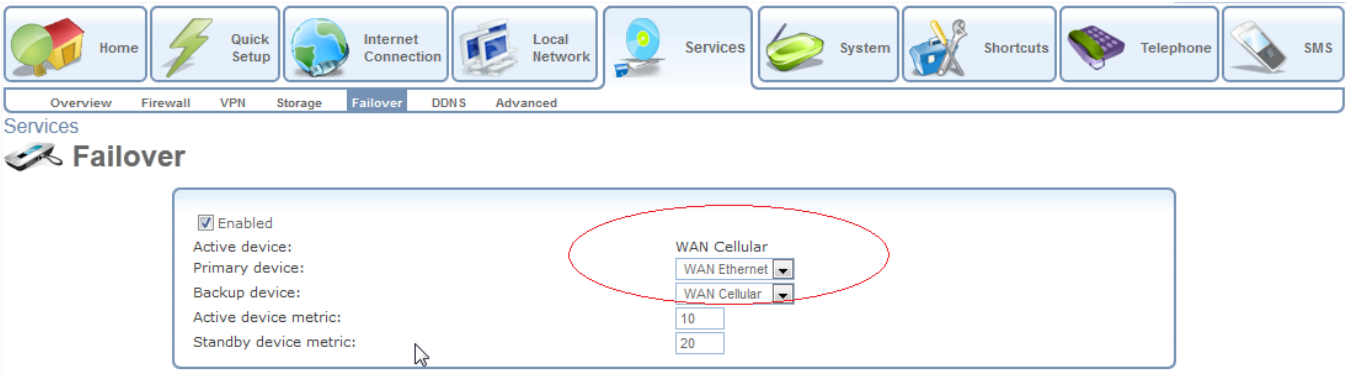
Home

Internet Connection	
Device:	WAN Cellular (Backup failover device, currently active)
Operator	PROXIMUS
Signal strength:	Very good (-67 dBm)
Connection status:	Connected
Connection Type:	HSDPA
Current connection time:	0:38:24 [hh:mm:ss]
<hr/>	
Device:	WAN Ethernet (Primary failover device)
Connection status:	Failed Connectivity Check

Home

Internet Connection	
Device:	WAN Cellular (Backup failover device, currently active)
Operator	PROXIMUS
Signal strength:	Very good (-67 dBm)
Connection status:	Connected
Connection Type:	UMTS
Current connection time:	0:00:21 [hh:mm:ss]
<hr/>	
Device:	WAN Ethernet (Primary failover device, currently active)
Connection status:	Waiting for DHCP Lease

Home Page view



Failover Configuration page view

5 System

This area enables the user to configure system settings and perform maintenance functions.

From this screen you can click on the tabs at the top left hand side to route to the following detailed screens:

- Overview - system overview including version, release date, platform, load average
- Settings - configure systems settings, date and time parameters and set the clock
- Users - list of remote users/groups, and ability to add, edit or delete users/groups
- Network Connections - configure parameters of physical connections, LAN/WAN
- Monitor - monitors traffic within local network or between local network/Internet
- Routing - routing overview + enable RIP, IGMP, Domain Routing, BGP, OSPF, PPPoE
- Management - ability to configure UPnP, SNMP and Remote Administration
- Maintenance - config file, reboot, restore settings, perform upgrade, diagnostics
- Objects and Rules - protocols, network objects, scheduler rules + X.509 certificates

5.1 Overview

System Information

Gateway ID:	000CE365F6AB	Upgrade
Software Version:	P1A08	
Release Date:	Jul 14 2008	
Platform:	BCM5354	
System Has Been Up For:	2 days, 17 hours	
Load Average (1 / 5 / 15 mins.):	0.02 / 0.01 / 0.00	

This screen displays general system information:

- Gateway ID: displays the 12 character gateway ID.
- Software Version: displays the 5 character software version.
- Release Date: displays the date the software was released.
- Platform: displays the platform the software runs on.
- System Has Been Up For: shows the time in hours and minutes that the system has been running.
- Load Average: shows the average load over 1, 5 and 15 minutes.

Click on the Upgrade hyperlink to be routed to the Firmware upgrade screen in the Maintenance tab in the System area

5.2 System Settings

Access GlobeSurfer® III+'s system settings by clicking the Settings tab in the System area.

From this screen you can click on the tabs at the top right hand side to route to the following detailed screens:

- Overview
- Date and Time

5.2.1 Overview/System Settings

To access the System Settings screen, click the Overview tab at the top right hand side of the Settings screen in the System area.

The screenshot displays the 'System Settings' interface of the GlobeSurfer III+ device. The top navigation bar includes tabs for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this, a sub-navigation bar shows tabs for Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The main content area is titled 'System Settings' and contains three sections:

- System:** Fields for 'GlobeSurfer's Hostname' (openng) and 'Local Domain' (home).
- GlobeSurfer Management Console:** Checkboxes for 'Automatic Refresh of System Monitoring Web Pages' and 'Warn User Before Configuration Changes', and a 'Session Lifetime' field set to 900 seconds.
- Management Application Ports:** A list of ports including Primary HTTP Management Port (80), Secondary HTTP Management Port (8080), Primary HTTPS Management Port (443), Secondary HTTPS Management Port (8443), Primary Telnet Port (23), Secondary Telnet Port (8023), Secure Telnet over SSL Port (992), Jungo.net Port (7020), and Jungo.net SSL Port (7021).

The System Settings screen allows you to configure various system and management parameters:

System:

- GlobeSurfer® III+'s Hostname: hostname is the URL address of the GlobeSurfer® III+.
- Local Domain: specify your network's local domain.
- GlobeSurfer® III+ Management Console:
- 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.
- Session Lifetime: controls the session lifetime (seconds) for logins to the management console. When the time has expired the login screen will appear again.

Management Application Ports: this section allows you to configure the following management application ports:

- Primary HTTP Management Port
- Secondary HTTP Management Port
- Primary HTTPS Management Port
- Secondary HTTPS Management Port
- Primary Telnet Port
- Secondary Telnet Port
- Secure Telnet over SSL Port
- Jungo.net Port
- Jungo.net SSL Port

Management Application SSL Authentication Options:

- Primary HTTPS Management SSL Client Authentication: select from the drop down list:
- None
- Optional
- Required

Secondary HTTPS Management SSL Client Authentication select from the drop down list:

- None
- Optional
- Required

Secure Telnet over SSL Client Authentication: select from the drop down list:

- None
- Optional
- Required
- System Logging:
- System Log Buffer Size: size in KB

Remote System Notify Level: select from the drop down list:

- None
- Error
- Warning
- Information
- Persistent System Log: select this checkbox to keep the system log.

Security Logging:

- Security Log Buffer Size: size in KB
- Remote Security Notify Level: select from the drop down list:

- None
- Error
- Warning
- Information
- Persistent Security Log: select this checkbox to keep the security log.

Outgoing Mail Server:

- Server: enter the hostname of your outgoing (SMTP) server.
- From Email Address: each email requires a from-address and some outgoing servers refuse to forward email without a valid from address for anti-spam considerations.
- Port: used to alter the server port, if your mail server does not use the standard port 25.
- Server Requires Authentication: select the checkbox if your outgoing email server requires authentication, and then enter:
 - User Name: your username
 - Password: your password

Swap:

- Enabled: select this checkbox to enable swapping.
- Status: shows the swap status. Possible options are:
 - Disabled
 - Inactive
 - Active
- Swap Size: enter the swap size in MB.

HTTP Interception:

- Intercept HTTP Traffic for Assisting with Internet Connectivity Problems: select this checkbox to intercept HTTP traffic.
- Perform Web Authentication Over HTTPS: select this checkbox to perform web authentication over HTTPS.

Host Information:

- Enable Auto Detection of Host Services: select this checkbox to enable automatic detection of host services.

Installation Wizard:

- Use Installation Wizard Pre-configured Values: select this checkbox if you wish to use the installation wizard's pre-configured values.

LCD Settings (Not applicable to GlobeSurfer III+):

- Screensaver Timeout: sets the time in seconds before the screensaver is displayed

- Go Home Timeout: sets the time in seconds for the Go Home timeout
- Contrast: sets the contrast level on the LCD

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

5.2.2 Date and Time

To access the Date and Time screen, click the Date and Time tab at the top right hand side of the Settings screen in the System area.

Localization

Local Time: Jul 31, 2008 02:06:17
 Time Zone: GMT (GMT+00:00)

Daylight Saving Time

☒ Enabled
 Start Time: Mar 28 00 : 00
 End Time: Oct 28 01 : 00
 Offset: 60 Minutes

Automatic Time Update

☒ Enabled
 Protocol: ☐ Time Of Day (TOD) ☒ Network Time Protocol (NTP)
 Update Every: 24 Hours Synchronize Now

Time Server	Action
ntp.jungo.com New Entry	

Status: Got time update from server, Last Update: Wed Jul 30 11:27:49 2008

To configure date and time settings enter the following:

Localization:

- Local Time: shows the current date and time. This is set automatically if automatic update has been chosen, or manually by pressing the Clock Set button at the bottom of the screen.
- Time Zone: select the local time zone from the pull-down menu.

Daylight Saving Time:

- Enabled: select this checkbox if you would like the Daylight Saving/British Summertime offset to be made to the time in the time zone.
- Start Time: enter the date and time when the daylight saving offset should start from.
- End Time: enter the date and time when the daylight saving offset should end.
- Offset: enter the number of minutes that should be added during the daylight saving period.

Automatic Time Update:

Enabled: select this checkbox if you want the GlobeSurfer® III+ to update the time automatically.

Protocol: select the protocol to be used to perform the time update by selecting one of the two following radio buttons:

- Time of Day (TOD)
- Network Time Protocol (NTP)
- Update Every: specify how often to perform the update (in hours). You can change the default timeserver address by clicking the New Entry link at the bottom of the section.
- Press the Sync Now button to synchronize the time.
- Status: shows the date and time when the time was last updated.

Click on the edit icon in the Time Server table to modify an entry, or click on the New Entry hyperlink or the add icon to add an entry. In both cases you will be routed to the Time Server Settings screen.

Press the OK button to apply changes and go back to the Home screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the Home screen.

Press the Clock Set button to go to the Clock Set screen.

Press the Refresh button to update the status and stay on this screen

5.2.2.1 Time Server Settings

To access the Time Server Settings screen, click the New Entry hyperlink from the Date and Time screen in the System area.

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance Objects and Rules

Settings

Time Server Settings

Enter server IP address or domain name:

Time Server:

OK Cancel

To configure time server settings enter the following:

- Time Server: enter server IP address or domain name

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.2.2.2 Clock Set

To access the Clock Set screen, click the Clock Set button on Date and Time screen in the System area.

The screenshot displays the GlobeSurfer III+ web interface. At the top, there is a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a secondary navigation bar with tabs for Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The 'Settings' tab is active, and the 'Clock Set' screen is displayed. The 'Clock Set' screen has a title bar with a clock icon and the text 'Clock Set'. Below the title bar, there are two input fields: 'Local Date:' and 'Local Time:'. The 'Local Date:' field has three dropdown menus for month (Jul), day (31), and year (2008). The 'Local Time:' field has three input boxes for hours (02), minutes (58), and seconds (34). At the bottom of the form, there are three buttons: 'OK', 'Apply', and 'Cancel'.

To set the clock enter the following:

- Local Date: choose the current month, day and year from the drop down lists.
- Local Time: manually enter the current hours, minutes and seconds.

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.3 Users

Access the list of defined remote users by clicking the Users tab in the System area.

Users

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator Permissions Wireless Permissions Microsoft File and Printer Sharing Access	
New User			

Groups

Name	Description	Members	Action
Users			
New Group			

[Close](#)

You can add, edit and delete users allowed to access the GlobeSurfer® III+ and your local network by managing the user table.

For each user the following data is displayed:

- Full Name: the remote user's full name
- User Name: the name the remote user will use to access your local network
- Permissions: the remote user's privileges on your local network
- Action: add, modify or delete
- For each group the following data is displayed:
 - Name
 - Description
 - Members
 - Action: add, modify or delete

Click on the Microsoft File and Printer Sharing Access Permission hyperlink to be routed to the File Server screen off the Storage tab in the Services area.

Click on a specific User hyperlink or the edit icon in the Users table to modify an entry, or click on the New User hyperlink or the add icon to add an entry. In both cases you will be routed to the User Settings screen.

Click on a specific Group hyperlink or the edit icon in the Groups table to modify an entry, or click on the New Group hyperlink or the add icon to add an entry. In both cases you will be routed to the Group Settings screen.

Press the Close button to go back to the previous screen.

5.3.1 User Setting

To access the User Settings screen, click New User hyperlink from the Users screen in the System area.

General

Full Name:

User Name:

New Password (case sensitive):

Retype New Password:

Permissions:

- ☐ Administrator Permissions
- ☐ Wireless Permissions
- ☐ Microsoft File and Printer Sharing Access
- ☐ Internet Printer Access
- ☐ Remote Access by VPN

802.1X Authentication

Authentication Method:

Disk Management

☒ Enable User Home Directory

Email Notification

[Click here to configure notification Mail Server](#)

Notification Address:

System Notify Level:

To configure user settings enter the following:

General:

- Full Name: the remote user's full name
- User Name: 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. This field is case sensitive.
- Retype New Password: if a new password was assigned, type it again to verify correctness.
- Permissions: selecting the remote user's privileges on your local network:
- Administrator Permissions: selecting this checkbox grants remote system setting modification via the web-based management console or telnet
- Wireless Permissions: selecting this checkbox grants wireless permissions
- Microsoft File and Printer Sharing Access: selecting this checkbox grants access to Microsoft's file and printer sharing.
- Microsoft File and Printer Sharing Access: click on the hyperlink and you will be routed to File Server screen off the Storage tab in the Services area.

Internet Printer Access: selecting this checkbox grants access to internet printers.

Internet Printer Access: click on the hyperlink and you will be directed to the Print Server screen off the Shared Printers tab in the Local Network area.

- Remote Access by VPN: selecting this checkbox enables remote access by VPN
- 802.1X Authentication:
- Authentication Method: choose a method from the drop down list – options are:
 - None
 - MD5
 - TLS
 - TTLS
- Disk Management:
 - Enable User Home Directory: selecting this checkbox enables the user's home directory.
- Email Notification:
 - Click here to configure notification Mail Server: click on the hyperlink and you will be routed to the System Settings Overview screen off the Settings tab in the System area
 - Notification Address: enter the appropriate address
 - Systems Notify Level: choose a method from the drop down list – options are:
 - None
 - Error
 - Warning
 - Information
- Security Notify Level: choose a method from the drop down list – options are:
 - None
 - Error
 - Warning
 - Information

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.3.2 Group setting

To access the Group Settings screen, click the New Group hyperlink from the Users screen in the System area.

The screenshot displays the 'Group Settings' interface within the GlobeSurfer III+ web application. The top navigation bar includes 'System' and 'Group Settings'. The main content area contains the following elements:

- Name:** A text input field with a dropdown menu currently set to 'Group'.
- Description:** A text input field.
- Group Members:** A section containing a checkbox labeled 'Administrator'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

To configure group settings enter the following:

- General:
- Name: group name
- Description: group description
- Group Members:
- Administrator: selecting this checkbox grants administrator status

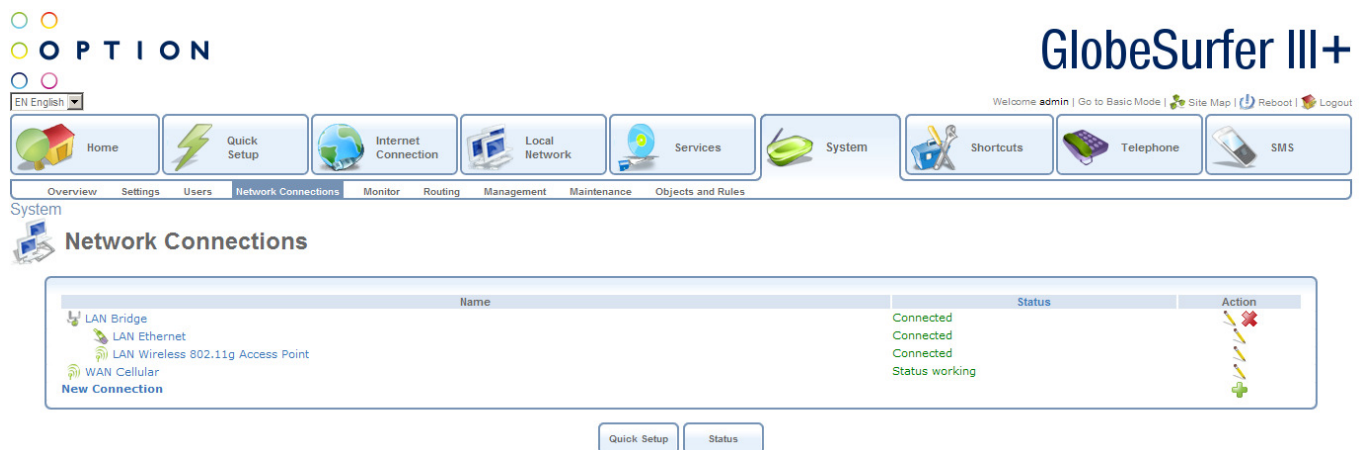
Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.4 Network Connection

GlobeSurfer® III+ supports various network connections, both physical and logical. The Network Connections screen enables you to configure the various parameters of your physical connections, the LAN and WAN, and create new connections, using tunneling protocols over existing connections, such as PPP and VPN.

When clicking the Network Connections tab in the System area, the following typical screen will appear:



This section describes the different network connections available with GlobeSurfer® III+ in their order of appearance in the Network Connections screen, as well as the connection types that you can create using the Connection Wizard.

GlobeSurfer® III+'s default network connections are:

- LAN - Creating a home/SOHO network
- LAN Bridge
- LAN Ethernet
- LAN Wireless
- WAN - Internet Connection
- WAN Cellular
- The logical network connections available with GlobeSurfer® III+ are:
- Virtual Private Network over the Internet
- Point-to-Point Tunneling Protocol Virtual Private Network
- Layer 2 Tunneling Protocol over Internet Protocol Security
- Internet Protocol Security
- Point-to-Point Tunneling Protocol Server
- Layer 2 Tunneling Protocol Server
- Internet Protocol Security Server
- Advanced Connections
- Point-to-Point Protocol over Ethernet
- Network Bridging
- VLAN Interface
- Point-to-Point Tunneling Protocol
- Point-to-Point Tunneling Protocol Virtual Private Network
- Point-to-Point Tunneling Protocol Server
- Layer 2 Tunneling Protocol
- Layer 2 Tunneling Protocol over Internet Protocol Security

Layer 2 Tunneling Protocol Server

- Internet Protocol Security
- Internet Protocol Security Server
- Internet Protocol over Internet Protocol
- General Routing Encapsulation

5.4.1 Connection wizard

The logical network connections can be easily created using the Connection Wizard. This wizard consists of a series of web-based management screens, intuitively structured to gather all the information needed to create a logical connection.

In order to create a connection using the Connection Wizard, click the New Connection hyperlink in the Network Connections screen. The Connection Wizard screen will appear.



This screen presents you with the main connection types. Each option that you choose will lead you to further options in a tree-like formation, adding more information with each step and narrowing down the parameters towards the desired network connection.

Connect to a Virtual Private Network over the Internet: selecting this option will take you to the Connect to a Virtual Private Network over the Internet screen. This section will help you connect GlobeSurfer® III+ to a business network using a Virtual Private Network (VPN) so you can work from home, your workplace or another location.



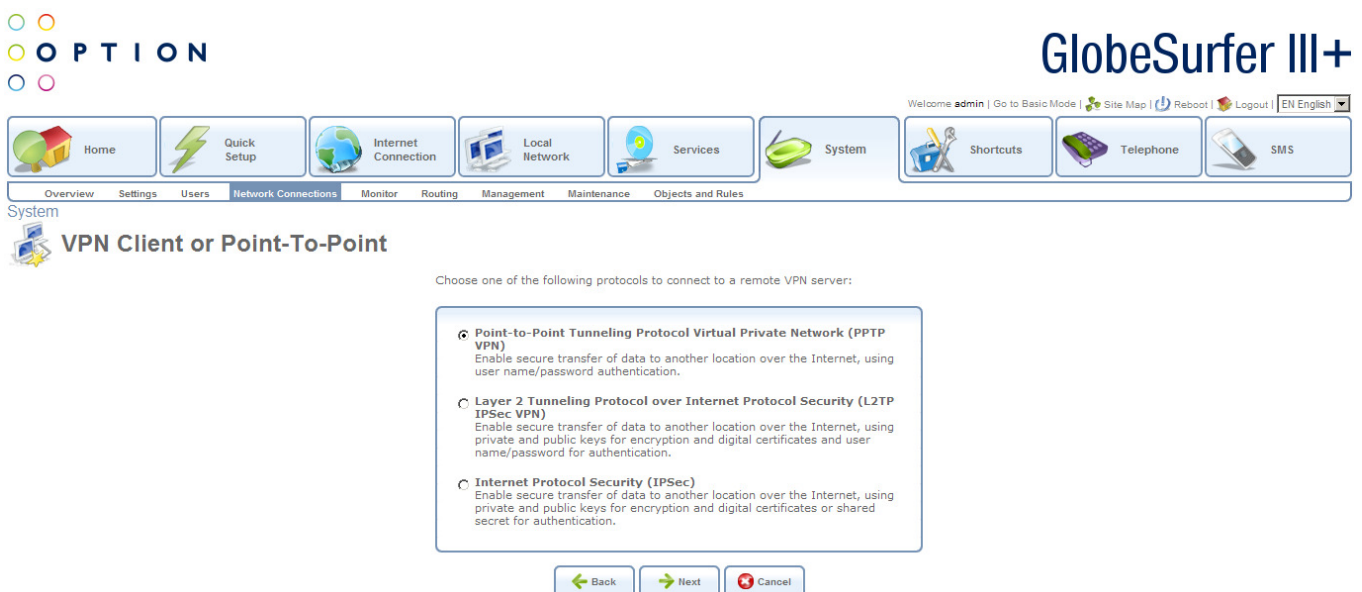
VPN Client or Point-To-Point: selecting this option will take you to the VPN Client or Point-To-Point screen.

From here you can choose one of the following protocols to connect to a remote VPN server:

Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN): enable the secure transfer of data to another location over the Internet, using name/password authentication

Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN): enable the secure transfer of data to another location over the Internet using private and public keys for encryption and digital certificates and user name/password for authentication

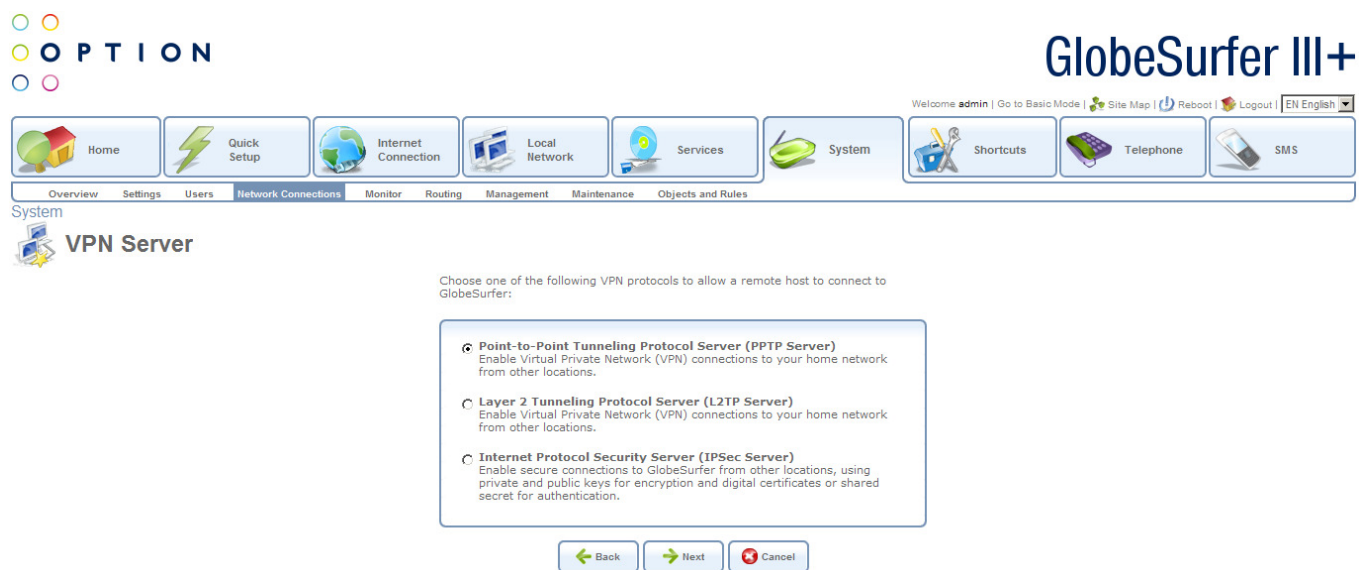
Internet Protocol Security (IPsec): enable the secure transfer of data to another location over the Internet using private and public keys for encryption and digital certificates or shared secret for authentication



VPN Server: selecting this option will take you to the VPN Server screen.

