

# RedPort

**GMN**  
Global Marine  
NETWORKS



# Administrator's Guide

## RedPort Routers

**wXa-202; wXa-303; wXa-305; wXa-500;  
wXa-503; wXa-513**

## Table of Contents

TABLE OF CONTENTS .....	2
GMN REDPORT WXA ROUTER ADMINISTRATOR GUIDE REVISION HISTORY .....	6
1 ABOUT THIS GUIDE .....	7
1.1 HOW TO USE THIS GUIDE .....	7
1.2 CONVENTIONS .....	9
2 INTRODUCTION .....	10
2.1 REDPORT WXA ROUTER FEATURES .....	10
2.2 APPLICABLE SYSTEMS .....	11
2.3 TECHNICAL SPECIFICATIONS .....	11
2.4 MANUFACTURER CONTACT INFORMATION .....	12
2.5 WARRANTY .....	12
3 SETTING UP YOUR REDPORT WXA ROUTER .....	14
3.1 INVENTORY .....	14
3.2 QUICK START .....	14
QUICK START GUIDE FOR WXA .....	14
3.3 CONNECTING YOUR SYSTEM .....	14
3.4 POWER-UP .....	15
3.5 POWER-DOWN .....	16
4 LOGGING IN TO THE WEB ADMINISTRATOR .....	17
4.1 USING THE LAN TO CONNECT .....	17
4.2 USING WLAN (Wi-Fi) TO CONNECT .....	18
4.3 CHANGING THE WEB ADMINISTRATOR PASSWORD .....	19
5 INITIAL INTERFACE CONFIGURATION .....	20
5.1 LAN SETUP .....	20
5.2 WAN SETUP .....	20
5.3 WAN2 (BACKUP WAN) SETUP .....	22
5.4 WLAN (Wi-Fi) SETUP .....	22
5.5 VOIP INTERFACE (WXA-503 MODEL ONLY) .....	24
6 BACKUP/RESTORE SYSTEM CONFIGURATION .....	25

7	LOCKING THE CONSOLE .....	27
8	TIME CONFIGURATION WITH NTP .....	28
8.1	NTP CLIENT .....	28
8.2	NTP SERVER .....	28
8.3	CONFIGURING NTP TIME CLIENT ON PCs .....	29
8.4	INTERNET POLLING INTERVAL .....	30
9	FIREWALL RULES - BLOCK UNWANTED TRAFFIC TO/FROM THE INTERNET .....	31
9.1	CONFIGURING FIREWALL RULES .....	32
9.2	EXAMPLE OF FIREWALL RULE CONFIGURATION .....	32
9.3	SYSTEM VS. USER GENERATED FIREWALL RULES .....	34
10	VPN ACCESS THROUGH WAN .....	35
10.1	ENABLING PPTP .....	35
10.2	WINDOWS 7 PPTP CLIENT SETUP .....	36
10.3	MAC OS X CLIENT SETUP .....	37
11	CAPTIVE PORTAL .....	39
11.1	LIMITATIONS .....	42
11.2	SETTING UP THE CAPTIVE PORTAL .....	42
11.3	BYPASSING THE CAPTIVE PORTAL .....	44
11.4	SETTING UP FOR THE BUY NOW LINKS .....	45
11.5	PINCODE RESTRICTIONS .....	47
11.6	PINCODE AUTHENTICATION .....	47
11.7	THE CDR AND PINCODE CALL LOGS .....	48
12	ASSIGNING STATIC IP ADDRESSES TO PCS ON THE LAN/WLAN .....	50
13	CACHING PROXY SERVER .....	52
13.1	LIMITATIONS .....	52
13.2	CUSTOMIZING THE PROXY SERVER .....	52
13.3	TRANSPARENT VS. MANUAL PROXY .....	58
13.4	REBUILD PROXY CACHE .....	62
14	CONTROLLING ACCESS TO THE WEB .....	64
14.1	BLACKLISTS .....	65
14.2	DYNAMIC CONTENT FILTERING .....	66
14.3	CUSTOM DESTINATIONS .....	67
14.4	ACCESS CONTROL LISTS (ACL) .....	68

14.5	WHITELISTS .....	69
14.6	APPLY YOUR CONFIGURATION .....	70
15	WEB LOGGING .....	71
15.1	CONFIGURATION.....	71
15.2	DISK-FULL ISSUES .....	71
15.3	REPORTS .....	72
16	GPS TRACKING .....	75
17	DISABLING SKYPE AND OTHER P2P APPLICATIONS.....	76
18	CONFIGURING FAILOVER FROM PRIMARY TO BACKUP SATELLITE LINK .....	77
18.1	SCHEME 1 - CLIENT BASED DNS LOOKUPS.....	78
18.2	SCHEME 2 - STATIC ROUTES TO DNS SERVERS.....	79
18.3	CONFIGURING FAILOVER POOL.....	81
18.4	POLICY BASED ROUTING.....	83
18.5	FAILOVER AND FIREWALL RULES .....	84
18.6	FAILOVER AND CAPTIVE PORTAL .....	85
18.7	FAILOVER AND PROXY WEB SERVICES.....	86
18.8	MANUAL FAILOVER .....	87
18.9	SWAPPING WAN/WAN2 CABLES .....	90
18.10	TESTING FAILOVER .....	90
18.11	MONITORING FAILOVER STATUS .....	90
19	FAILOVER TO SERIAL/USB SATELLITE TERMINAL .....	91
19.1	MANUAL FAILOVER .....	91
19.2	MANUAL FAILOVER USING TELNET .....	93
19.3	AUTOMATIC FAILOVER WITH XGATE.....	94
20	LOAD BALANCING.....	95
20.1	CREATING LOAD BALANCING POOL.....	96
20.2	STICKY CONNECTIONS .....	96
20.3	LOAD BALANCING AND THE PROXY SERVER .....	97
21	POWER-ON/OFF PROCEDURES .....	98
22	RESETTING TO FACTORY DEFAULTS.....	100
23	FIRMWARE UPGRADE.....	102
23.1	FIRMWARE UPGRADE FROM WEB INTERFACE .....	102
23.2	FIRMWARE UPGRADE FROM CONSOLE .....	104