From here you can choose one of the following VPN protocols to allow a remote host to connect to GlobeSurfer® III+:

- **Point-to-Point Tunneling Protocol Server (PPTP Server):** enable Virtual Private Network (VPN) connections to your home network from other locations
- **Layer 2 Tunneling Protocol Server (L2TP Server):** enable Virtual Private Network (VPN) connections to your home network from other locations
- **Internet Protocol Security Server (IPSec Server):** enable secure connections to GlobeSurfer® III+ from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication



Going back to the Connection Wizard page:

- **Advanced Connection:** selecting this option will take you to the Advanced Connection screen. This section is a central starting point for all the advanced logical network connections. In addition, it provides the sequence for creating the Network Bridge and VLAN Interface connections.

From here you can choose your connection type:

- **Point-to-Point Protocol over EthernetServer (PPTP Server):** connect to the Internet using a PPP tunnel over the Ethernet protocol
- **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):** connect to the Internet using a PPTP connection
- **Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN):** enable secure transfer of data to another location over the Internet, using user name/password authentication
- **Point-to-Point Tunneling Protocol Server (PPTP Server):** enable Virtual Private Network (VPN) connections to your home network from other locations
- **Layer 2 Tunneling Protocol (L2TP):** connect to the Internet using an L2TP connection

- Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN): enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password authentication
- Layer 2 Tunneling Protocol Server (L2TP Server): enable Virtual Private Network (VPN) connections to your home network from other locations
- 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 or shared secret for authentication
- Internet Protocol Security Server (IPsec Server): enable secure connections to GlobeSurfer® III+ from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication
- Internet Protocol over Internet Protocol (IPIP): enable transfer of data to another location over the Internet, using a non-encrypted virtual private network
- General Routing Encapsulation (GRE): enable transfer of data to another location over the Internet, using a non-encrypted virtual private network



How to configure a LAN Bridge will be described in the next section. For more information on how to configure the other advanced connections, please contact the Option customer support centre.

5.5 LAN Bridge

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.

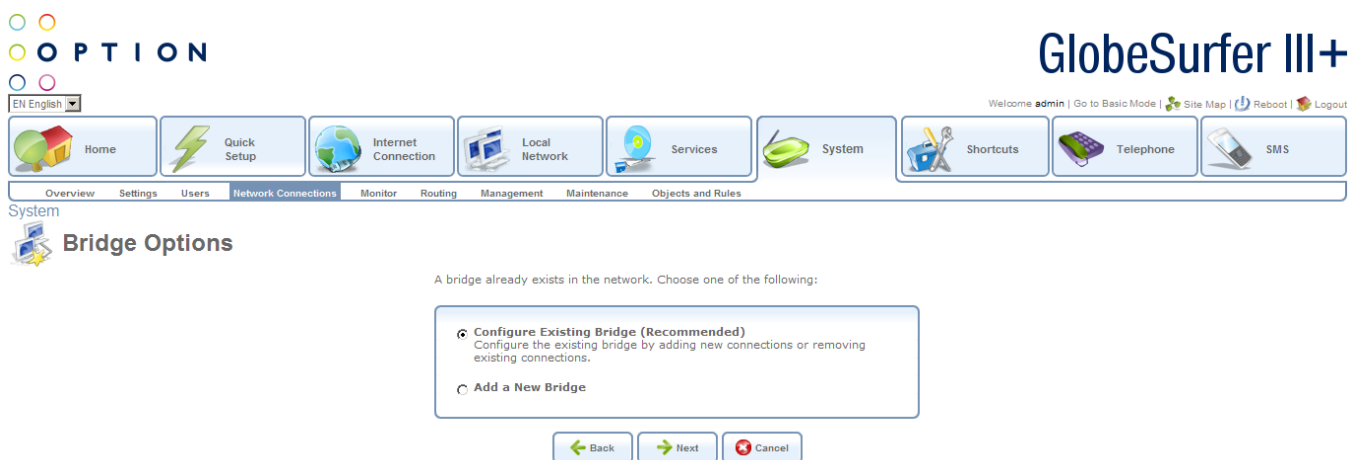
Please note, that when a bridge is removed, its underlying devices inherit the bridge's DHCP settings. For example, the removal of a bridge that is configured as DHCP client automatically configures the LAN devices formerly constituting the bridge as DHCP clients, with the exact DHCP client configuration.

To configure an existing bridge or create a new one, perform the following steps:

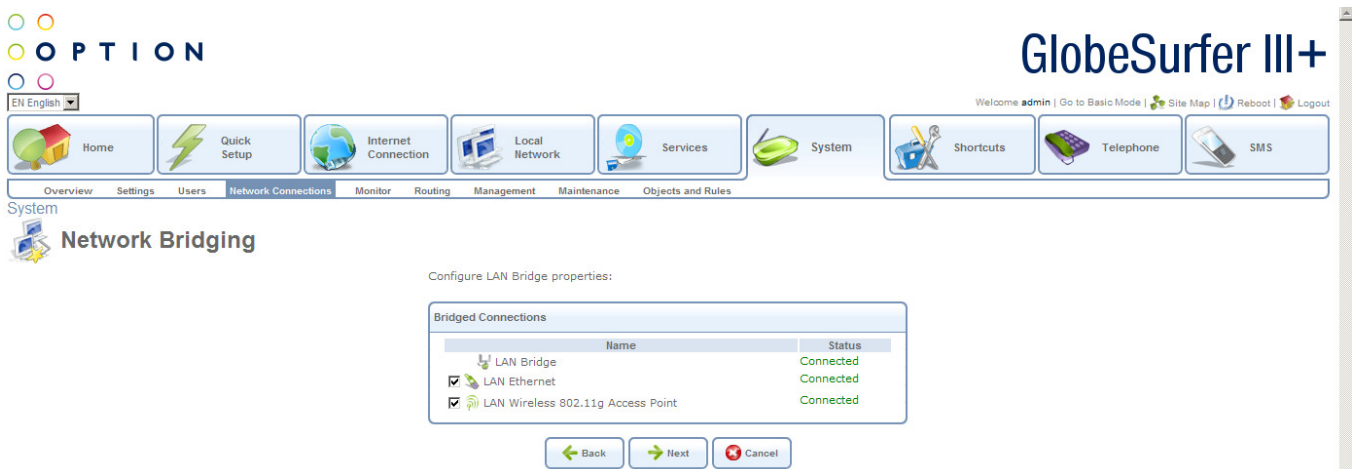
Click the New Connection hyperlink in the Network Connections screen. The Connection Wizard screen will appear.

Select the Advanced Connection radio button and click Next. The Advanced Connection screen will appear.

Select the Network Bridging radio button and click Next. The Bridge Options screen will appear.



Configure Existing Bridge: select this option and click Next. (This option will only appear if a bridge exists). The Network Bridging screen will appear allowing you to add new connections or remove existing ones, by checking or unchecking their respective check boxes. For example, checking the LAN Wireless check box will add the Wireless LAN interface to the existing bridge.



Add a New Bridge: select this option and click Next. A different Network Bridging screen will appear allowing you to add a bridge over the unbridged connections, by checking their respective check boxes.

The screenshot shows the 'Network Bridging' configuration screen in the GlobeSurfer III+ management console. The interface includes a top navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a secondary navigation bar with tabs for Overview, Settings, Users, Network Connections (selected), Monitor, Routing, Management, Maintenance, and Objects and Rules. The main content area is titled 'Network Bridging' and contains a section 'Configure your bridge properties:' with a table titled 'Bridged Connections'.

Name	Status
<input type="checkbox"/> LAN Ethernet	Connected
<input type="checkbox"/> LAN Wireless 802.11g Access Point	Connected

At the bottom of the configuration area are three buttons: 'Back', 'Next', and 'Cancel'.

Important notes:

- The same connections cannot be shared by two bridges.
- A bridge cannot be bridged.
- Bridged connections will lose their IP settings.

Click Next. The Connection Summary screen will appear, corresponding to your changes.

The screenshot shows the 'Connection Summary' screen in the GlobeSurfer III+ management console. The interface is similar to the previous screen, with the 'Network Connections' tab selected. The main content area is titled 'Connection Summary' and contains a message: 'You have successfully completed the steps needed to create the following connection:'.

- Network Bridge
- LAN Ethernet, LAN Wireless 802.11g Access Point will be bridged
- Bridged connections are about to lose their IP settings. If the bridge is removed the connections should be configured
- GlobeSurfer Management Console might lose its connectivity

Below the list is a checkbox labeled 'Edit the Newly Created Connection'.

At the bottom, there is a message: 'Press Finish to create the connection.' and three buttons: 'Back', 'Finish', and 'Cancel'.

Check the Edit the Newly Created Connection check box if you wish to be routed to the new connection's configuration screen after clicking Finish. Click Finish to save the settings.

The new bridge will be added to the network connections list, and will be configurable like any other bridge.

5.5.1.1 General

From the Network Connections screen, if you click on a LAN Bridge connection, you will be routed to the LAN Bridge Properties screen.

From this screen you can click on the tabs at the top left hand side to route to the following detailed screens:

- General – displays an overview of the LAN Bridge
- Settings – allows you to edit general LAN Bridge parameters
- Routing - allows you to set up your gateway to use static or dynamic routing
- Bridging - allows you to specify LAN devices to join under the network bridge
- Advanced - allows you to enable the firewall and add additional IP addresses

The screenshot displays the GlobeSurfer III+ web interface. At the top, there is a navigation bar with tabs: Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a secondary navigation bar with tabs: Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The main content area shows the 'LAN Bridge Properties' dialog box, which is currently open. The dialog box has a 'General' tab selected. It displays various network parameters for the 'LAN Bridge' (br0), including its status (Connected), network type (LAN), and underlying device (LAN Ethernet). It also shows connection statistics such as download and upload rates, MAC address, IP address, subnet mask, and total connection time. At the bottom of the dialog box are three buttons: OK, Apply, and Cancel.

LAN Bridge Properties

Name:	LAN Bridge
Device Name:	br0
Status:	Connected
Network:	LAN
Underlying Device:	LAN Ethernet LAN Wireless 802.11g Access Point
Connection Type:	Bridge
Download Rate:	100 Mbps
Upload Rate:	100 Mbps
MAC Address:	00:0c:e3:65:f6:ac
IP Address:	192.168.1.1 1.1.1.1
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Received bytes:	10.1 [MB]
Sent bytes:	28.7 [MB]
Total connection time:	69:57:22 [hh:mm:ss]
Current connection time:	8:07:29 [hh:mm:ss]

OK Apply Cancel

5.5.1.2 Settings

OPTION

EN English

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance Objects and Rules

System

LAN Bridge Properties

General Settings Routing Bridging Advanced

Device Name: br0
 Status: Connected
 Schedule: Always
 Network: LAN
 Connection Type: Bridge
 Physical Address: 00:0c:e3:65:16:ac
 MTU: Automatic 1500

Internet Protocol: Use the Following IP Address
 IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0

DNS Server: Use the Following DNS Server Addresses
 Primary DNS Server: 0.0.0.0
 Secondary DNS Server: 0.0.0.0

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
 Lease Time in Minutes: 60

The top part of the configuration window displays general communication parameters. It is not recommended to change the default values in this screen unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

You can view and configure the following general connection settings:

- General
- Device Name: name of LAN bridge
- Status: options are:
 - Connected
 - Disconnected
- Schedule: this drop down list contains schedule information, options are:
 - Always
- Network: this drop down list shows the network types, options are:
 - LAN
 - WAN

- DMZ
- Connection Type: this will be Bridge
- Physical Address: the physical address of the network card used for your network. Some cards allow you to change this address.
- MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Options from the drop down list are:
 - Automatic: the gateway will select the best MTU for your Internet connection – this is the default setting
 - Automatic by DHCP: the gateway will select the best MTU by DHCP
 - Manual: this allows you to enter the largest packet size that will be transmitted. The recommended size is 1492. You should leave this value in the 1200 to 1500 range.
- Internet Protocol - please note that according to the selection you make in the Internet Protocol drop down list, the screen will refresh and display relevant configuration settings.
- Internet Protocol drop down list: select one of the following options:
 - No IP Address: select if you require this connection to have no IP address.
 - Obtain an IP Address Automatically: select if you require this connection to try to obtain its IP address from a DHCP server.
 - 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.
 - IP Address: enter the IP address provided by your service provider
 - Subnet Mask: enter the subnet mask
 - DNS Server - please note that according to the selection you make in the DNS Server drop down list, the screen will refresh and display relevant configuration settings.
 - DNS Server drop down list: select one of the following options:
 - No DNS Server: select if you require this connection to have no DNS Server.
- Use the Following DNS Server Addresses: it is possible to specify IP addresses of primary and secondary DNS servers if, for instance, local domain names should be handled by local name servers. Note that for the Cellular WAN interface, DNS servers are configured separately.
 - Primary DNS Server : enter server address
 - Secondary DNS Server: enter server address
- IP Address Distribution - this section allows you to configure the gateway's Dynamic Host Configuration Protocol (DHCP) server parameters. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure your network PCs as DHCP clients.

IP Address Distribution drop down list: select one of the following options:

 - Disabled: select if you would like to assign IP addresses to your network computers statically.

- DHCP Server: select if you are going to provide the range of IP addresses to assign.
- DHCP Relay: your gateway can act as a DHCP relay in case you would like to dynamically assign IP addresses from a DHCP server other than your gateway's DHCP server. Note that when selecting this option you must also change GlobeSurfer® III+'s WAN to work in routing mode.
- Start IP Address: the first IP address that may be assigned to a LAN host. Since the gateway's default IP address is 192.168.1.1, this address must be 192.168.1.2 or greater.
- End IP Address: the last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.
- Subnet Mask: a mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.0.0.
- Lease Time in Minutes: each device will be assigned an IP address by the DHCP server for this amount of 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, 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: click this checkbox if you would like the gateway to assign a host name automatically for the DHCP client if it doesn't have one
- New IP Address hyperlink: this will appear on the screen if DHCP Relay has been chosen.

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

If DHCP Relay has been chosen, click the New IP Address link. The DHCP Relay Server Address screen will appear:

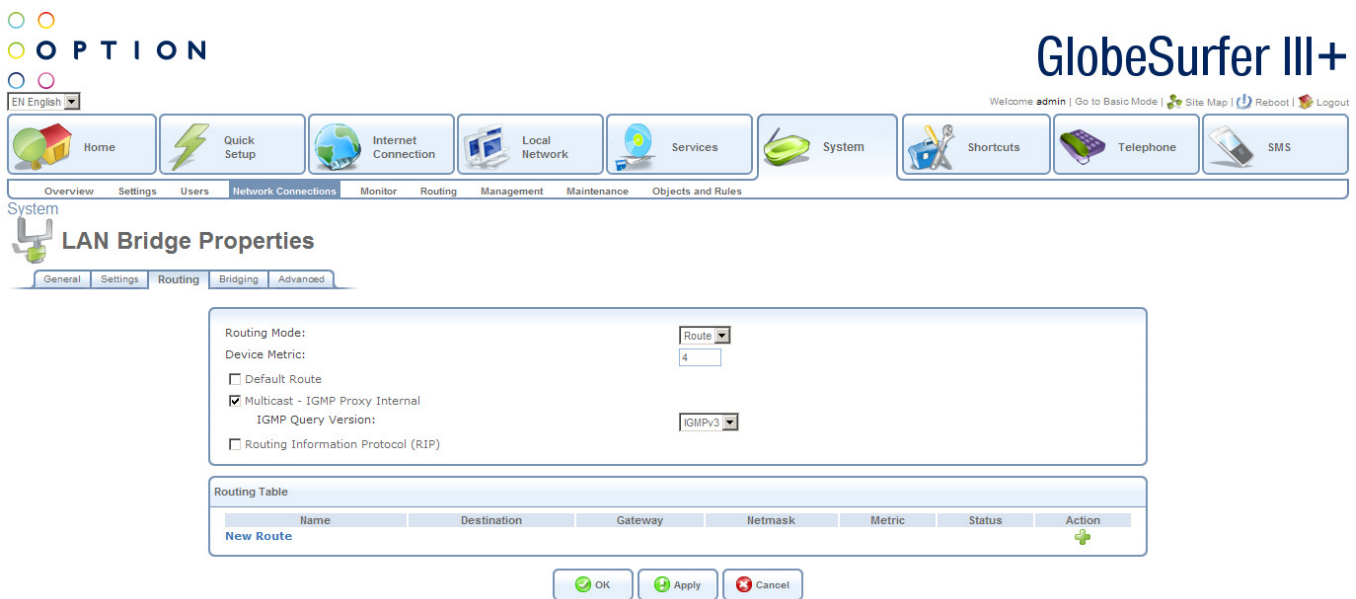
The screenshot shows the 'DHCP Relay Server Address' configuration page. At the top, there's a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-menu bar with links like Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The main title 'DHCP Relay Server Address' is displayed with a gear icon. The central part of the screen features a text input field labeled 'IP Address:' followed by a numeric keypad with digits 0-9. At the bottom, there are two buttons: 'OK' with a green checkmark and 'Cancel' with a red X.

IP Address: specify the IP address of the DHCP server.

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.5.1.3 Routing



You can choose to setup your gateway 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.

Device Metric: the device metric is a value used by the gateway 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.

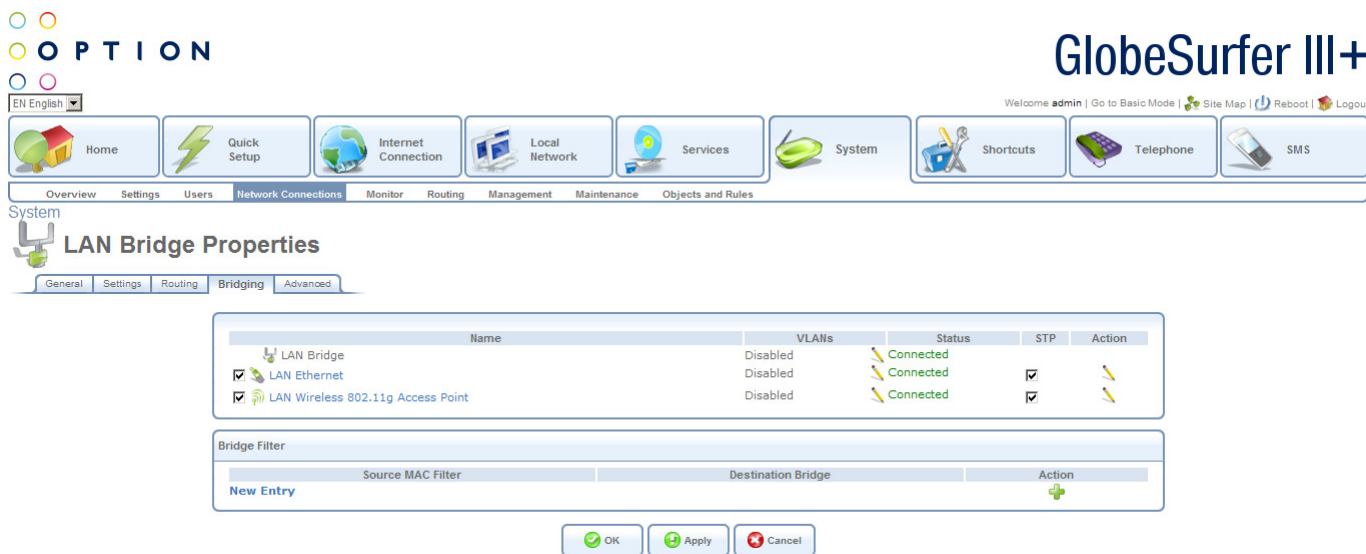
Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

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. Use the New Route button to add a route or edit existing routes.

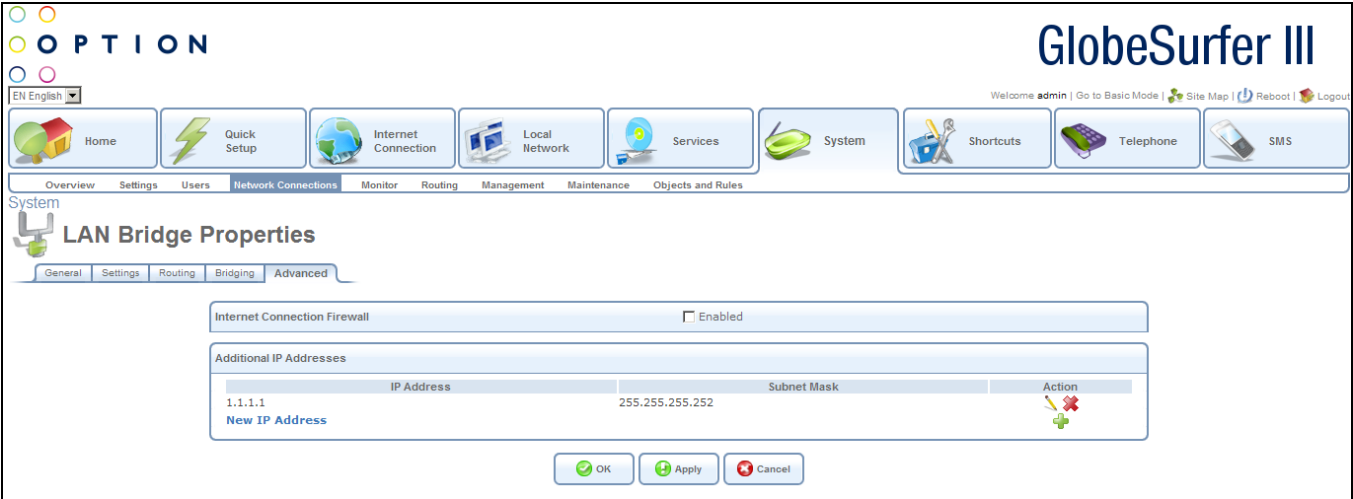
5.5.1.4 Bridging



The bridge section allows you to specify the LAN devices that you would like to join under the network bridge.

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 gateway.

5.5.1.5 Advanced



Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection.

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

You can add alias names (additional IP addresses) to the gateway by clicking the New IP Address link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1.

5.5.2 LAN Ethernet

A LAN Ethernet connection connects computers to GlobeSurfer® III+ using Ethernet cables, either directly or via network hubs and switches.

Note that available configuration options may vary depending on if the LAN Ethernet interface is part of a bridge or not.

5.5.2.1 General

The screenshot shows the GlobeSurfer III web interface. The top navigation bar includes links for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. The main menu includes Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The 'System' section is active, displaying 'LAN Ethernet Properties'. The 'General' tab is selected, showing the following information:

Name:	LAN Ethernet
Device Name:	bcm0.1
Status:	Connected
Network:	LAN
Connection Type:	Ethernet
Download Rate:	100 Mbps
Upload Rate:	100 Mbps
MAC Address:	00:0c:e3:65:f6:ac
IP Address Distribution:	Disabled
Received bytes:	0.0 [MB]
Sent bytes:	1.6 [MB]
Total connection time:	70:27:45 [hh:mm:ss]
Current connection time:	8:37:52 [hh:mm:ss]

At the bottom of the window are three buttons: OK, Apply, and Cancel.

5.5.2.2 Settings

The screenshot shows the same GlobeSurfer III web interface, but the 'Settings' tab is selected in the 'LAN Ethernet Properties' window. The settings are as follows:

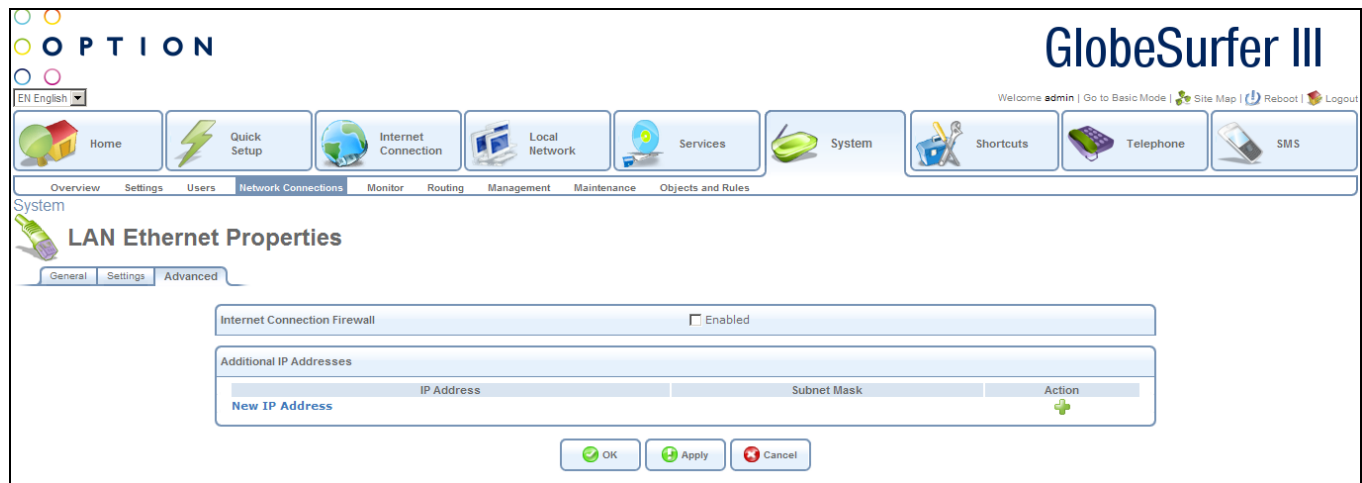
Device Name:	bcm0.1
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Ethernet
Physical Address:	00:0c:e3:65:f6:ac
MTU:	Automatic 1500

At the bottom of the window are three buttons: OK, Apply, and Cancel.

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 gateway 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. Manual, allows you to enter the largest packet size that will be transmitted. The recommended size is 1492. You should leave this value in the 1200 to 1500 range. To have the gateway select the best MTU for your Internet connection, select Automatic (default setting).

5.5.2.3 Advanced



Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection.

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

You can add alias names (additional IP addresses) to the gateway by clicking the New IP Address link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1.

5.5.3 LAN Wireless

The LAN Wireless interface in the GlobeSurfer® III+ provides wireless connectivity for IEEE 802.11b/g equipped WLAN clients. GlobeSurfer® III+ integrates multiple layers of security. These include the IEEE 802.1x port based authentication protocol, RADIUS client, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Wi-Fi Protected Access (WPA) and industry leading GlobeSurfer® III+ Firewall and VPN applications. In addition, GlobeSurfer III+'s built-in authentication server enables home/SOHO users to define authorized wireless users without the need for an external RADIUS server.

To configure the LAN Wireless connection:

Click the Network Connections tab, the Network Connections screen will appear. Click the wireless connection link (or its Edit action button) to view its properties. The LAN Wireless Properties screen will appear.

5.5.3.1 General

The screenshot shows the 'General' tab of the 'LAN Wireless 802.11g Access Point Properties' configuration window. The interface includes a top navigation bar with 'OPTION' and 'GlobeSurfer III' branding, and a secondary bar with various system icons. The main content area displays the following configuration details:

Name:	LAN Wireless 802.11g Access Point
Device Name:	eth0
Status:	Connected
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Download Rate:	54 Mbps
Upload Rate:	54 Mbps
MAC Address:	00:0c:e3:65:f6:ab
IP Address Distribution:	Disabled
Encryption:	Disabled
Received bytes:	11.4 [MB]
Sent bytes:	35.3 [MB]
Total connection time:	71:31:46 [hh:mm:ss]
Current connection time:	9:13:53 [hh:mm:ss]

At the bottom of the configuration window are three buttons: 'OK', 'Apply', and 'Cancel'.

5.5.3.2 Settings

The screenshot shows the 'Settings' tab of the 'LAN Wireless 802.11g Access Point Properties' configuration window. The interface is identical to the previous one, but the configuration details are as follows:

Device Name:	eth0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Physical Address:	00:0c:e3:65:f6:ab
MTU:	Automatic

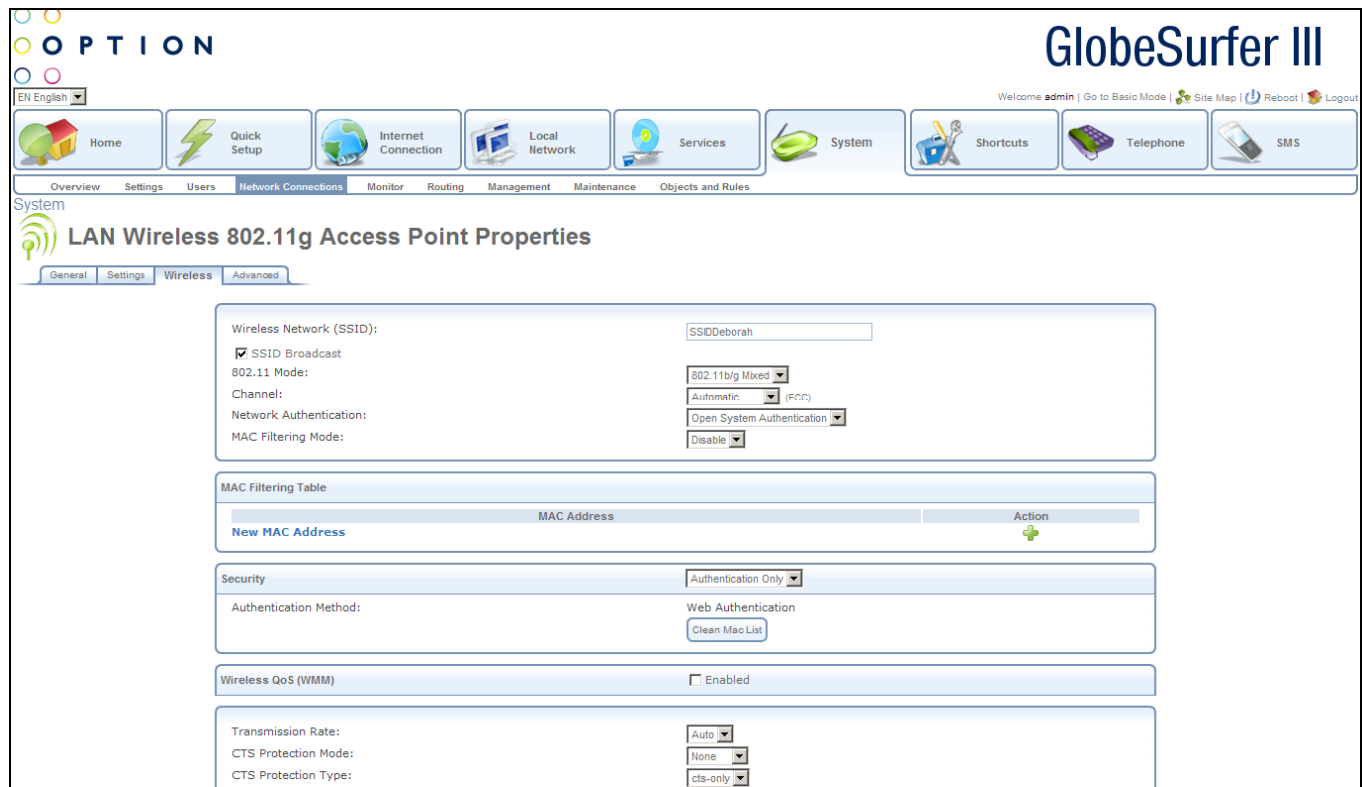
At the bottom of the configuration window are three buttons: 'OK', 'Apply', and 'Cancel'.

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 gateway 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. Manual, allows you to enter the largest packet size that will be transmitted. The recommended size is 1492. You should leave this value in the 1200 to 1500 range. To have the gateway select the best MTU for your Internet connection, select Automatic (default setting).

5.5.3.3 Wireless



OPTION

Welcome **admin** | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users **Network Connections** Monitor Routing Management Maintenance Objects and Rules

LAN Wireless 802.11g Access Point Properties

General Settings **Wireless** Advanced

Wireless Network (SSID):

☒ SSID Broadcast

802.11 Mode:

Channel: (FCC)

Network Authentication:

MAC Filtering Mode:

MAC Address	Action
New MAC Address	+

Security:

Authentication Method:

[Clean Mac List](#)

Wireless QoS (WMM) ☐ Enabled

Transmission Rate:

CTS Protection Mode:

CTS Protection Type:

The wireless access point settings are:

5.5.3.3.1 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 to a unique name.

5.5.3.3.2 SSID Broadcast

Select this check box to enable the SSID's broadcast. SSID broadcast is used in order to hide the name of the AP (SSID) from clients that should not be aware to its existence.

5.5.3.3.3 802.11 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.

5.5.3.3.4 Channel

Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on different channels in order to function correctly.

5.5.3.3.5 Frame Burst

Frame Bursting is a method to increase the speed of 802.11g-based wireless networks by unwrapping short 802.11g packets and re-bundling them into a larger packet to reduce the impact of mandatory gaps

between packets. If you are experiencing problems with your wireless connection, try to disable Frame Burst.

5.5.3.3.6 Network Authentication

The WPA network authentication method is Open System Authentication, meaning that a network key is not used for authentication. When using the 802.1X WEP or Non-802.1X WEP security protocols, this field changes to a combo box, offering the Shared Key Authentication method (which uses a network key for authentication), or both methods combined.

5.5.3.3.7 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® III+ automatically use the fastest possible data transmission rate.

5.5.3.3.8 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 gateway and Wireless-G products.

5.5.3.3.9 CTS Protection Type

CTS Protection Type defines if the CTS Protection Mode defined above should use CTS only or both RTS/CTS.

5.5.3.3.10 Beacon Interval

A beacon is a packet broadcast by GlobeSurfer® III+ to synchronize the wireless network. The Beacon Interval value indicates how often the beacon is sent.

5.5.3.3.11 DTIM Interval

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

5.5.3.3.12 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.

5.5.3.3.13 RTS Threshold

GlobeSurfer® III+ 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 preset threshold, the RTS/CTS mechanism is not active. If you encounter inconsistent data flow, try a minor reduction of the RTS threshold size.

5.5.3.3.14 MAC Filtering Mode

You can filter wireless users according to their MAC address, either allowing or denying access. Choose the action to be performed by selecting it from the drop down menu. Then use the MAC Filtering Settings option to add and remove MAC Addresses to the list of allowed or denied clients.

To configure your wireless security, enable this feature by checking its Enabled check-box on the Configure LAN Wireless Access Point screen. The screen will refresh, displaying the wireless security options. Click Apply to if you wish to save this change.

5.5.3.3.15 Stations Security Type

Select the type of security protocol for securing your wireless network. Choose between WPA, WPA2, WPA and WPA2, 802.1X WEP, and Non-802.1X WEP. The screen will refresh, presenting each protocol's configuration respectively.

WPA - a data encryption method for 802.11 wireless LANs.

Authentication Method:

Select the authentication method you would like to use. You can 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 the Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES) for the encryption algorithm. Group Key Update Interval defines the time interval in seconds for updating a group key.

WPA2 – an enhanced version of WPA, and defines the 802.11i protocol.

Authentication Method:

Select the authentication method you would like to use. You can 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:

The encryption algorithm used for WPA2 is the Advanced Encryption Standard (AES). Group Key Update Interval defines the time interval in seconds for updating a group key.

WPA and WPA2 Mixed Mode – a mixed data encryption mode.

Authentication Method:

Select the authentication method you would like to use. You can 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:

The encryption algorithm used for WPA and WPA2 is either the Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES). Group Key Update Interval defines the time interval in seconds for updating a group key.

- 802.1X WEP - a data encryption method utilizing a statically or automatically defined key for wireless clients that use 802.1X for authentication and WEP for encryption. You may define up to four keys but use only one at a time.

Generate Keys:

Automatically select this option to generate the encryption keys automatically rather than entering them manually. The screen will refresh, hiding the table of keys described below.

Group Key Update Interval:

Defines the time interval in seconds for updating a group key. Active Select the encryption key to be activated. Encryption Key Type the encryption key until the entire field is filled. The key cannot be shorter than the field's length.

Format:

Select the character type for the key: Hex or ASCII.

Key Length:

Select the key length in bits: 40 or 104 bits.

5.5.3.3.16 DHCP Relay

Your gateway can act as a DHCP relay in case you would like to dynamically assign IP addresses from a DHCP server other than your gateway's DHCP server. Note that when selecting this option you must also change GlobeSurfer® III+'s WAN to work in routing mode.

After selecting DHCP Relay from the drop down menu, a New IP Address link will appear

Click the New IP Address link. The DHCP Relay Server Address screen will appear:

Specify the IP address of the DHCP server.

Click OK to save the settings.

Disabled:

Select Disabled from the combo-box if you would like to statically assign IP addresses to your network computers.

You can choose to setup your gateway 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.

5.5.3.3.17 Device Metric

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

5.5.3.3.18 Default Route

Select this check box to define the GlobeSurfer as the default route to other networks including the Internet.

5.5.3.3.19 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.

5.5.3.3.20 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. Use the New Route button to add a route or edit existing routes.

5.5.3.4 Advanced

Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection.

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

You can add alias names (additional IP addresses) to the gateway by clicking the New IP Address link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1.

5.5.4 WAN Cellular

The WAN Cellular connection connects the GlobeSurfer® III+ to the Internet and other networks through the GSM and UMTS mobile telecommunications standards. The WAN Cellular Properties screen displays a summary of the connection properties.

5.5.4.1 General

The screenshot shows the 'WAN Cellular Properties' window with the 'General' tab selected. The window has a title bar with 'OPTION' and 'GlobeSurfer III'. Below the title bar is a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. The main content area displays the following information:

Name:	WAN Cellular
Device Name:	eth1
Status:	Status working
Network:	WAN
Connection Type:	Cellular
IP Address:	10.34.68.204
Subnet Mask:	255.255.255.0
DNS Server:	149.254.201.126 149.254.192.126
Access point name:	general.t-mobile.uk
Operator:	T-Mobile
Signal strength:	Low (-97 dBm)
Connection status:	Connected
Received bytes:	5.5 [MB]
Sent bytes:	7.4 [MB]
Total connection time:	72:17:10 [hh:mm:ss]
Current connection time:	10:29:18 [hh:mm:ss]

Buttons at the bottom include 'Disconnect', 'OK', 'Apply', and 'Cancel'.

5.5.4.2 Settings

The screenshot shows the 'WAN Cellular Properties' window with the 'Settings' tab selected. The window has a title bar with 'OPTION' and 'GlobeSurfer III'. Below the title bar is a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. The main content area displays the following settings:

Device Name:	eth1
Status:	Status working
Schedule:	Always
Network:	WAN
Connection Type:	Cellular
MTU:	Automatic 1500

Internet Protocol section:

☐ Override Subnet Mask

DNS Server section:

Obtain DNS Server Address Automatically

UMTS section:

Access point name:	general.t-mobile.uk
Network Authentication:	None
Login User Name (case sensitive):	
Login Password:	
Network type:	Automatic
UMTS connect method:	<input checked="" type="radio"/> Connect Manually <input type="radio"/> Automatically connect upon traffic <input type="radio"/> Always connected

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 gateway is configured to operate with the default values, no parameter modification is necessary. You can configure the following general connection settings:

MTU: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Manual, allows you to enter the largest packet size that will be transmitted. The recommended size is 1492. You should leave this value in the 1200 to 1500 range. To have the gateway select the best MTU for your Internet connection, select Automatic (default setting).

It is possible to specify IP addresses of primary and secondary DNS servers if for instance local domain names should be handled by local name servers. Note that for the Cellular WAN interface, DNS servers are configured separately.

If the Internet Protocol setting mentioned above is set to Obtain an IP address automatically, then there is also an option to configure the DNS Server setting to obtain DNS Server settings automatically.

5.5.4.3 Routing

The screenshot shows the 'WAN Cellular Properties' configuration window with the 'Routing' tab selected. The 'Routing Mode' is set to 'NAPT' and the 'Device Metric' is set to '20'. The 'Default Route' checkbox is checked, while 'Multicast - IGMP Proxy Default' and 'Routing Information Protocol (RIP)' are unchecked. Below these settings is a 'Routing Table' section with a table header: Name, Destination, Gateway, Netmask, Metric, Status, and Action. A 'New Route' link is present below the table. At the bottom of the window are 'OK', 'Apply', and 'Cancel' buttons.

You can choose to setup your gateway 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 modes: Route Use route mode if you want your GlobeSurfer® III+ to function as a router between two networks.

5.5.4.3.1 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.

5.5.4.3.2 Device Metric

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

5.5.4.3.3 Default Route

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

5.5.4.3.4 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.

5.5.4.3.5 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. Use the 'New Route' button to add a route or edit existing routes.

5.5.4.4 Advanced

The screenshot displays the 'WAN Cellular Properties' configuration page in the 'Routing' tab. The 'Routing Mode' is set to 'NAPT'. The 'Device Metric' is set to '20'. The 'Default Route' checkbox is checked. The 'Multicast - IGMP Proxy Default' and 'Routing Information Protocol (RIP)' checkboxes are unchecked. Below these settings is a 'Routing Table' section with a table header: Name, Destination, Gateway, Netmask, Metric, Status, and Action. A 'New Route' button is located at the bottom left of the table. At the bottom of the page are 'OK', 'Apply', and 'Cancel' buttons.

Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection.

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

5.5.5 Configuring your Windows XP clients

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

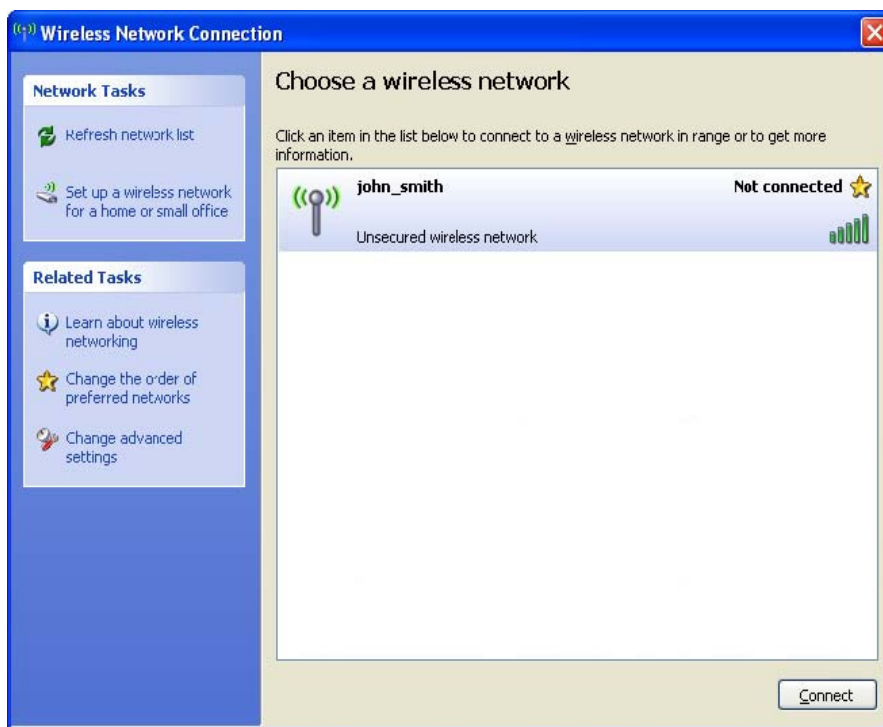
Note: The following description and images are in accordance with Microsoft® Windows® XP, Version 2002, running Service Pack 2.

Open your Network Connections window from Window®'s Control Panel.

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® III+'s wireless connection. Note that the connection's status is "Not connected" and defined as Unsecured wireless network.

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





An icon will appear in the notification area, announcing the successful initiation of the wireless connection.



You can now use GlobeSurfer® III+'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. Such a user has access to any disk shares available in your network. To prevent this scenario, the next logical step is to secure your wireless network, allowing only specific users to connect.

5.6 Monitor

Access GlobeSurfer® III+'s monitoring settings by clicking the Monitor tab in the System area.

From this screen you can click on the tabs at the top right hand side to route to the following detailed screens:

- Network
- CPU
- Log

5.6.1 Network Connection

To access the Network Connections screen, click the Network tab at the top right hand side of the Monitor screen in the System area.

Name	LAN Bridge	LAN Ethernet	LAN Wireless 802.11g Access Point	WAN Cellular
Device Name	br0	bcm0.1	eth0	eth1
Status	Connected	Connected	Connected	Status working
Network	LAN	LAN	LAN	WAN
Underlying Device	LAN Ethernet			
	LAN Wireless 802.11g Access Point			
Connection Type	Bridge	Ethernet	Wireless 802.11g Access Point	Cellular
Download Rate	100 Mbps	100 Mbps	54 Mbps	
Upload Rate	100 Mbps	100 Mbps	54 Mbps	
MAC Address	00:0c:e3:65:f6:ac	00:0c:e3:65:f6:ac	00:0c:e3:65:f6:ab	
IP Address	192.168.1.1			10.34.68.204
	1.1.1.1			
Subnet Mask	255.255.255.0			255.255.255.0
DNS Server				149.254.201.126
				149.254.192.126
IP Address Distribution	DHCP Server	Disabled	Disabled	
Encryption			Disabled	
Access point name				general.t-mobile.uk
Operator				T-Mobile
Signal strength				Low (-97 dBm)
Connection status				Connected
Received bytes	44.4 [MB]	0.0 [MB]	49.1 [MB]	33.1 [MB]
Sent bytes	150.7 [MB]	10.8 [MB]	174.3 [MB]	17.5 [MB]
Received Packets	354610	0	354610	11023
Sent Packets	182628	127864	495384	65684
Received bytes	46546027	0	51510735	34668685
Sent bytes	157986628	11372089	182762177	18394154
Receive Errors	0	0	0	0
Receive Drops	0	0	0	0
Total connection time	61:22:46 [hh:mm:ss]	61:22:47 [hh:mm:ss]	61:50:46 [hh:mm:ss]	61:20:46 [hh:mm:ss]
Current connection time	61:20:24 [hh:mm:ss]	61:20:24 [hh:mm:ss]	61:20:24 [hh:mm:ss]	61:20:15 [hh:mm:ss]

This screen displays a table summarizing the monitored connection data. GlobeSurfer® III+ constantly monitors traffic within the local network and between the local network and the Internet. You can view statistical information about data received from and transmitted to the Internet (WAN) and to computers in the local network (LAN).

Click on the LAN Bridge hyperlink to be routed to the LAN Bridge Properties screen in the Network Connections tab in the System area

Click on the LAN Ethernet hyperlink to be routed to the LAN Ethernet Properties screen in the Network Connections tab in the System area

Click on the LAN Wireless 802.11g Access Point hyperlink to be routed to the LAN Wireless 802.11g Access Point Properties screen in the Network Connections tab in the System area

Click on the WAN Cellular hyperlink to be routed to the WAN Cellular Properties screen in the Network Connections tab in the System area

Click on the IP Address Distribution hyperlink to be routed to the IP Address Distribution screen in the Network Connections tab in the Services

Press the Close button to go to the Home screen.

Press the Automatic Refresh Off button to keep the screen as it is and not constantly update.

Press the Automatic Refresh On button to constantly update the displayed parameters.

Press the Reset Statistics button to reset the Received bytes (MB), Sent bytes (MB), Received Packets, Sent Packets, Received bytes, Sent bytes, Receive Errors, Receive Drops and Current connection time fields to zero.

Press the Refresh button to update the display manually.

5.6.2 CPU

To access the CPU screen, click the CPU tab at the top right hand side of the Monitor screen in the System area.

The screenshot shows the GlobeSurfer III web interface. The top navigation bar includes links for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. The 'Monitor' tab is selected, and the 'CPU' sub-tab is active. The main content area displays system uptime and load average, gateway ID, and a table of running processes with their memory usage.

System Has Been Up For: 2 days, 13 hours
Load Average (1 / 5 / 15 mins.): 0.24 / 0.26 / 0.29

Gateway ID: 000CE365F6AB

Process	Total Virtual Memory (VmData)	Heap size (VmSize)
init	532 kB	1252 kB
openrg	5248 kB	13592 kB
l2tpd	788 kB	1540 kB
pluto	1120 kB	2480 kB
smbd	1872 kB	6516 kB
smbd	1872 kB	6516 kB
nmdbd	1508 kB	3260 kB
_pluto_adns	1032 kB	1924 kB

At the bottom of the screen, there are three buttons: Close, Automatic Refresh On, and Refresh.

This screen shows various details of all the processes in the system and the current uptime.

Press the Close button to go to the Home screen.

Press the Automatic Refresh Off button to keep the screen as it is and not refresh automatically.

Press the Automatic Refresh On button to enable the screen to be refreshed automatically at regular intervals.

Press the Refresh button to refresh the screen manually.

5.6.3 System Log

To access the System Log screen, click the Log tab at the top right hand side of the Monitor screen in the System area.

The screenshot shows the 'System Log' interface in the GlobeSurfer III web management system. At the top, there's a navigation bar with various system management tabs. Below this, the 'System Log' section is active, showing a table of log entries. The table has four columns: 'Time', 'Component', 'Severity', and 'Details'. The log entries show various system events, including warnings and information messages. A filter section is located above the table, allowing users to select a component and severity level. Buttons for 'Close', 'Clear Log', 'Download Log', and 'Refresh' are present at the top of the log area.

Time	Component	Severity	Details
Jul 30 21:30:18 2008	LibJutil	Warning	sys_if_ioctl_mi_execute:470: Both tried MII ioctl 8947/89F0 failed: Operation not supported. [repeated 56 times, last time on Jul 30 21:59:28 2008]
Jul 30 21:29:30 2008	IGMP	Information	Adding multicast group 239.255.255.250 to device br0 port 0
Jul 30 21:29:30 2008	IGMP	Information	Adding multicast group 224.0.0.103 to device br0 port 0
Jul 30 21:29:17 2008	Web-Based Management	Notice	Cannot resolve AJAX server host www.jungo.net
Jul 30 21:29:07 2008	LibJutil	Warning	sys_if_ioctl_mi_execute:470: Both tried MII ioctl 8947/89F0 failed: Operation not supported. [repeated 4 times, last time on Jul 30 21:29:07 2008]
Jul 30 21:27:33 2008	IGMP	Information	Removing multicast group 239.255.255.250 from device br0 port 0
Jul 30 21:01:48 2008	IGMP	Information	Removing multicast group 224.0.0.103 from device br0 port 0
Jul 30 19:11:20 2008	Kernel	Notice	opening uses obsolete (PF_INET, SOCK_PACKET)
Jul 30 19:11:20 2008	LibJutil	Information	estream_connect_done 69: connection failed
Jul 30 19:11:20 2008	LibJutil	Information	estream_connect_done 69: connection failed
Jul 30 19:11:20 2008	LibJutil	Information	estream_connect_done 67: connection failed
Jul 30 19:11:20 2008	LibJutil	Information	estream_connect_done 66: connection failed
Jul 30 19:11:20 2008	LibJutil	Information	estream_connect_done 64: connection failed
Jul 30 18:09:28 2008	IGMP	Information	Adding multicast group 239.255.255.250 to device br0 port 0

This screen displays the system log. Filters on the log are displayed and can be added, modified and deleted. For each filter the following data is shown:

Component: components the filter applies to: choose from the drop down list

Severity: events of this severity or higher will appear in the log: choose from the drop down list:

- None
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information
- Debug
- Action: add, modify or delete

Click the New Filter hyperlink to add a new filter.

Press the Apply Filters button to apply the filters you have set up, to the log.

Press the Reset Filters button to delete all filters.

For each log entry the following data is shown:

- Time: date and time stamp
- Component: area of system where event happened
- Severity: level of severity of log entry
- Details: description of log entry. Warnings are shown in orange. Errors are shown in red.

Press the Close button to go to the Home screen.

Press the Clear Log button to delete all the log entries.

Press the Download log button to save the log to an Excel spreadsheet.

Press the Refresh button to update the data.

5.7 Routing

Access GlobeSurfer® III+'s routing settings by clicking the Routing tab in the System area.

From this screen you can click on the tabs at the top right hand side to route to the following detailed screens:

- General
- BGP and OSPF
- PPoE Relay

5.7.1 General/Routing

To access the General/Routing screen, click the General tab at the top right hand side of the Routing screen in the System area.

OPTION

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor **Routing** Management Maintenance Objects and Rules

Routing

General BGP and OSPF PPPoE Relay

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

Routing Information Protocol (RIP) ☐ Enabled

☐ Poison Reverse

☐ Do not Advertise Direct Connected Routes

Internet Group Management Protocol (IGMP) ☒ Enabled

☒ IGMP Fast Leave

☐ IGMP Multicast to Unicast

Domain Routing (add route entry according to interface from which DNS record is received) ☐ Enabled

OK Apply Cancel

For each route the following data is displayed:

- Name: the type of network device (LAN Bridge or WAN Cellular).
- 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.
- Gateway: the IP address of the GlobeSurfer® III+.
- Netmask: the network mask is used in conjunction with the destination to determine when a route is used.
- 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.
- Status
- Action: add, modify or delete

You can add, edit and delete routing rules from the routing table in the manner described in section **Error! Reference source not found..**

Click the New Route icon to go to the Route Settings screen

The following data can be modified:

Routing Information Protocol (RIP): select this checkbox in order to enable connections previously defined to use RIP. If this checkbox is not selected, RIP will be disabled for all connections, including those defined to use RIP.

Poison Reverse: select this checkbox set Poison Reverse

Do not Advertise Direct Connected Routes: select this checkbox if you do not wish to advertise direct connected routes

Internet Group Management Protocol (IGMP): GlobeSurfer® III+ 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 may be useful when connected to the Internet through a router. When an application running on a LAN computer sends out a request to join a multicast group, GlobeSurfer® III+ will listen and intercept this group's messages, sending them to the subscribed application. Select this checkbox to enable this feature.

IGMP Fast Leave: select this checkbox to set IGMP Fast Leave

IGMP Multicast to Unicast: select this checkbox to set IGMP Multicast to Unicast

Domain Routing: when GlobeSurfer® III+'s DNS server receives a reply from an external DNS server, it will add a routing entry for the IP address of the reply through the device from which it arrived. This means that future packets from this IP address will be routed through the device from which the reply arrived. Select the checkbox to enable domain routing.

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.7.1.1 Route Settings

The screenshot displays the 'Route Settings' configuration page in the GlobeSurfer III web interface. The top navigation bar includes icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Settings, Users, Network Connections, Monitor, Routing (selected), Management, Maintenance, and Objects and Rules. The main content area is titled 'Route Settings' and contains a form with the following fields:

- Name: A dropdown menu currently set to 'LAN Bridge'.
- Destination: A text input field containing '0.0.0.0'.
- Netmask: A text input field containing '255.255.255.255'.
- Gateway: A text input field containing '0.0.0.0'.
- Metric: A text input field containing '0'.

At the bottom of the form are two buttons: 'OK' and 'Cancel'.

When adding a routing rule, you need to specify:

- **Name:** select the type of network device (LAN Bridge or WAN Cellular).
- **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® III+.
- **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.

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.7.2 BGP and OSPF

To access the BGP and OSPF screen, click the BGP and OSPF tab at the top right hand side of the Routing screen in the System area.

The screenshot displays the 'BGP and OSPF' configuration page in the GlobeSurfer III+ web interface. The page is organized into three main configuration sections, each with a 'Set Default Values' button and a text area for configuration commands.

- Border Gateway Protocol (BGP):** This section is checked as 'Enabled'. The configuration file contains the commands:


```
router bgp <AS number>
log syslog
```
- Open Shortest Path First (OSPF):** This section is also checked as 'Enabled'. The configuration file contains the commands:


```
router ospf
log syslog
```
- Zebra (required for BGP and OSPF):** This section is for Zebra configuration. The configuration file contains the commands:


```
interface eth1
log syslog
```

At the bottom of the page, there are three buttons: 'OK', 'Apply', and 'Cancel'.

The following data can be modified:

- **Border Gateway Protocol (BGP):** select this checkbox to enable BGP, then enter:
- **BGP Configuration File:** by clicking on the Set Default Value button
- **Zebra Configuration File:** by clicking on the Set Default Value button
- **Open Shortest Path First (OSPF):** select this checkbox to enable OSPF, then enter:
- **OSPF Configuration File:** by clicking on the Set Default Value button

- Zebra Configuration File: by clicking on the Set Default Value button

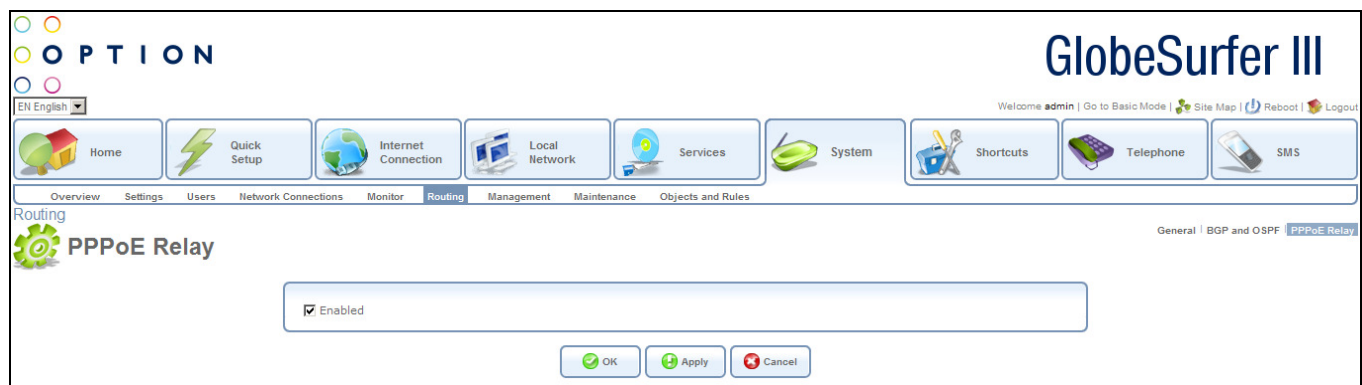
Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.7.3 PPPoE Relay

To access the PPPoE screen, click the PPPoE tab at the top right hand side of the Routing screen in the System area.



The following data can be modified:

Point-to-Point Protocol over Ethernet (PPPoE): select this checkbox to enable PPPoE. This is a specification for connecting users on an Ethernet network to the Internet by using a broadband connection (typically through a DSL modem).

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.8 Management

Access GlobeSurfer® III+'s management settings by clicking the Management tab in the System area.

From this screen you can click on the tabs at the top right hand side to route to the following screens:

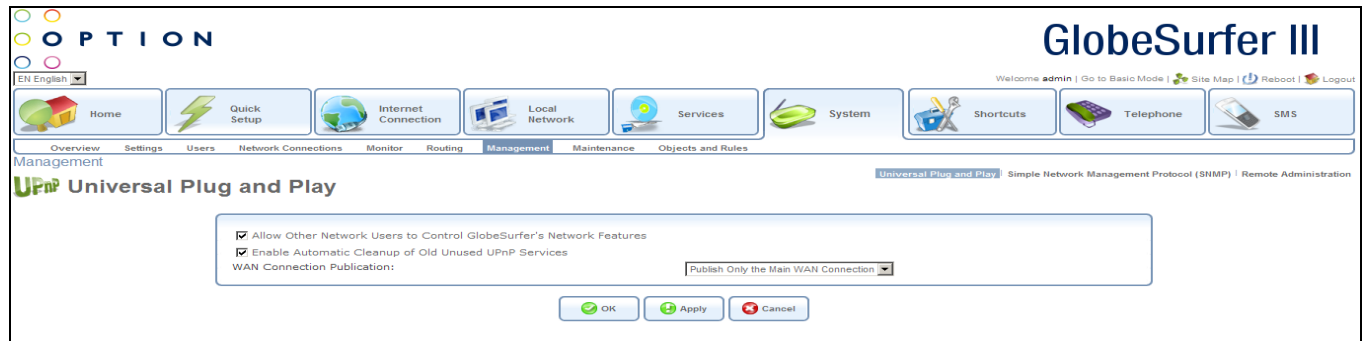
Universal Plug and Play

Simple Network Management Protocol (SNMP)

Remote Administration

5.8.1 Universal Plug and Play

To access the UPnP screen, click the Universal Plug and Play tab at the top right hand side of the Management screen in the System area.



The following data can be modified:

Allow Other Network Users to Control GlobeSurfer® III+'s Network Features: select this checkbox to enable the UPnP feature. This will enable you to define UPnP services on any LAN host.

Enable Automatic Cleanup of Old Unused UPnP Services: select this 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 that 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 the case where the limit might 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 services that are no longer valid and will remove them, preventing services exhaustion.

WAN Connection Publication: select an option from the drop down list:

- Publish Only the Main WAN Connection
- Publish All WAN Connections

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.8.2 Simple network Management Protocol (SNMP)

To access the SNMP screen, click the Simple Network Management Protocol tab at the top right hand side of the Management screen in the System area.

SNMP enables network management systems to remotely configure and monitor GlobeSurfer® III+. Your Internet service provider (ISP) may use SNMP in order to identify and resolve technical problems. Your ISP should provide technical information regarding the properties of GlobeSurfer® III+'s SNMP agent.

The following SNMP parameters can be modified, as provided by your Internet service provider:

- Enabled: select this checkbox to enable SNMP
- Allow Incoming WAN Access to SNMP: select this checkbox to allow incoming WAN access
- SNMP community strings are passwords used in SNMP messages between the management system and GlobeSurfer® III+.
- Read-Only Community Name: a read-only community allows the manager to monitor GlobeSurfer® III+.
- Read-Write Community Name: a read-write community allows the manager to both monitor and configure GlobeSurfer® III+.
- Trusted Peer: enter the IP address, or subnets of addresses, that identify which remote management stations are allowed to perform SNMP operations on GlobeSurfer® III+, choose one of the following from the drop down list:
 - Any Address
 - Specify an IP Address
 - Specify a Subnet
- SNMP Traps: messages sent by GlobeSurfer® III+ to a remote management station, in order to notify the manager about the occurrence of important events or serious conditions. GlobeSurfer® III+ supports both SNMP version 1 and SNMP version 2c traps.
- Enabled: select this checkbox to enable SNMP traps, and then enter:
 - Version: select one of the following from the drop down list:
 - SNMP v1
 - SNMP v2c
 - Destination
 - Community

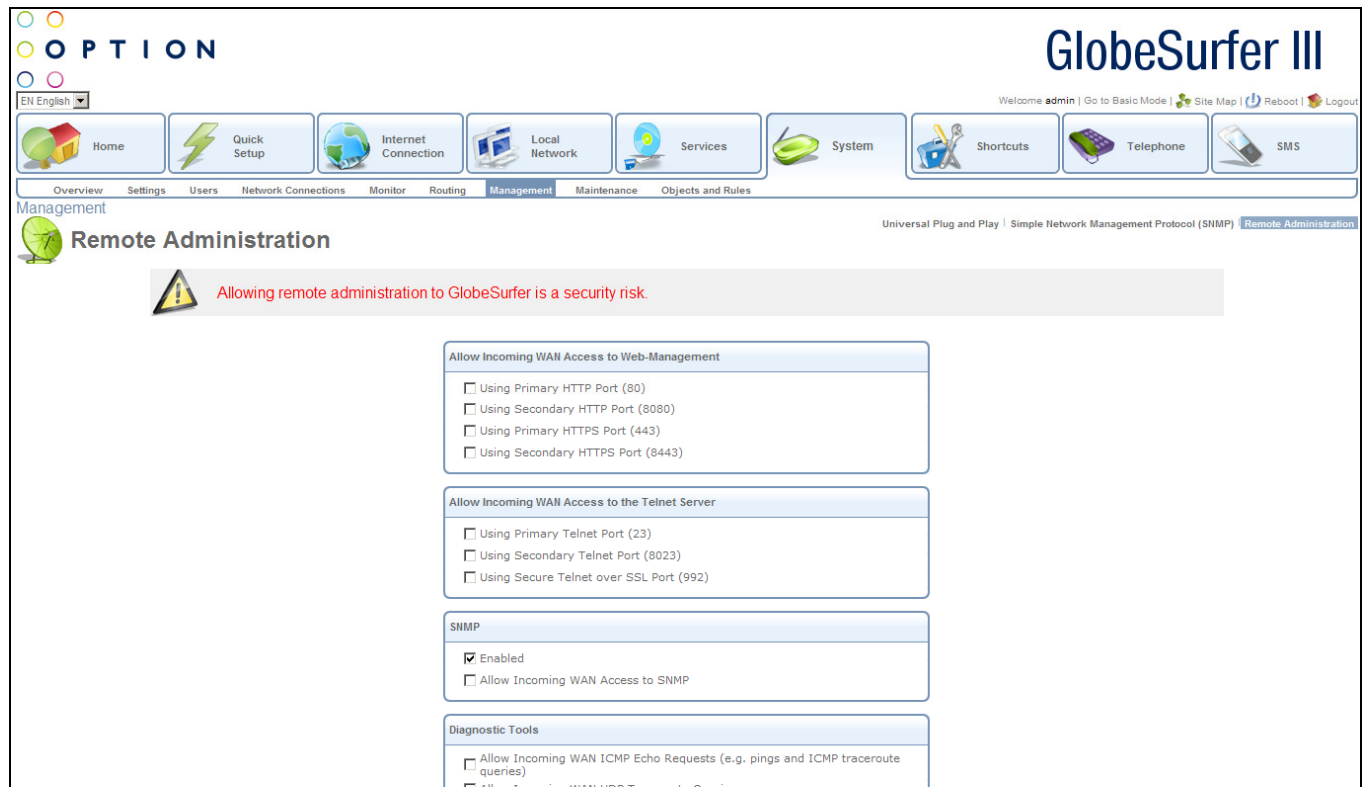
Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.8.3 Remote Administration

To access the Remote Administration screen, click the Remote Administration tab at the top right hand side of the Management screen in the System area.



It is possible to access and control GlobeSurfer® III+ not only from within the home network, but also from the Internet. This allows you to view or change settings while travelling. It also enables you to allow your ISP to change settings or help you troubleshoot functionality or communication issues from a remote location.

Remote access to GlobeSurfer® III+ is blocked by default to ensure the security of your home network. However, 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.

Note: Web-Management, Telnet and SSH 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 gateway from the home network. Therefore, remote access to Telnet or HTTP services should be blocked and should only be permitted when absolutely necessary.

The following data can be modified:

Allow Incoming WAN Access to Web-Management: used to obtain access to the Web-based Management and gain access to all system settings and parameters (using a browser). Both secure (HTTPS) and non-secure (HTTP) access is available. Select the checkboxes required:

- Using Primary HTTP Port (80)
- Using Secondary HTTP Port (8080)
- Using Primary HTTPS Port (443)
- Using Secondary HTTPS Port (8443)
- Allow Incoming WAN Access to the Telnet Server: used to create a command-line session and gain access to all system settings and parameters (using a text-based terminal).
- Using Primary Telnet Port (23)
- Using Secondary Telnet Port (8023)
- Using Secure Telnet over SSL Port (992)
- SNMP: used to allow Simple Network Management Protocol (SNMP) requests to remotely configure and monitor GlobeSurfer® III+. For more information, please refer to section o.
- Enabled: select this checkbox to enable SNMP
- Allow Incoming WAN Access to SNMP select this checkbox to allow incoming WAN access
- Diagnostic Tools: used for troubleshooting and remote system management by you or your Internet Service Provider. The utilities that can be used are Ping and Traceroute (over UDP).
- Allow Incoming WAN ICMP Echo Requests (e.g. pings and ICMP traceroute queries): select this checkbox to allow incoming WAN ICMP echo requests
- Allow Incoming WAN UDP Traceroute Queries: select this checkbox to allow incoming WAN UDP traceroute queries
- Additional Jnet Ports
- Allow Jnet Commands From Remote Upgrade Server: select this checkbox to allow Jnet commands from a remote upgrade server
- Remote Upgrade Server URL: click on this hyperlink to route to the Firmware upgrade screen in the Maintenance tab in the System area.
- Enable Incoming Jnet Requests to Port 7020: select this checkbox to enable incoming Jnet requests to port 7020 and then click on this hyperlink to route to the System Settings screen in the Settings tab in the System area
- Allow Incoming WAN Access to Jnet: select this checkbox to allow incoming WAN access to Jnet
- Enable Incoming Jnet-SSL Requests to Port 7021: select this checkbox to enable incoming Jnet-SSL requests to port 7021 and then click on this hyperlink to route to the System Settings screen in the Settings tab in the System area
- Allow Incoming WAN Access to Jnet-SSL: select this checkbox to allow incoming WAN access to Jnet-SSL

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.9 Maintenance

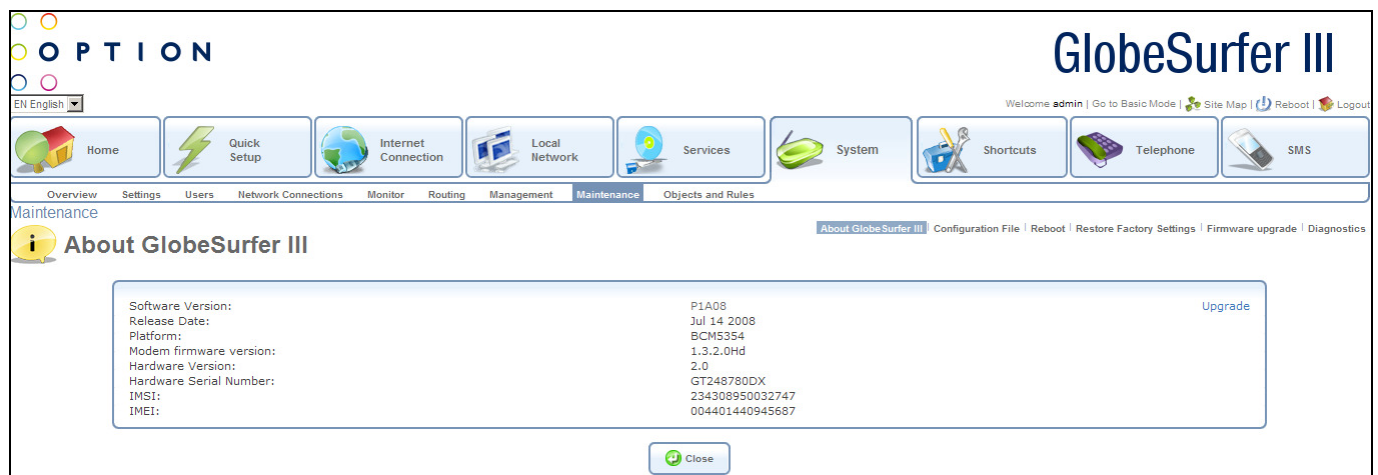
Access GlobeSurfer® III+'s maintenance settings by clicking the Maintenance tab in the System area.

From this screen you can click on the tabs at the top right hand side to route to the following detailed screens:

- About GlobeSurfer® III+
- Configuration File
- Reboot
- Restore Factory Settings
- Firmware upgrade
- Diagnostics

5.9.1 About GlobeSurfer III+

To access the About GlobeSurfer® III+ screen, click the About GlobeSurfer® III+ tab at the top right hand side of the Maintenance screen in the System area.



This screen shows technical information regarding GlobeSurfer® III+ including:

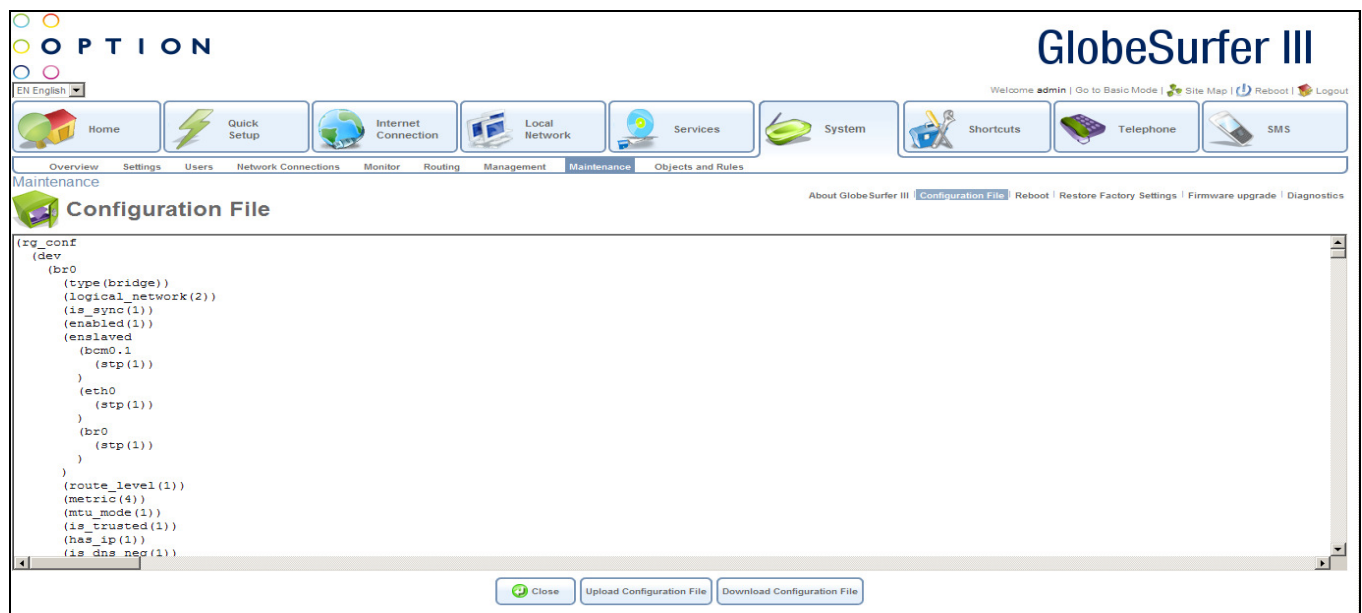
- Software Version
- Release Date
- Platform
- Modem firmware version
- Hardware Version
- Hardware Serial Number
- IMSI
- IMEI

Click on the Upgrade hyperlink in the top right hand corner to upgrade. This routes you to the Firmware upgrade screen in the Maintenance tab in the System area.

Press the Close button to go back to the Home screen.

5.9.2 Configuration File

To access the Configuration File screen, click the Configuration File tab at the top right hand side of the Maintenance screen in the System area.



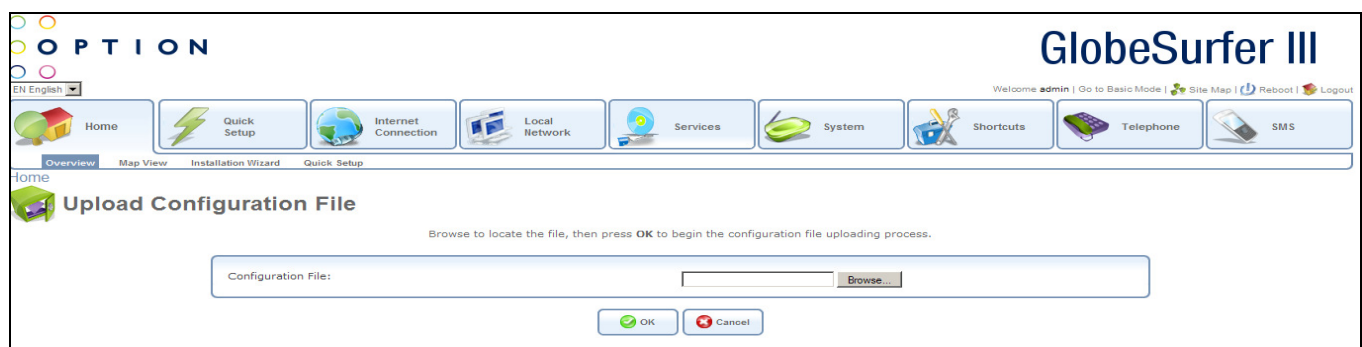
Click the Upload Configuration File button to load a configuration file and restart GlobeSurfer® III+. This routes you to the Upload Configuration File screen.

Click the Download Configuration File button to save a copy of the configuration file.

Press the Close button to go to the Home screen.

5.9.2.1 Upload Configuration File

To access the Upload Configuration File screen, click the Upload Configuration File button in the Configuration File screen.



Press Browse to locate the configuration file.

Press the OK button to begin the configuration file uploading process.

Press the Cancel button to reject changes and go to the Home screen.

5.9.3 Reboot

To access the Reboot screen, click the Reboot tab at the top right hand side of the Maintenance screen in the System area.

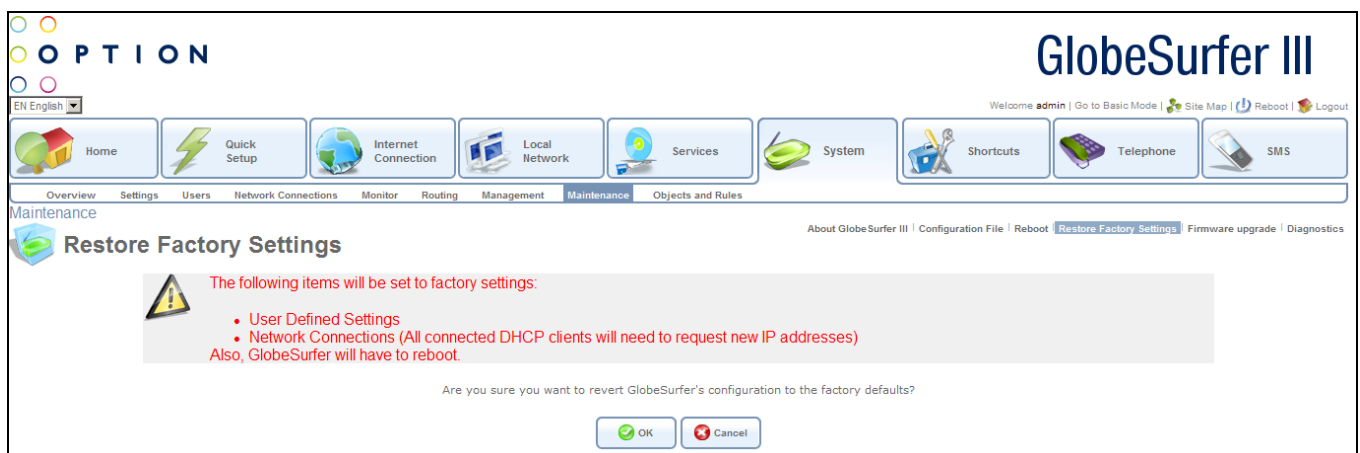


Press the OK button to reboot GlobeSurfer® III+. This may take one minute. To re-enter the management console after rebooting GlobeSurfer® III+, click the browser's Refresh button.

Press the Cancel button to cancel the reboot and go to the Home screen.

5.9.4 Restore Factory Settings

To access the Restore Factory Settings screen, click the Restore Factory Settings tab at the top right hand side of the Maintenance screen in the System area.



You may sometimes wish to restore GlobeSurfer® III+'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.

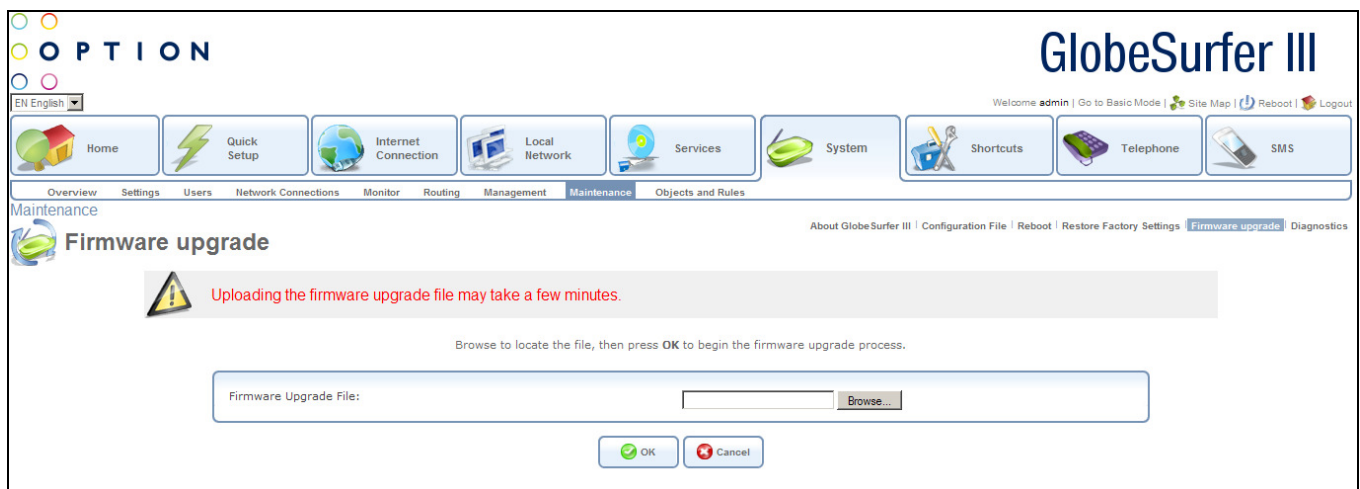
Note: All web-based management settings and parameters, not only those in the Advanced section, will be restored to their default values. This includes the administrator password - a user-specified password will no longer be valid.

Press the OK button to restore GlobeSurfer® III+'s configuration to the factory defaults.

Press the Cancel button to cancel the restore and go to the Home screen.

5.9.5 Firmware Upgrade

To access the Firmware upgrade screen, click the Firmware upgrade tab at the top right hand side of the Maintenance screen in the System area.



GlobeSurfer® III+ 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.

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

Enter the path of the software image file, or press the Browse button to browse for the firmware upgrade file on your PC.

Press the OK button to begin the firmware upgrading process.

Press the Cancel button to cancel the upgrade and go to the Home screen.

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

Press the OK button to begin the firmware upgrading process. The upgrade process will begin and should take no longer than one minute to complete.

Press the Cancel button to cancel the upgrade and go to the Home screen.

When the upgrading is ready the GlobeSurfer® III+ will automatically reboot. The new software version will run, maintaining your custom configurations and settings.

5.9.6 Diagnostics

To access the Diagnostics screen, click the Diagnostics tab at the top right hand side of the Maintenance screen in the System area.

GlobeSurfer III

Welcome **admin** | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance Objects and Rules

Diagnostics

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

Ping (ICMP Echo)

Destination: Go

Number of pings: Status:

ARP

Destination: Go

Status:

Traceroute

Destination: Go

Status:

Close Refresh

The Diagnostics screen can assist you in testing network connectivity and viewing statistics, such as the number of packets transmitted and received, round-trip time and success status.

The following data can be modified:

- Ping (ICMP Echo): this can be used to diagnose network connectivity:
- Destination: enter the IP address or URL to be tested
- Number of pings: enter the number of pings you would like to perform
- Status: shows the current status

Press the Go button to run the ping diagnostic. In a few seconds, diagnostic statistics will be displayed. If no new information is displayed, press the Refresh button.

Address Resolution Protocol (ARP): this is a method for finding a host's hardware address when only its network layer address is known:

- Destination: enter the IP address or URL to be tested
- Status: shows the current status

Press the Go button to run the ARP diagnostic

Traceroute: this can be used to perform a traceroute:

- Destination: enter the IP address or URL to be tested
- Status: shows the current status

Press the Go button to run the traceroute. The screen will be constantly refreshed. To stop the trace and view the results, press the Cancel button.

Press the Close button to go to the Home screen.

Press the Refresh button to refresh the screen and update the status fields.

5.10 Objects and Rules

Access GlobeSurfer® III+'s objects and rules settings by clicking the Objects and Rules tab in the System area.

From this screen you can click on the tabs at the top right hand side to route to the following detailed screens:

- Protocols
- Network Objects
- Scheduler Rules
- Certificates

5.10.1 Protocols

To access the Protocols screen, click the Protocols tab at the top right hand side of the Objects and Rules screen in the System area.

Protocols	Ports	Action
FTP	TCP Any -> 21	[Edit] [Delete] [Add]
HTTP	TCP Any -> 80	[Edit] [Delete] [Add]
HTTPS	TCP Any -> 443	[Edit] [Delete] [Add]
IMAP	TCP Any -> 143	[Edit] [Delete] [Add]
L2TP	UDP Any -> 1701	[Edit] [Delete] [Add]
Ping	ICMP Echo Request	[Edit] [Delete] [Add]
POP3	TCP Any -> 110	[Edit] [Delete] [Add]
SMTP	TCP Any -> 25	[Edit] [Delete] [Add]
SNMP	UDP Any -> 161	[Edit] [Delete] [Add]
Telnet	TCP Any -> 23	[Edit] [Delete] [Add]
TFTP	UDP 1024-65535 -> 69	[Edit] [Delete] [Add]
Traceroute	UDP 32769-65535 -> 33434-33523	[Edit] [Delete] [Add]

[New Entry](#)

[Close] [Advanced >>]

The Protocols feature incorporates a list of preset and user-defined applications and common port settings. You can use protocols in various security features such as Access Control and Port Forwarding. You may add new protocols to support new applications or edit existing ones according to your needs.

For each protocol the following data is displayed:

- Protocols
- Ports
- Action: add, modify or delete

Click on a Protocol hyperlink or the edit icon in the table to modify an entry, or click on the New Entry hyperlink or the add icon to add an entry. In both cases you will be routed to the Edit Service screen.

Press the Close button to go to the previous screen.

Press the Advanced button to display an extended version of the screen with more protocols.

Press the Basic button to display a limited version of the screen with fewer protocols.

Option

Welcome **admin** | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance **Objects and Rules**

Edit Service

Service Name: L2TP
Service Description: Layer Two Tunneling Protocol

Server Ports		
Protocol	Server Ports	Action
UDP	Any -> 1701	[edit] [delete] [add]
New Server Ports		

Opened Ports		
Protocol	Opened Ports	Action
UDP	Any -> Same as Initiating Ports	[edit] [delete] [add]
New Opened Ports		

OK Cancel

Enter the following data:

- Service Name: name of the service
- Service Description: description of the service
- For each server port the following data is displayed:
 - Protocol
 - Server Ports
 - Action: add, modify or delete
- For each opened port the following data is displayed:
 - Protocol
 - Opened Ports
 - Action: add, modify or delete

Click on a Protocol hyperlink or the edit icon in the Server Ports table to modify an entry, or click on the New Server Ports hyperlink or the add icon to add an entry. In both cases you will be routed to the Edit Service Server Ports screen.

Click on a Protocol hyperlink or the edit icon in the Opened Ports table to modify an entry, or click on the New Opened Ports hyperlink or the add icon to add an entry. In both cases you will be routed to the Edit Service Opened Ports screen.

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

The screenshot shows the GlobeSurfer III web interface. At the top, there's a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The main content area is titled 'Edit Service Server Ports' and contains a form with the following fields:

Protocol	TCP
Source Ports:	Any
Destination Ports:	Any

At the bottom of the form are two buttons: 'OK' and 'Cancel'.

You may choose any of the protocols available in the drop down list, or add a new one by selecting Other. When selecting a protocol from the drop down list, the screen will refresh, presenting the appropriate fields to enter for that protocol. Select a protocol and enter the relevant information.

The following fields should be entered:

- Protocol: choose from the drop down list:
- TCP, then enter
- Source Ports, then choose from the drop down list:
 - Any
 - Single, then enter port number
 - Range, then enter range values
- Destination Ports, then choose from the drop down list:
 - Any
 - Single, then enter port number
 - Range, then enter range values
- UDP, then enter
- Source Ports, then choose from the drop down list:
 - Any
 - Single, then enter port number
 - Range, then enter range values
- Destination Ports, then choose from the drop down list:
 - Any
 - Single, then enter port number
 - Range, then enter range values
- ICMP, then enter
- ICMP Message by choosing from the drop down list:

- Echo Reply
 - Network Unreachable
 - Host Unreachable
 - Protocol Unreachable
 - Port Unreachable
 - Destination Network Unknown
 - Destination Host Unknown
 - Redirect for Network
 - Redirect for Host
 - Echo Request
 - Other
 - GRE
 - ESP
 - AH
- Other, then enter
 - Protocol Number

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

The screenshot shows the GlobeSurfer III web interface. At the top, there's a navigation bar with icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a sub-navigation bar with tabs for Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The 'Objects and Rules' tab is selected, and the 'Edit Service Opened Ports' screen is displayed. The screen has a title bar with 'Edit Service Opened Ports' and a sub-tab for 'Protocols'. The main content area contains a form with a 'Protocol' dropdown menu set to 'TCP'. Below it are 'Source Ports' and 'Destination Ports' dropdown menus, both set to 'Any'. At the bottom of the form are 'OK' and 'Cancel' buttons.

You may choose any of the protocols available in the drop down list, or add a new one by selecting Other. When selecting a protocol from the drop down list, the screen will refresh, presenting the appropriate fields to enter for that protocol. Select a protocol and enter the relevant information.

The following fields should be entered:

Protocol: choose from the drop down list:

- TCP, then enter
 - Source Ports, then choose from the drop down list:

- Any
- Single, then enter port number
- Range, then enter range values
- Destination Ports, then choose from the drop down list:
 - Any
 - Single, then enter port number
 - Range, then enter range values
 - Same as Initiating Ports
- UDP, then enter
 - Source Ports, then choose from the drop down list:
 - Any
 - Single, then enter port number
 - Range, then enter range values
- Destination Ports, then choose from the drop down list:
 - Any
 - Single, then enter port number
 - Range, then enter range values
 - Same as Initiating Ports
- ICMP, then enter
- ICMP Message by choosing from the drop down list:
 - Echo Reply
 - Network Unreachable
 - Host Unreachable
 - Protocol Unreachable
 - Port Unreachable
 - Destination Network Unknown
 - Destination Host Unknown
 - Redirect for Network
 - Redirect for Host
 - Echo Request
 - Other
 - GRE
 - ESP
 - AH
- Other, then enter

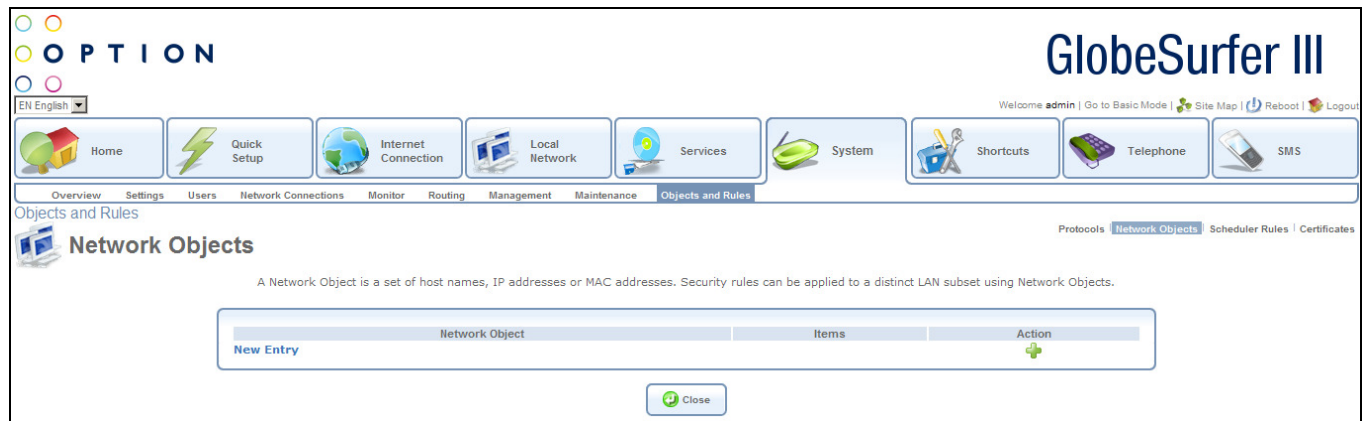
- Protocol Number

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.10.2 Network Objects

To access the Network Objects screen, click the Network Objects tab at the top right hand side of the Objects and Rules screen in the System area.



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

For each network object the following data is displayed:

- Network Object
- Items
- Action: add, modify or delete

Click on the New Entry hyperlink or the add icon to add an entry. You will be routed to the Edit Network Object screen (see below).

Press the Close button to go to the previous screen

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance Objects and Rules

Objects and Rules

Protocols Network Objects Scheduler Rules Certificates

Edit Network Object

Network Object

Description: Global Object

Items

Item	Action
New Entry	+

OK Cancel

Enter the following data:

Description: name of the network object

Click on the New Entry hyperlink or the add icon to add an entry. You will be routed to the Edit Item screen (see below).

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

OPTION

EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance Objects and Rules

Objects and Rules

Protocols Network Objects Scheduler Rules Certificates

Edit Item

Network Object Type: IP Subnet

Subnet IP Address: 0 0 0 0

Subnet Mask: 0 0 0 0

OK Cancel

You may choose any of the object types available in the drop down list. When selecting an object type from the drop down list, the screen will refresh, presenting the appropriate fields to enter for that object type. Select an object type and enter the relevant information.

The source address should be entered in one of the following:

Network Object Type: choose from the drop down list:

- IP Address, then enter

- IP address
- IP Subnet, then enter
 - Subnet IP Address
 - Subnet Mask
- IP Range, then enter
 - From IP Address
 - To IP Address
- MAC Address, then enter
 - MAC Address
 - MAC Mask
- Host Name, then enter
 - Host Name
- DHCP Option, then choose from the drop down list:
 - Vendor Class ID
 - Client ID
 - User Class ID

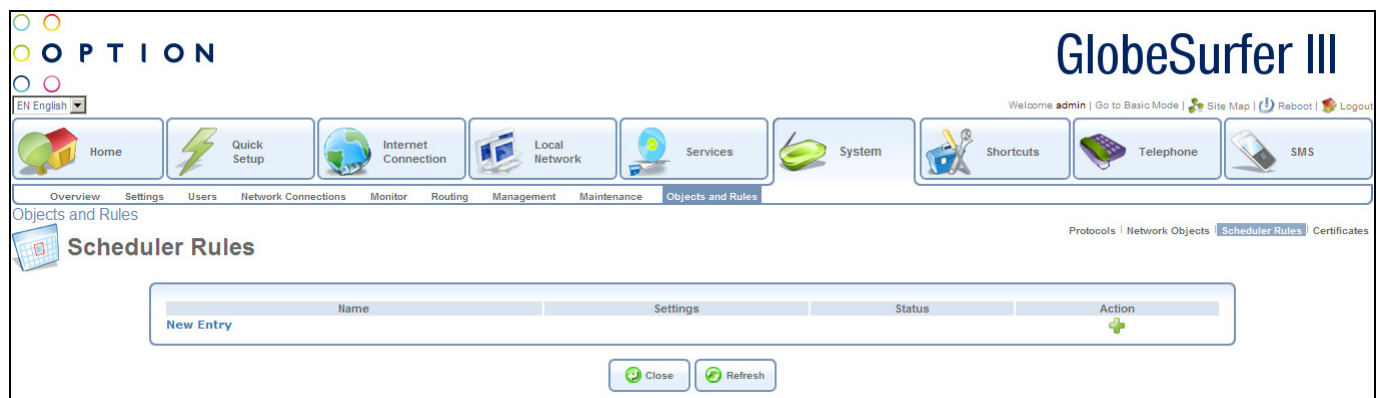
then enter the appropriate ID

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.10.3 Scheduler Rules

To access the Scheduler Rules screen, click the Scheduler Rules tab at the top right hand side of the Objects and Rules screen in the System area.



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.

For each scheduler rule the following data is displayed:

- Name
- Settings
- Status
- Action: add, modify or delete

Click on the New Entry hyperlink or the add icon to add an entry. You will be routed to the Edit Scheduler Rule screen (see below).

Press the Close button to go to the previous screen.

Press the Refresh button to refresh the screen.

The screenshot displays the 'Edit Scheduler Rule' page in the GlobeSurfer III web interface. The top navigation bar features the 'OPTION' logo, a language dropdown set to 'EN English', and a series of icons for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a secondary navigation bar with tabs for Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The main content area is titled 'Edit Scheduler Rule' and contains a form with the following elements:

- A 'Name' field with the value 'Scheduler Rule'.
- 'Rule Activity Settings' with two radio buttons: 'Rule will be Active at the Scheduled Time' (selected) and 'Rule will be Inactive at the Scheduled Time'.
- A table with the header 'Time Segments' and an 'Action' column. Below the table is a 'New Time Segment Entry' link and a green plus icon.
- 'OK' and 'Cancel' buttons at the bottom.

Enter the following data:

- Name: name for the rule
- Rule Activity settings: choose from the following radio buttons to specify if the rule will be active/inactive during the designated time period:
 - Rule will be Active at the Scheduled Time
 - Rule will be Inactive at the Scheduled Time

Click on the New Time Segment hyperlink or the add icon to add an entry. You will be routed to the Edit Time Segment screen (see below).

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

OPTION **GlobeSurfer III**

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance **Objects and Rules**

Protocols | Network Objects | **Scheduler Rules** | Certificates

Edit Time Segment

Days of Week

☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday
☐ Sunday

Hours Range

Start Time	End Time	Action
New Hours Range Entry		

OK Cancel

Enter the following data:

Days of Week: select days of the week when the rule should apply

Click on the New Hours Range hyperlink or the add icon to add an entry. You will be routed to the Edit Hour Range screen (see below).

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

OPTION **GlobeSurfer III**

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout | EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance **Objects and Rules**

Protocols | Network Objects | **Scheduler Rules** | Certificates

Edit Hour Range

Start Time: : :00

End Time: : :00

OK Cancel

This screen allows the entry of the hours during the day when the rules will apply. The following fields should be entered:

- Start Time in hours and minutes
- End Time in hours and minutes

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

5.10.4 Certificates

5.10.4.1 Overview

Public-key cryptography uses a pair of keys: a public key and a corresponding private key. These keys can play opposite roles, either encrypting or decrypting data. Your public key is made known to the world, while your private key is kept secret.

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 the public key can encrypt information that can only be decrypted with the matching private key. Similarly, the person with the private key can encrypt information that can only be decrypted with the matching public key.

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 pre-existing security arrangement to authenticate each other and exchange messages securely.

GlobeSurfer® III+ makes use of public-key cryptography to encrypt and authenticate keys for the encryption of Wireless and VPN data communication, the Web Based Management (WBM) utility and secured telnet.

5.10.4.2 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.

5.10.4.3 X.509 Certificate Format

GlobeSurfer® III+ 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, 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=Option Wireless Sweden AB, EMAIL=info@option.com, OU=Development Department, O=Option Wireless Sweden AB, 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.

5.10.4.4 *GlobeSurfer® III+ Certificate Stores*

GlobeSurfer® III+ maintains two certificate stores:

- **GlobeSurfer® III+ Local Store:** this store contains a list of approved certificates that are used to identify GlobeSurfer® III+ to its clients. The list also includes certificate requests that are pending a CA's endorsement. You can obtain certificates for GlobeSurfer® III+ using the following methods:
 - **Requesting an X509 Certificate:** this method creates both a private and a matching public key. The public key is then sent to the CA to be certified.
 - **Creating a Self-Signed Certificate:** this method is the same as requesting a certificate, only the authentication of the public key does not require a CA. This is mainly intended for use within small organizations.
 - **Loading a PKCS#12 Format Certificate:** this method loads a certificate using an already available and certified set of private and public keys.
- **Certificate Authority (CA) Store:** this store contains a list of the trusted certificate authorities, which are used to check certificates presented by GlobeSurfer® III+ clients.

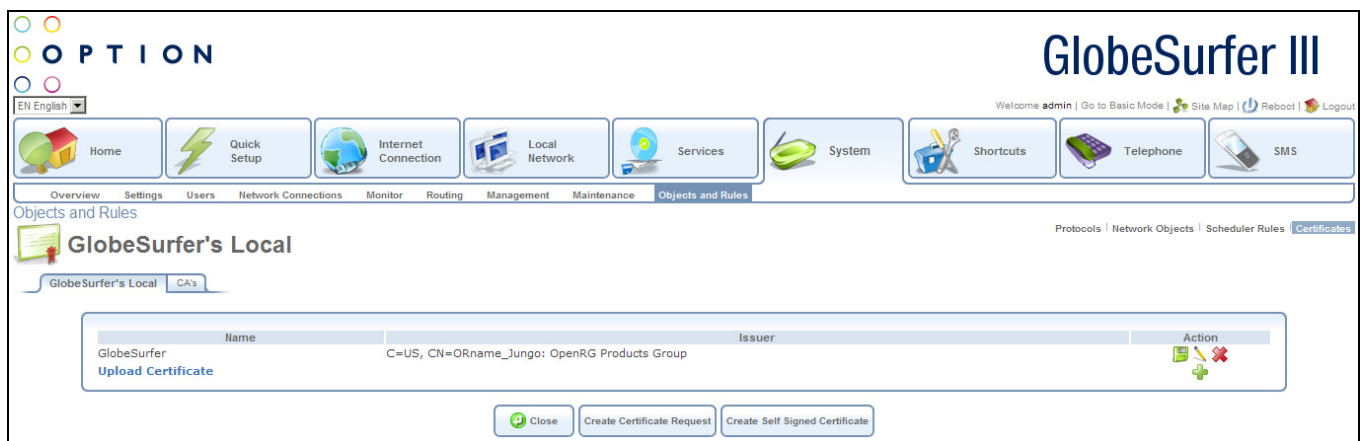
5.10.4.5 *Requesting an X.509 Certificate*

To obtain an X509 certificate, you must ask a CA to issue you one. 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

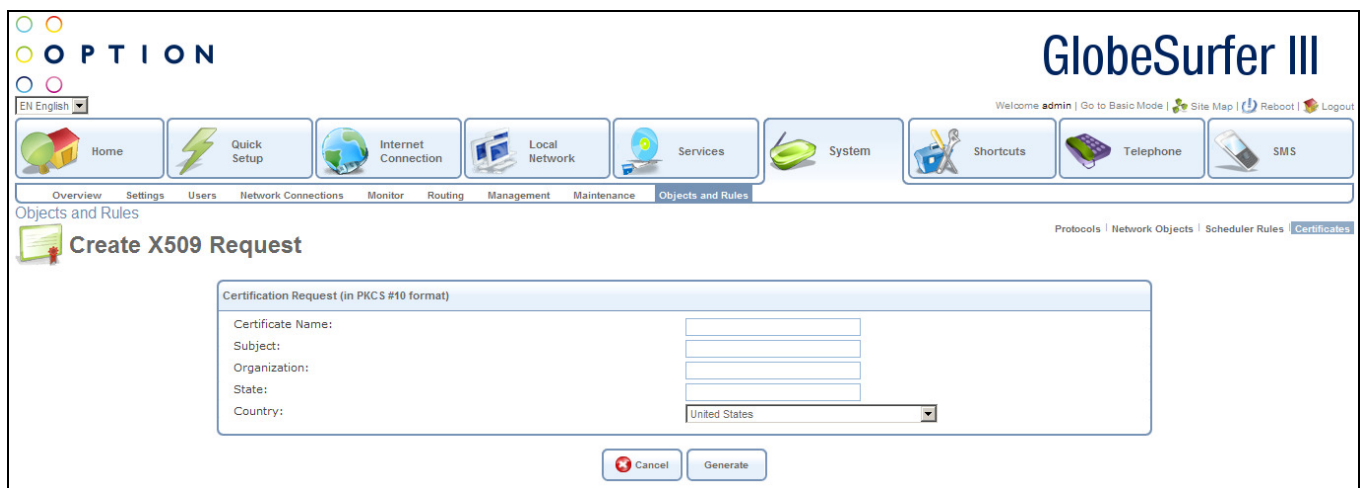
then performs some due diligence in verifying that the information you provided is correct and, if so, generates the certificate and returns it.

You might think of an X509 certificate as looking like 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.

Click the Certificates tab in the top right hand corner of the Objects and Rules screen in the System area. The GlobeSurfer® III+'s Local screen will appear.



Click the Create Certificate Request button. The Create X509 Request screen will appear.



Enter the following certification request parameters:

- Certificate Name
- Subject
- Organization
- State

- Country

Click the Generate button. A screen will appear stating that the certification request is being generated.

OPTION

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance Objects and Rules

Objects and Rules

New X509 Request

Generating request. This can take some time. Please wait.

Press the Refresh button to update the data.

Abort Refresh

Protocols | Network Objects | Scheduler Rules | Certificates

After a short while, press the Refresh button, until the Save Certificate Request screen appears.

Click the Save Certificate Request button and save the request to a file.

Click the Close button. The main GlobeSurfer® III+'s Local screen will reappear, listing your certificate as Unsigned.

In this state, the request file may be opened at any time by pressing the Save icon under the Action column and then Open in the dialog box (Windows only).

After receiving a reply from the CA in form of a .pem file, click the Upload Certificate link. The Load GlobeSurfer® III+'s Local Certificate screen will appear.

OPTION

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Overview Settings Users Network Connections Monitor Routing Management Maintenance Objects and Rules

Objects and Rules

Load GlobeSurfer's Local Certificate

Browse to locate either PEM-encoded signed certificate or Personal Information Exchange PKCS#12 file (.PFX,.P12), then press Upload.

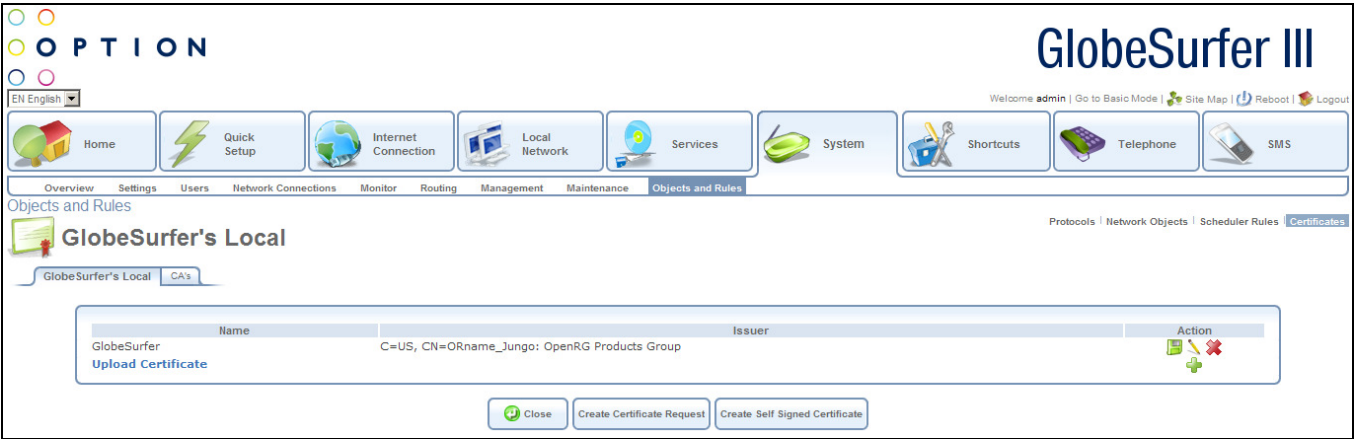
Certificate File: Browse...

Personal Information Exchange PKCS#12 File Password (leave empty if no password is required):

Upload Cancel

Protocols | Network Objects | Scheduler Rules | Certificates

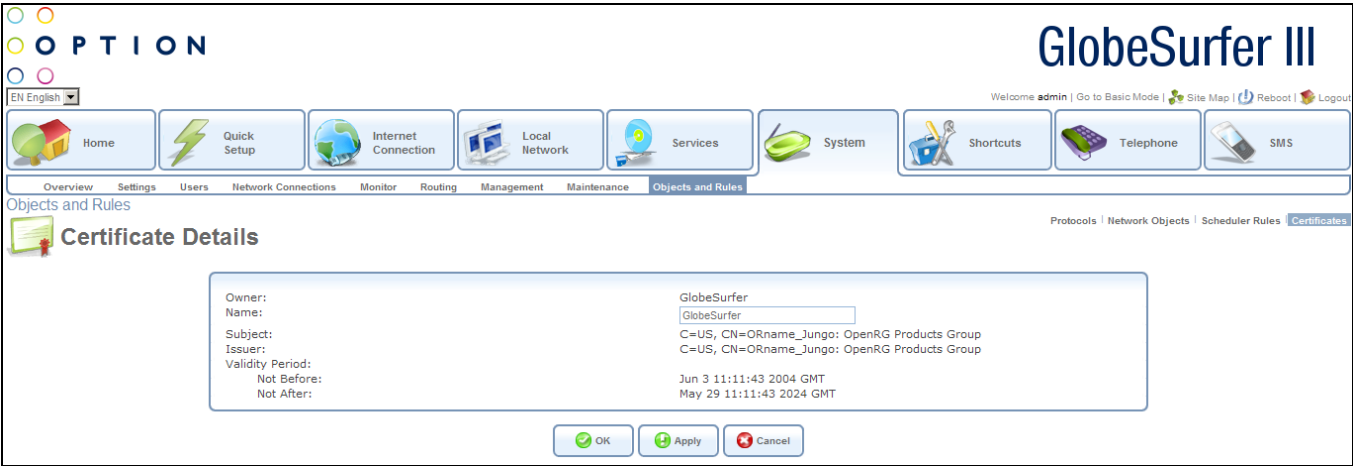
Use the Browse button to browse to the signed certificate .pem file. Leave the password entry empty and press Load to load the signed certificate. The GlobeSurfer® III+'s Local screen will appear, displaying the certificate name and issuer.



You can click the Save icon under the Action column, and then Open in the dialogue box to view the Certificate window (Windows only) box to save the certificate to a file.



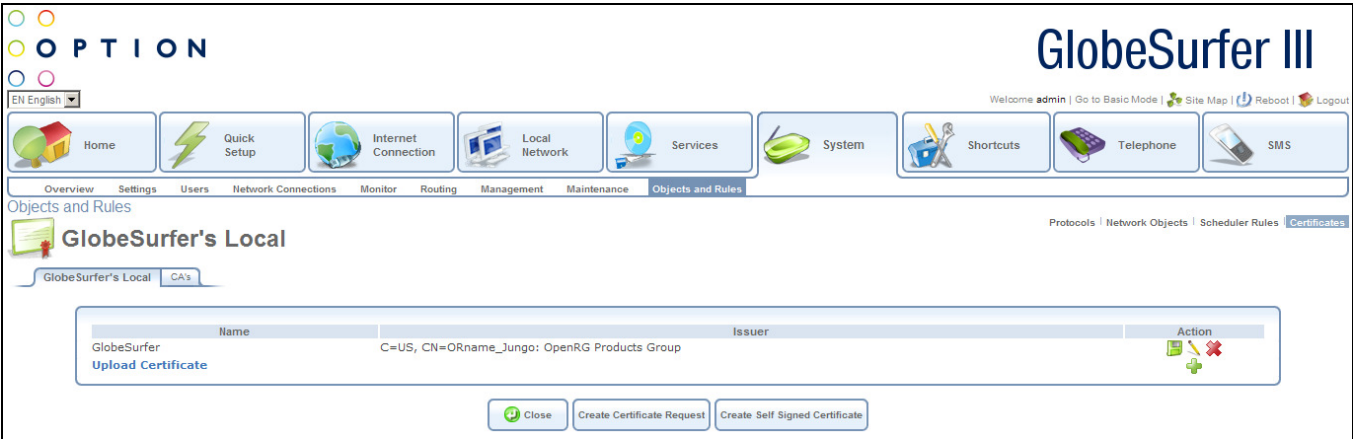
You can also click the Edit icon under the Action column to view the Certificate Details screen.



5.10.4.6 Creating a Self-Signed Certificate

A default self-signed certificate is included in GlobeSurfer® III+, in order to enable certificate demanding services such as HTTPS. Note that if deleted, this certificate is restored when GlobeSurfer® III+'s Restore Factory Settings operation is run.

To create a self-signed certificate, click the Certificates tab in the top right hand corner of the Objects and Rules screen in the System area. The GlobeSurfer® III+'s Local screen will appear.



Click the Create Self Signed Certificate button. The Create Self Signed X509 Certificate screen will appear.

The screenshot shows the GlobeSurfer III web interface. The top navigation bar includes links for Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below this is a secondary navigation bar with links for Overview, Settings, Users, Network Connections, Monitor, Routing, Management, Maintenance, and Objects and Rules. The main content area is titled 'Create Self Signed X509 Certificate'. It contains a form with the following fields: Certificate Name (text input), Subject (text input), Organization (text input), State (text input), and Country (dropdown menu with 'United States' selected). At the bottom of the form are 'Cancel' and 'Generate' buttons.

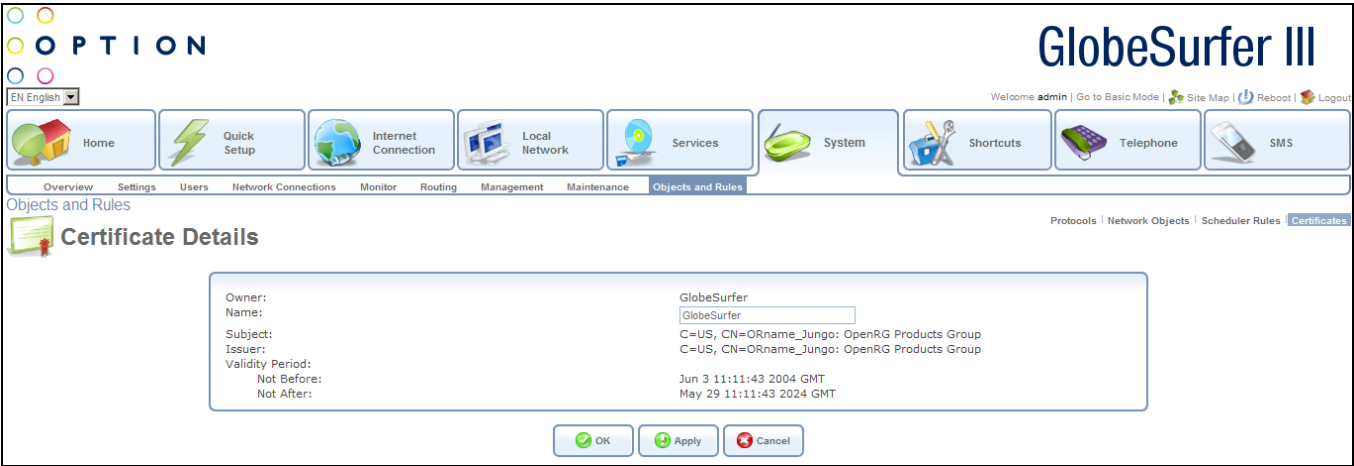
Enter the following certification request parameters:

- Certificate Name
- Subject
- Organization
- State
- Country

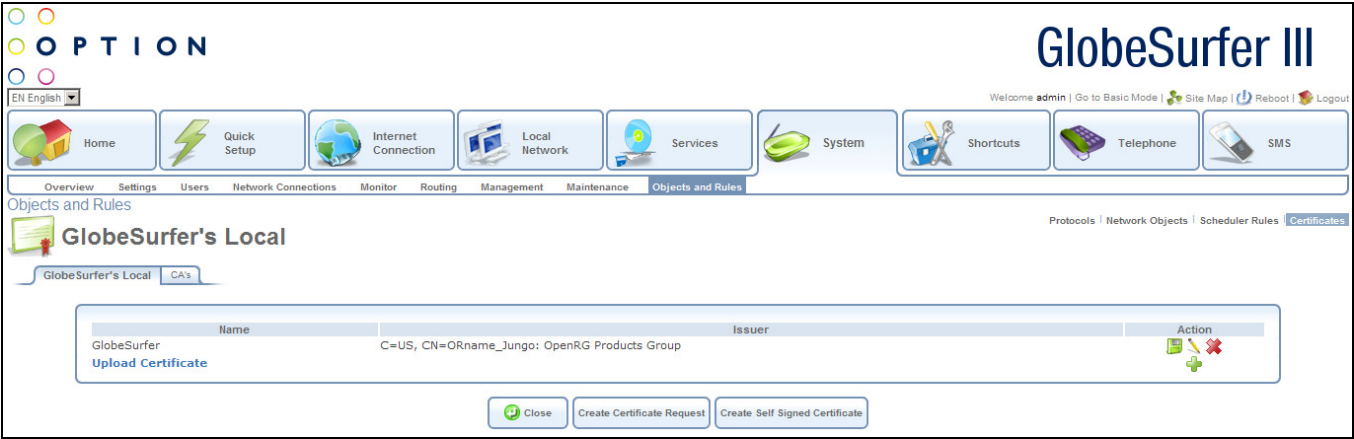
Click the Generate button. A screen will appear stating that the certification request is being generated.

The screenshot shows the GlobeSurfer III web interface after clicking the 'Generate' button. The main content area is titled 'New Self Signed X509 Certificate'. It displays a warning message: 'Generating certificate. This can take some time. Please wait.' Below the message is a text prompt: 'Press the Refresh button to update the data.' At the bottom are 'Abort' and 'Refresh' buttons.

After a short while, press the Refresh button, until the Certificate Details screen appears.



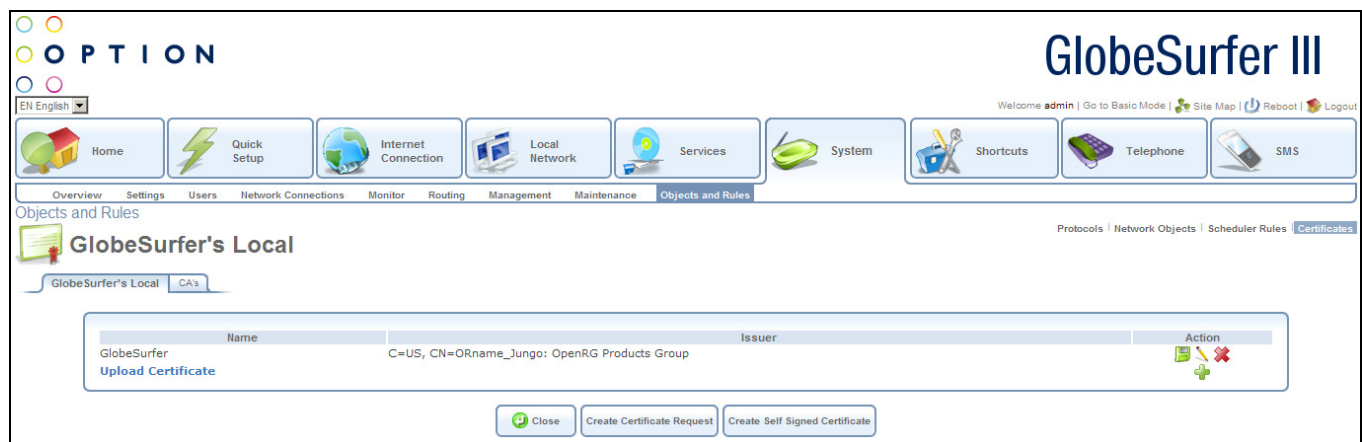
Click the OK. The main GlobeSurfer® III+'s Local screen will reappear, displaying the certificate name and issuer.



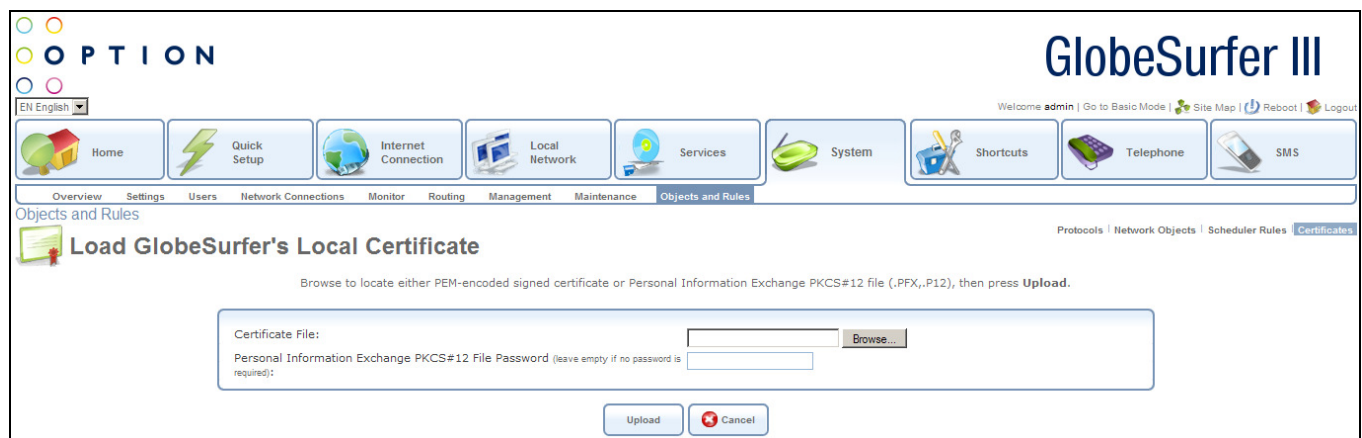
5.10.4.7 Loading a PKCS#12 Format Certificate

You can also load certificates in PKCS#12 format (usually stored in .p12 files) to GlobeSurfer® III+'s certificate store. You must first obtain the .p12 file, containing the private and public keys and optional CA certificates.

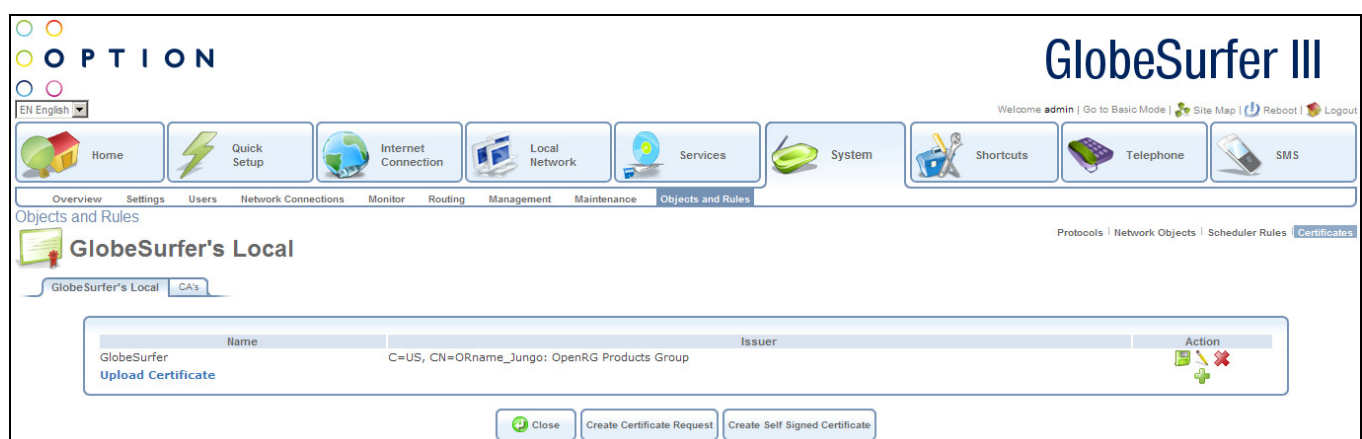
Click the Certificates tab in the top right hand corner of the Objects and Rules screen in the System area. The GlobeSurfer® III+'s Local screen will appear.



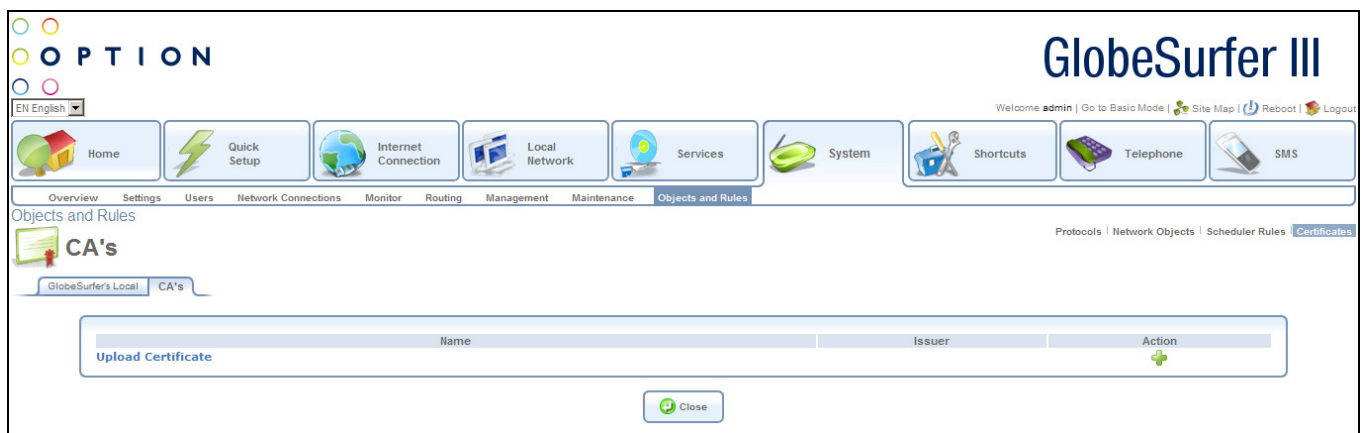
Click the Upload Certificate link. The Load GlobeSurfer® III+'s Local Certificate screen will appear.



Use the Browse button to browse to the .p12 file. If the private key is encrypted using a password, type it in the password entry (otherwise leave the entry empty) and press Load to load the certificate. The GlobeSurfer® III+'s Local screen will appear, displaying the certificate name and issuer.

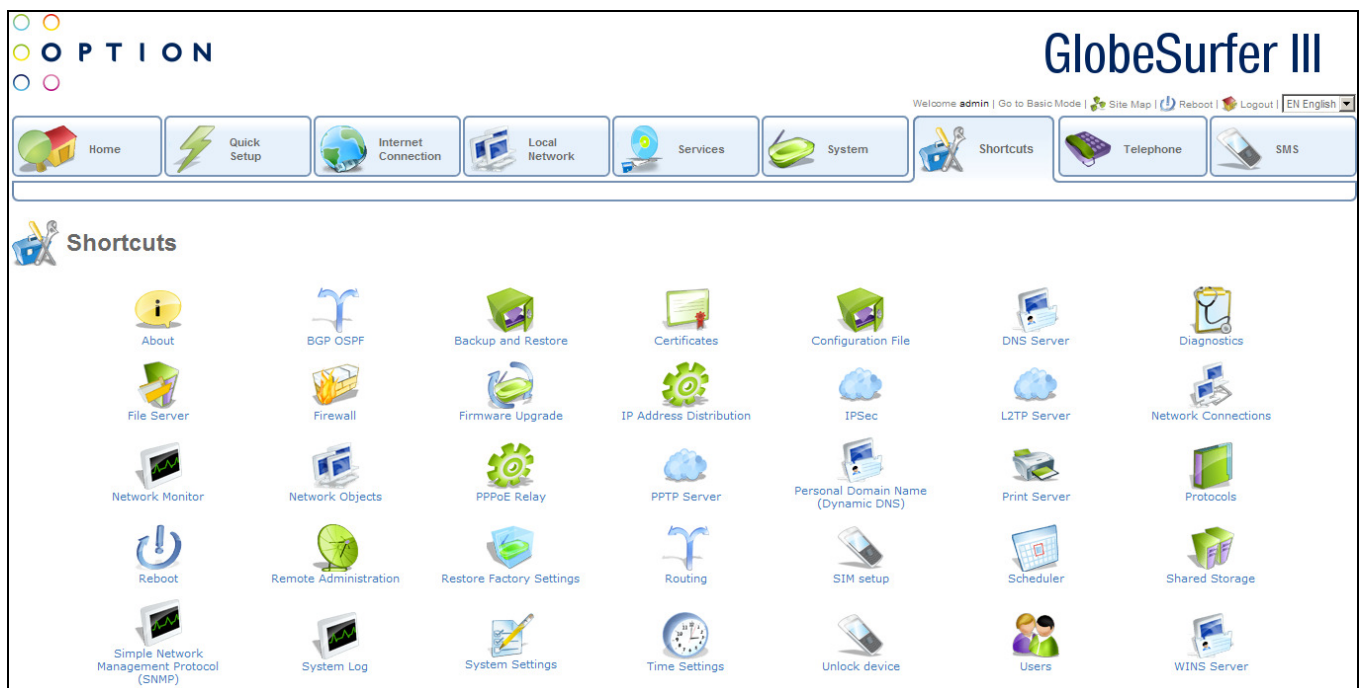


If the .p12 file contained any CA certificates, they will be displayed in the CA store (click the CAs tab to view the CA certificates).



6 Shortcuts

This page displays icon shortcuts in alphabetical order for many of the GlobeSurfer® III+ functions to enable quick and easy access to all areas.



Click on the shortcut you require, and you will be routed immediately to the correct page.

Shortcuts available are:

- About
- BGP OSPF
- Backup and Restore
- Certificates
- Configuration File
- DNS Server

- Diagnostics
- File Server
- Firewall
- Firmware Upgrade
- IP Address Distribution
- IPSec
- L2TP Server
- Network Connections
- Network Monitor
- Network Objects
- PPPoE Relay
- PPTP Server
- Personal Domain Name (Dynamic DNS)
- Print Server
- Protocols
- Reboot
- Remote Administration
- Restore Factory Settings
- Routing
- SIM setup
- Scheduler
- Shared Storage
- Simple Network Management Protocol (SNMP)
- System Log
- System Settings
- Time Settings
- Unlock device
- Users
- WINS Server

7 Telephone

GlobeSurfer® III+ is equipped with a telephony connector and can replace a regular fixed line service (POTS). In order to setup fixed line telephony to make phone calls through GlobeSurfer® III+, connect GlobeSurfer® III+ to the first telephony plug. Note that you should configure your country in the GlobeSurfer® III+ Installation wizard.

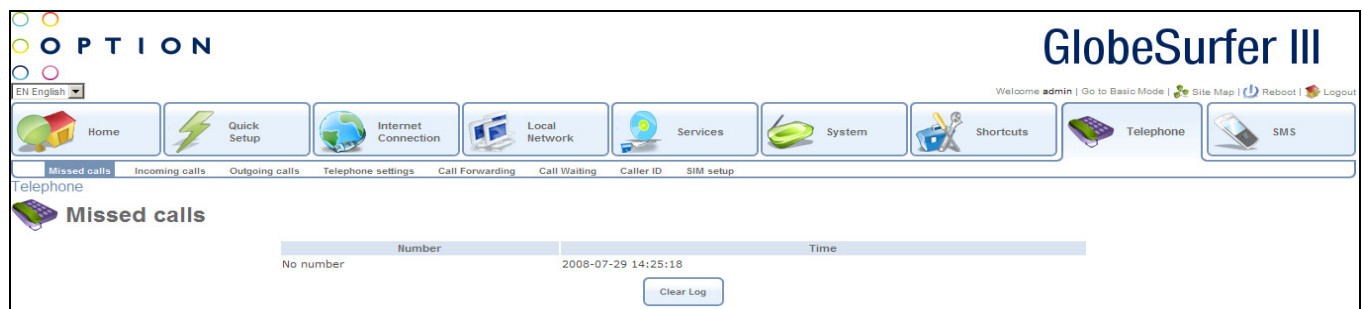
From this screen you can click on the tabs at the top left hand side to route to the following detailed screens:

- Missed calls – list of calls received but not answered
- Incoming calls – list of calls received and answered
- Outgoing calls – calls initiated from your phones

- Telephone settings – controls behavior of fixed line telephony
- Call Forwarding – allows you to forward calls to other numbers
- Call Waiting – allows you to activate or deactivate call waiting
- Caller ID – allows you to identify the telephone number of caller
- SIM setup – allows you to change or enable the SIM PIN number

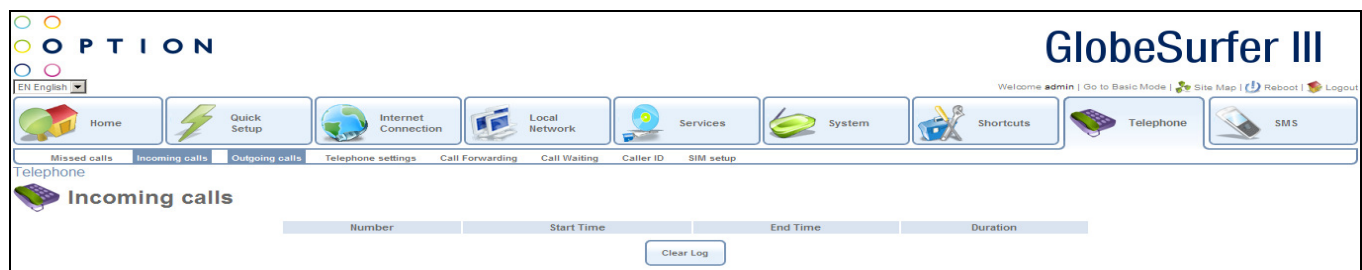
7.1 Missed calls

The Missed calls screen shows a list of calls, with Caller ID if received, that were not answered including a time stamp of the event. By clicking Clear Log you will erase the history of missed calls.



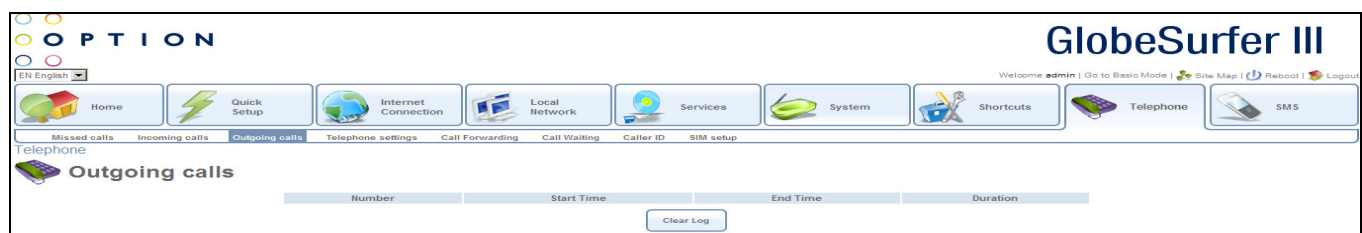
7.2 Incoming calls

The Incoming calls screen shows calls, with Caller ID if received, that were received and answered including a time stamp and duration of the event. By clicking Clear Log you will erase the history of incoming calls.



7.3 Outgoing calls

The Outgoing calls screen shows calls, with Caller ID, that have been initiated from your telephones using GlobeSurfer® III+ including a time stamp and duration of the event. By clicking Clear Log you will erase the history of outgoing calls.



7.4 Telephone settings

The Telephone settings screen controls the behavior of the fixed line telephony support of GlobeSurfer® III+.

Use the Telephone settings screen to make the following settings:

- Caller ID: select from the following options:
 - ETSI DTMF
 - ETSI FSK ring pulse
 - ETSI FSK dualtone
 - ETSI FSK Line reversal + dualtone
 - ETSI FSK during ring
 - Bellcore
 - Australia
- International Dialing Code: enter the prefix for the country
- Dialling timeout (seconds): type in the number of seconds to set the delay between pressing a dial-key on phone and when the call is placed
- Use # to end dialling: clicking this checkbox allows you to press the # key instead of waiting for the timeout
- Call log: clicking this checkbox keeps a log of incoming, outgoing and missed calls

Press the OK button to apply changes and go back to the previous screen.

Press the Apply button to apply changes and stay on this screen.

Press the Cancel button to reject changes and go back to the previous screen.

7.5 Call Forwarding

The Call Forwarding screen allows you to forward calls to other numbers when there is no answer, or the number is unreachable or busy.

OPTION

GlobeSurfer III

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout | EN English

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

Missed calls Incoming calls Outgoing calls Telephone settings **Call Forwarding** Call Waiting Caller ID SIM setup

Call Forwarding

Deactivate all Clear all numbers Check all

All calls

Number: Status: Deactivated

Activate Deactivate Clear number

No answer

Number: Status: Deactivated

Activate Deactivate Clear number

Unreachable

Number: Status: Deactivated

Activate Deactivate Clear number

Busy

Number: Status: Deactivated

Activate Deactivate Clear number

Refresh

Use the Call Forwarding screen to make the following settings:

Deactivate all: clicking this button will deactivate all the call forwarding set up on the page, for all calls, no answer, unreachable and busy calls

Clear all numbers: clicking this button will delete all the telephone numbers set up on the page for all calls, no answer, unreachable and busy calls

Check all: clicking this button will check all the statuses on the page for all calls, no answer, unreachable and busy calls

All calls: the following options apply to all calls:

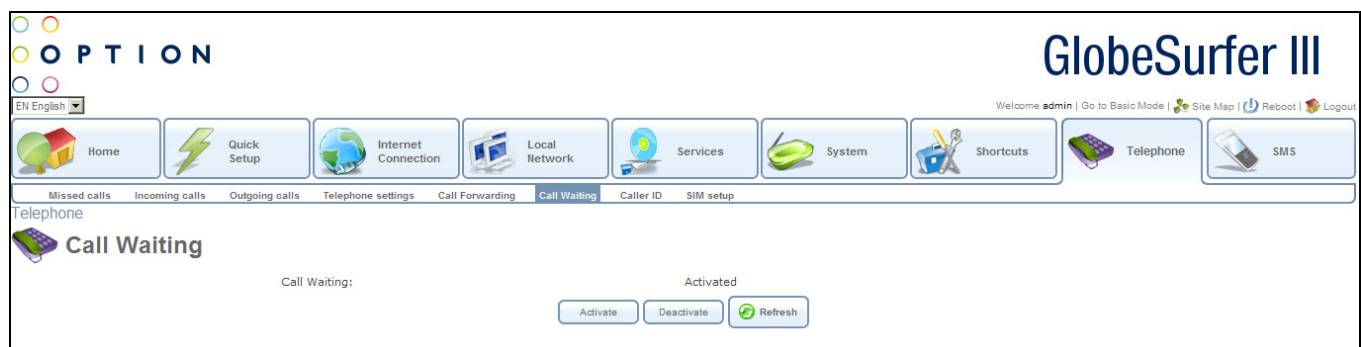
- **Activate:** clicking this button will forward all calls to the number provided
- **Deactivate:** clicking this button will stop the forwarding of all calls
- **Clear number:** clicking this button will delete the number provided
- **Number:** enter the phone number to forward all calls to
- **Status:** displays the status of all call forwarding as Activated or Deactivated
- **No answer:** the following options apply to unanswered calls:
 - **Activate:** clicking this button will forward unanswered calls to the number provided
 - **Deactivate:** clicking this button will stop the forwarding of unanswered calls
 - **Clear number:** clicking this button will delete the phone number provided
 - **Number:** enter the phone number to forward unanswered calls to

- Status: displays the status of unanswered call forwarding as Activated or Deactivated
- Unreachable: the following options apply to calls when the number is unreachable:
 - Activate: clicking this button will forward unreachable calls to the phone number provided
 - Deactivate: clicking this button will stop the forwarding of unreachable calls
 - Clear number: clicking this button will delete the phone number provided
 - Number: enter the phone number to forward calls to when the number is unreachable
 - Status: displays the status of unreachable call forwarding as Activated or Deactivated
- Busy: the following options apply to calls when the number is busy:
 - Activate: clicking this button will forward busy calls to the phone number provided
 - Deactivate: clicking this button will stop the forwarding of busy calls
 - Clear number: clicking this button will delete the phone number provided
 - Number: enter the phone number to forward calls to when the number is busy
 - Status: displays the status of busy call forwarding as Activated or Deactivated

Press the Refresh button to refresh the screen.

7.6 Call Waiting

The Call Waiting screen allows you to activate or deactivate call waiting functionality.



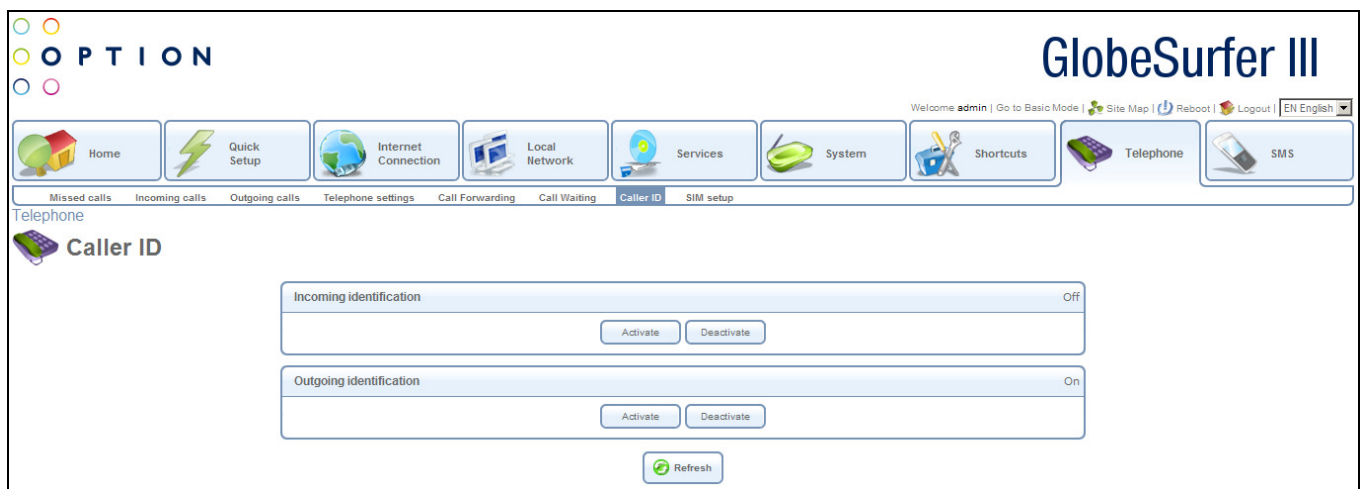
Use the Call Waiting screen to make the following settings:

- Call Waiting: displays the status of the call waiting functionality as Activated or Deactivated
- Activate: clicking this button will activate call waiting
- Deactivate: clicking this button will deactivate call waiting

Press the Refresh button to refresh the screen.

7.7 Caller ID

The Caller ID screen allows the system to identify the telephone number of the caller on either inbound or outbound calls.



Use the Caller ID screen to make the following settings:

Incoming identification: the following options apply to incoming telephone calls:

- Status: displays On or Off
- Activate: clicking this button will activate identification of caller for incoming calls
- Deactivate: clicking this button will deactivate identification of caller for incoming calls

Outgoing identification: the following options apply to outgoing telephone calls:

- Status: displays On or Off
- Activate: clicking this button will activate identification of caller for outgoing calls
- Deactivate: clicking this button will deactivate identification of caller for outgoing calls

Press the Refresh button to refresh the screen.

7.8 SIM Setup

The SIM card in the GlobeSurfer® III+ 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® III+ 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.

From this screen you can click on the tabs at the top right hand side to route to the following detailed screens:

- SIM PIN change – change the PIN on your SIM card
- SIM PIN enable – activates the use of a PIN on the SIM card
- SIM PIN2 change – change the PIN2 on your SIM card
- Unlock device – if your device is locked, it can be unlocked from here

7.8.1 SIM PIN Change

The screenshot shows the 'SIM PIN change' screen within the 'SIM setup' section of the GlobeSurfer III web interface. The interface includes a top navigation bar with 'OPTION' and 'GlobeSurfer III' branding, and a secondary bar with various system settings like Home, Quick Setup, Internet Connection, Local Network, Services, System, Shortcuts, Telephone, and SMS. Below these, a sub-menu lists 'Missed calls', 'Incoming calls', 'Outgoing calls', 'Telephone settings', 'Call Forwarding', 'Call Waiting', 'Caller ID', and 'SIM setup'. The main content area displays 'SIM PIN change' with a message: 'The PIN code cannot be changed as PIN is not enabled'. An 'OK' button is at the bottom.

To change the PIN of your SIM card or save the PIN on GlobeSurfer® III+, perform the following:

Enter the PIN code in the first field to be able to change any settings.

To be forced to enter the PIN code each time the GlobeSurfer® III+ is started, de-select the Enabled checkbox at Save PIN.

If you want to change the PIN code, enter a new PIN code in the New PIN code and Verify new PIN code fields.

Press the OK button to apply changes and go back to the previous screen.

7.8.2 SIM PIN enable

The screenshot shows the 'SIM PIN enable' screen within the 'SIM setup' section of the GlobeSurfer III web interface. The layout is similar to the previous screen, but the main content area displays 'SIM PIN enable'. It includes a 'PIN code:' label next to an empty text input field, and a 'PIN enabled:' label next to an unchecked checkbox labeled 'Enabled'. At the bottom, there are 'OK' and 'Cancel' buttons.

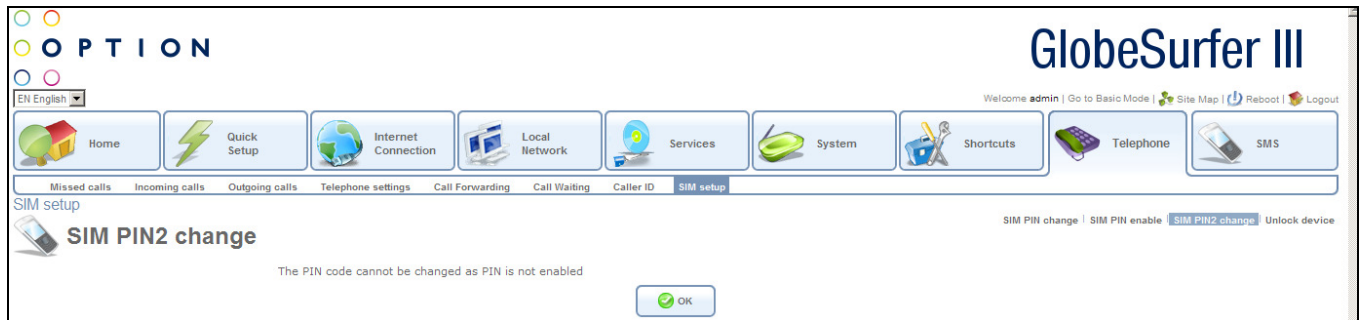
Use the SIM PIN enable screen to make the following changes:

- PIN code: enter the PIN code you wish to use
- PIN enabled: clicking this checkbox enables the PIN on your SIM card – to disable the PIN, de-select the checkbox

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

7.8.3 SIM PIN2 change



Use the SIM PIN2 change screen to make the following changes:

- New PIN2 code: enter the new PIN code you wish to use
- Verify new PIN2 code: enter the new PIN code again exactly as before to confirm the entry

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

7.8.4 Unlock device

In case the GlobeSurfer® III+ 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® III+:

Click the Unlock device tab - if the GlobeSurfer® III+ really is locked, the Unlock device screen will appear.

Unlock code: the unlock code from your ISP.

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.

8 SMS

The GlobeSurfer® III+ can send and receive SMS text messages. It supports both incoming and outgoing concatenated messages, and it can send flash-SMSs.

When the GlobeSurfer® III+ receives a new SMS text message, this is indicated by an envelope symbol shown on the GlobeSurfer® III+ display.

From this screen you can click on the tabs at the top left hand side to route to the following detailed screens:

- SMS create – allows you to type in a new SMS message
- Inbox - SMSs received + ability to reply/delete/archive/forward
- Outbox – list of SMSs in outbox
- Sent – list of SMSs sent out + ability to delete/forward/archive
- Drafts – list of SMSs saved as drafts and not yet sent out
- Templates – list of SMSs that can be used as template for future
- Archive – list of archived inbound or sent SMSs
- SIM card – list of SMSs stored on SIM card in GlobeSurfer® III+
- Settings - set SMSC number to send SMSs from GlobeSurfer® III+

8.1 SMS Create

Creating and sending SMS text messages:

Select the SMS Create tab.

Type your message text in the SMS message field.

The Characters left field shows how much space is left.

Enter the mobile number of the person you want to contact in the Phone numbers field. Use the standard mobile number format: +4976123456 for international, and 076123456 for national numbers.

Tip: You can enter several numbers separated by commas (no spaces allowed), up to a maximum of ten phone numbers.

OPTION

Welcome admin | Go to Basic Mode | Site Map | Reboot | Logout

Home Quick Setup Internet Connection Local Network Services System Shortcuts Telephone SMS

SMS create Inbox Outbox Sent Drafts Templates Archive SIM card Settings

SMS

SMS create

Write your SMS message here
SMS message:

Characters left: 160/1

Phone numbers:

Flash SMS: ☐ Enabled

Cancel Send SMS Save as template Save as draft

You can select the Flash SMS Enabled checkbox if you want the message text displayed immediately when received (not supported by all phones).

Click Send SMS when ready to send. You will be redirected to an intermediate page that gives you information about the send progress. After the SMS text message has been successfully sent, it will be stored in the Sent folder, see section o. Alternatively you can:

Click Save as draft to save in the Drafts folder for completion later.

Click Save as template to save the message as a template for future use.

Tip: GlobeSurfer® III+ supports concatenated SMS, which works as follows: if you want to send a longer than standard SMS of 160 characters you can type almost the equivalent of 4 standard messages (up to 609 characters). When you send the message it will be counted as separate messages.

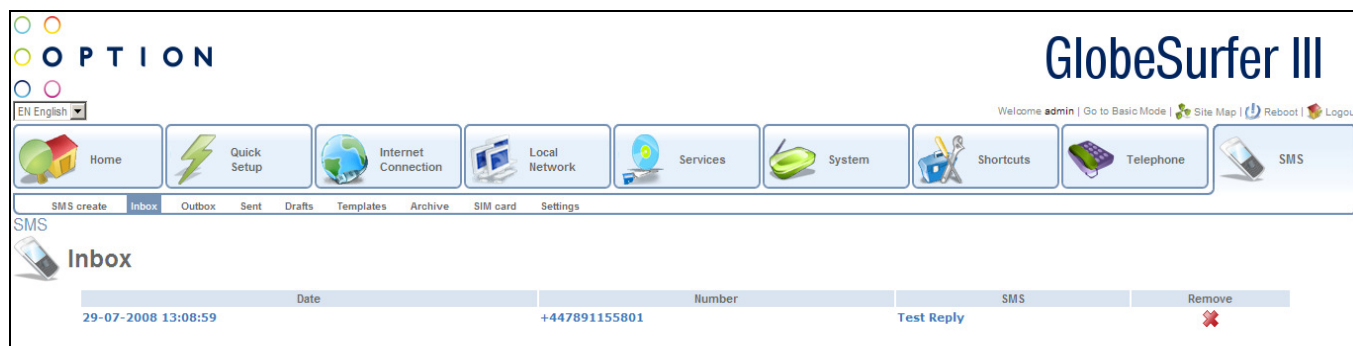
Note: When you send an SMS, you may incur a charge depending on your subscription with your mobile operator.

Press the Cancel button to reject changes and go back to the previous screen.

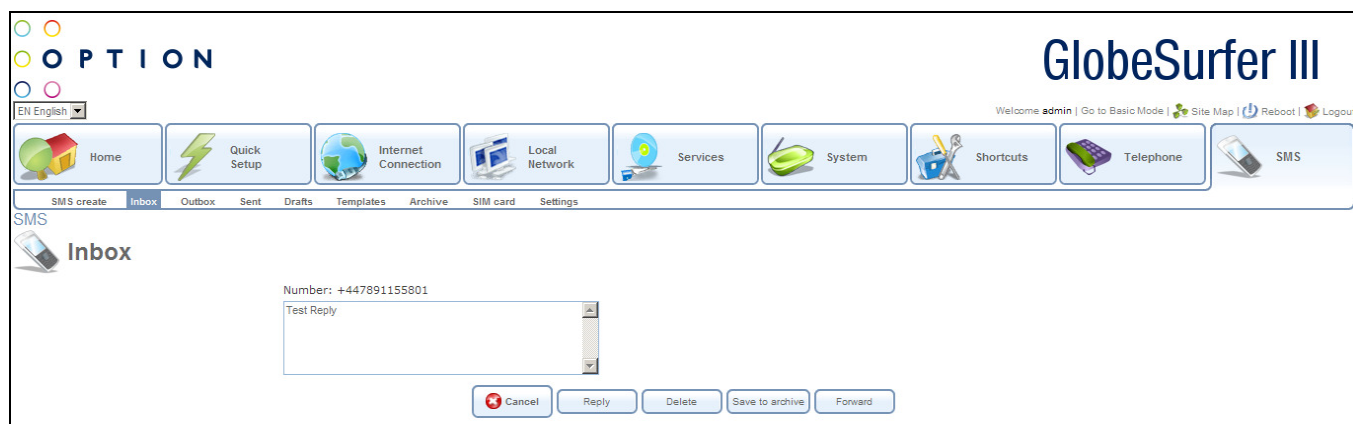
8.2 Inbox

Handling SMS text messages in the Inbox:

Select the Inbox tab to display the messages, with unread message in bold.



Click the SMS that you want to read. The message text is shown.



When you have read the SMS you can click on:

Reply: the message text is displayed in the SMS create tab with the phone number of the sender already filled in.

Delete: the SMS is permanently removed without confirmation.

Save to archive: the SMS is moved to the Archive tab, see section o.

Forward: the message text is displayed in the SMS create tab ready for you to enter a phone number.

Press the Cancel button to reject changes and go back to the previous screen.

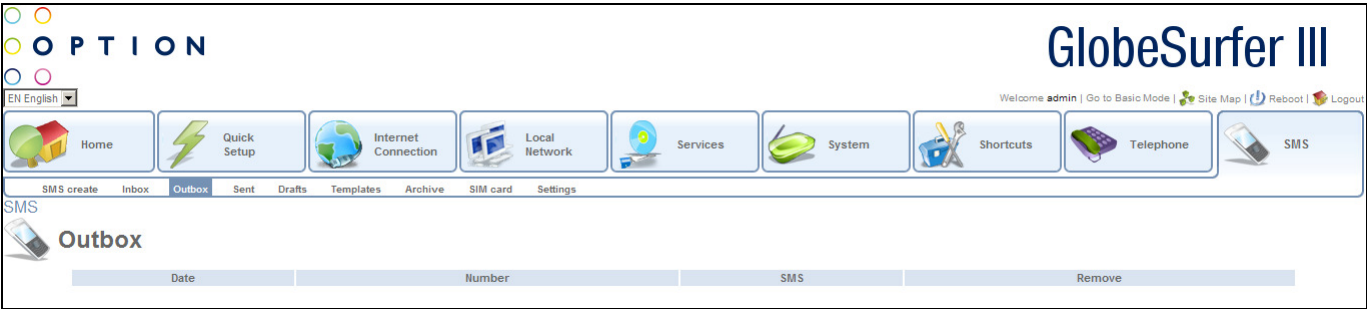
To delete an SMS from the list of messages in the Inbox tab:

Select the Inbox tab.

Click the Remove icon for the message that you want to delete; the SMS is permanently removed without confirmation.

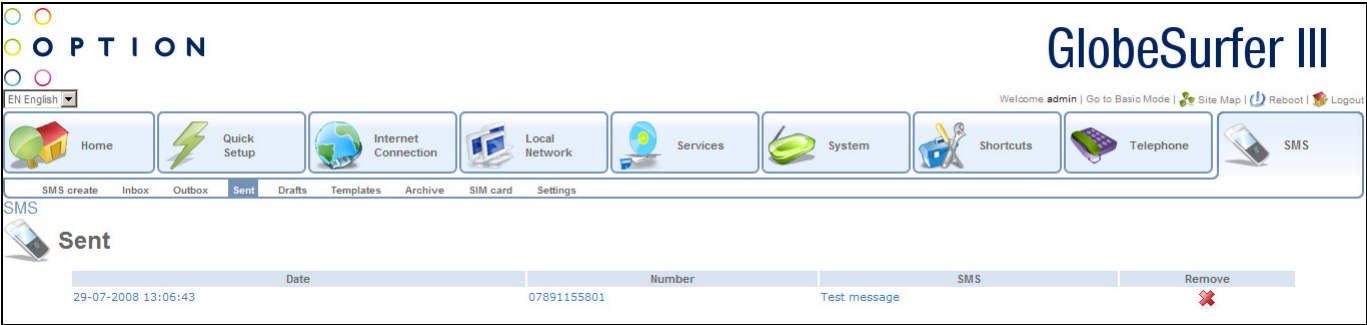
8.3 Outbox

After a SMS text message has been sent from your GlobeSurfer® III+ it will be stored temporarily in the Outbox folder until it is sent.



8.4 Sent

After a SMS text message has been sent from your GlobeSurfer® III+ it will be stored in the Sent folder. From here it is possible to open any sent message and choose to delete, forward or save it to the archive.



8.5 Drafts

While creating a new SMS text message from the SMS create tab it is possible to choose to save it as draft instead of sending it directly. This SMS will then be accessible from the Drafts folder. When clicking on an SMS in the Drafts folder, you will be directed back to the SMS create tab where it can be finalized.

Note that when an SMS text message in the Drafts folder has been opened and then sent, it will be removed from the Drafts folder.



8.6 Templates

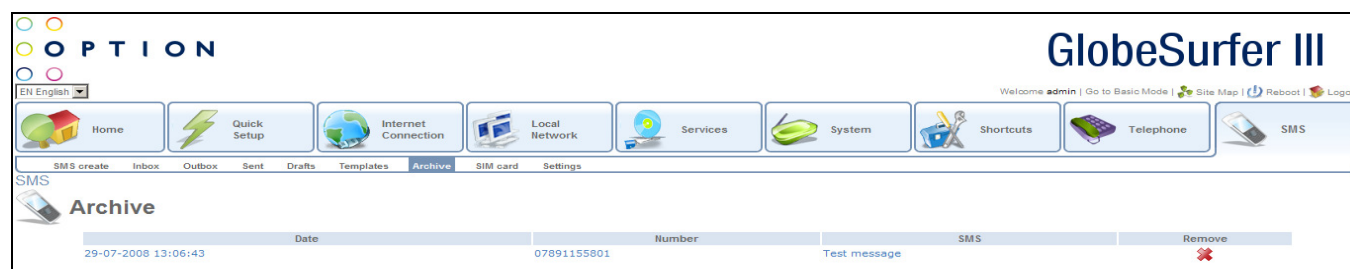
From the SMS create tab it is possible to choose to save a text message as a template instead of sending it directly. When a message is saved as a template, it can be loaded from the Templates folder. This is convenient when SMS messages are often sent to the same recipient or with similar content.

To remove a template, simply click the remove icon for that specific template.



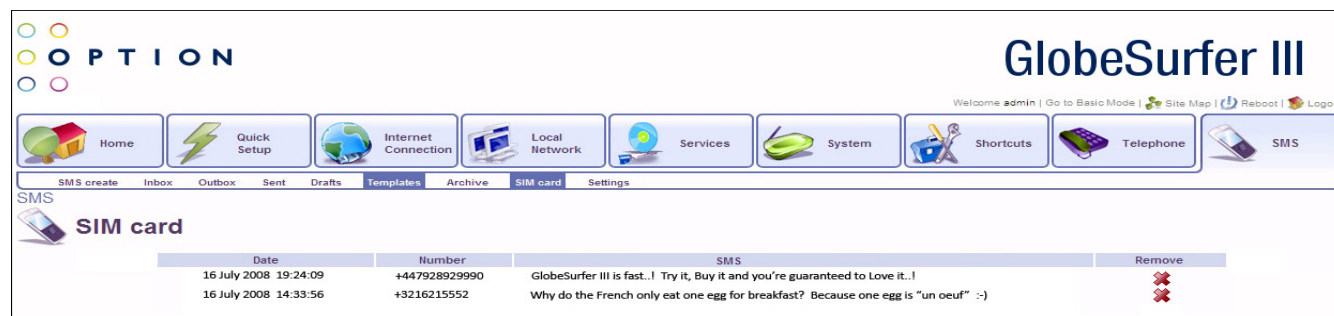
8.7 Archive

SMS text messages from Inbox or Sent folders can be stored in the archive. When selecting the Archive tab, stored messages are listed and it is possible to open any message and choose to delete, forward or reply to that message.



8.8 SIM card

The SIM card tab shows SMS text messages that are stored on the SIM card inserted in the GlobeSurfer® III+. After opening an SMS from the SIM card folder you can choose to delete it, reply to it, forward it or save it to the Archive folder.

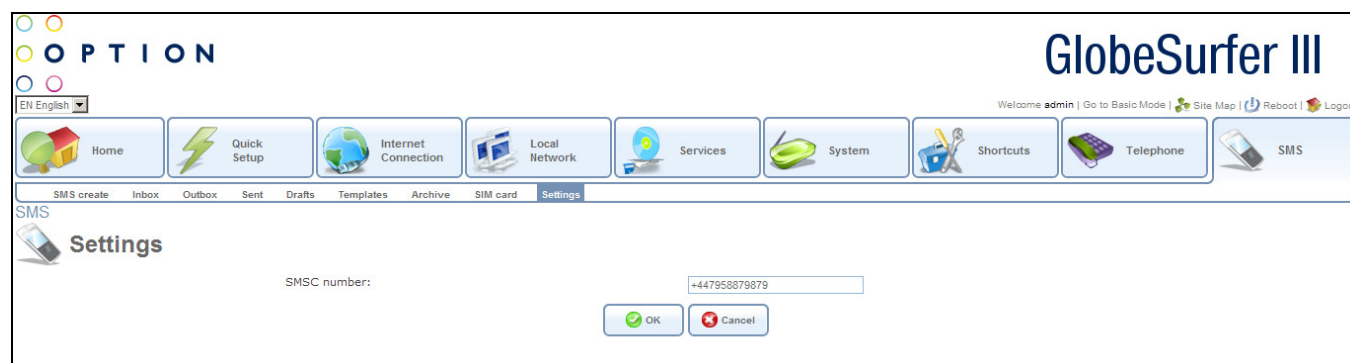


8.9 Settings

On the Settings tab it is possible to define the SMSC number which is the number to the Short Message Service Centre that will be used for sending SMS messages from your GlobeSurfer® III+ unit. This number is usually already filled in by default, but if necessary you can use the Settings tab to change it.

Press the OK button to apply changes and go back to the previous screen.

Press the Cancel button to reject changes and go back to the previous screen.



9 List of Acronyms

ALG Application-Level Gateway

API Application Programming Interface

CPE Customer Premise Equipment

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

DNS Domain Name System

DOCSIS Data Over Cable Service Interface Specification

DSL Digital Subscriber Line

FTP File Transfer Protocol

HomePNA Home Phoneline Network Alliance

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

POTS Plain Old Telephony Service

PPP Point-to-Point Protocol

PPTP Point-to-Point Tunnelling Protocol

RG Residential Gateway

RIP Routing Information Protocol

SNMP Simple Network Management Protocol

SPI Stateful Packet Inspection

TCP Transmission Control Protocol

TFTP Trivial File Transfer Protocol

UDP User Datagram Protocol

UPnP Universal Plug and Play

URL Universal Resource Locator

USB Universal Serial Bus

VPN Virtual Private Network

WAN Wide Area Network

10 Glossary

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) - a 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.

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.

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.

Broadcast: Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients.

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 your cable television.

Caller ID: A service within telephony networks that enables the receiver of a call to see the number calling.

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.

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.

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® III+ 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.

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.

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.

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, file from one computer to another.

Gateway: A device that acts as a central point for networked devices, receives transmitted messages, and forwards them. GlobeSurfer® III+ 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 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® III+) 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.

MPPE: Microsoft Point to Point Encryption (MPPE) is a means of representing Point to Point Protocol (PPP) packets in an encrypted form.

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.

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 file servers, 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.

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.

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 non-profit 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).

IPsec: 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).

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.

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 your base station's current settings 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 resetting the base station.

RJ-11 connector: An attachment used to join a telephone line to a device such as a modem or the external telephone lines.

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. Typically used in relation to Ethernet twisted pair cable. 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.

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.

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.