APPENDIX A: RESOURCES AND QUICK START GUIDE .....	106
APPENDIX B: OPENING A CONSOLE WINDOW.....	110

## GMN RedPort wXa Router Administrator Guide Revision History

Date	Revision	Author
February 10, 2010	Revision 1.06	Luis Soltero, Ph.D., MCS
May 22, 2012	Revision 2	Susan Beck

## 1 About this guide

This document is divided into the following chapters:

1. About this guide
2. Introduction
3. Setting up Your RedPort wXa Router
4. Logging in to the Web Administrator
5. Initial Interface Configuration
6. **5.6 Backup/Restore System Configuration**
7. Locking the Console
8. Time Configuration with NTP
9. Firewall Rules - Block Unwanted Traffic to/from the Internet
10. VPN access through WAN
11. Captive Portal
12. Assigning Static IP addresses to PCs on the LAN/WLAN
13. Caching Proxy Server
14. Controlling Access to the Web
15. Web Logging
16. GPS Tracking
17. Disabling Skype and other P2P Applications
18. Configuring Failover from Primary to Backup Satellite Link
19. Failover to Serial/USB Satellite Terminal
20. Load Balancing
21. Power-On/Off Procedures
22. Resetting to Factory Defaults
23. Firmware Upgrade
- Appendix A: Resources and Quick Start Guide
- Appendix B: Opening a Console Window

---

### 1.1 How to Use this Guide

This guide is intended for administrators of RedPort wXa routers.

The following chapter references will help you in configuring your RedPort wXa router whether you are performing an initial configuration or implementing one of the more advanced configuration schemes. Note these chapter references are internal links for this Administrator Guide.

## 1.1.1 Initial Configuration

For initial configuration, refer to the following chapters:

- Introduction
- Setting up Your RedPort wXa Router
- Logging in to the Web Administrator
- Initial Interface Configuration

## 5.6 Backup/Restore System Configuration

- Locking the Console
- Power-On/Off Procedures
- Resetting to Factory Defaults
- Firmware Upgrade
- Appendix A: Resources and Quick Start Guide
- Appendix B: Opening a Console Window

## 1.1.2 Advanced Configurations

Find information for more advanced configurations in the following chapters:

- Time Configuration with NTP
- Firewall Rules - Block Unwanted Traffic to/from the Internet
- VPN access through WAN
- Captive Portal
- Assigning Static IP addresses to PCs on the LAN/WLAN
- Caching Proxy Server
- Controlling Access to the Web
- Web Logging
- GPS Tracking



Disabling Skype and other P2P Applications  
Configuring Failover from Primary to Backup Satellite Link  
Failover to Serial/USB Satellite Terminal  
Load Balancing

---

## 1.2 Conventions

This document uses the following typographical conventions:

- **Command** and **option names** appear in bold type in definitions and examples.
- *Variable* information appears in italic type.
- Screen output, examples and code samples appear in `courier` type.

In addition, the following symbols may be used in command syntax definitions.

- Square brackets [ ] surround optional items.
- Angle brackets < > surround user-supplied values.
- Pipe symbol | separates mutually exclusive values for an argument.

---

**Note:** General notes will appear like this.

---

Comments will appear in a box like this.

---

**Warning:** Warnings will appear like this.

---

Web links will look like this: [www.globalmarinenet.com](http://www.globalmarinenet.com)  
[www.redportglobal.com](http://www.redportglobal.com)

## 2 Introduction

Global Marine Networks (GMN), the leaders in advancing satellite data speeds and services, helps Fixed and Mobile Satellite Services providers and their customers by offering the industry's fastest, most reliable and easy-to-use email, web, VoIP and other hardware and software services to maritime, oil and gas, first responder and business continuity users. The company's products include XGate high-speed satellite email, WeatherNet weather and oceanographic data software, and vessel tracking systems.

Ship to shore network management solutions are sold by GMN under the RedPort Global brand name at [www.redportglobal.com](http://www.redportglobal.com) and as white-label solutions for the world's premier satellite data service providers.

GMN has numerous awards and certifications for technical innovation and holds pending patents on its products. For more information on how GMN is Making Airtime Count™ - whether ship to shore, or in remote or emergency communications environments visit [www.globalmarinenet.com](http://www.globalmarinenet.com).

---

### 2.1 RedPort wXa Router Features

Welcome to the RedPort wXa satellite appliance. With wXa configured for use with your satellite broadband device you will be able to increase satellite data transfer efficiency, decrease airtime costs, and generate revenue by selling services to end users.

This guide covers several models of RedPort wXa routers. Features vary by model. The RedPort router that you purchased may have some or all of the features listed here.

wXa is a full-featured industrial router with web caching and compression built into it. With local caching and fast, reliable, data compression, you will be able to realize up to 5x faster Internet browsing. Data caching and compression speeds up network access to data files resulting in faster download times that can produce dramatic airtime savings.

Standard controls prevent airtime abuse and unwanted costly transmissions. Optional captive portal pincode sales to passengers, crew and other end users, will generate an ongoing revenue

stream. Users have a simple, convenient, and cost effective way to access satellite data services and managers have an additional income stream based on time or data consumed. Resellers have the option of customizing the captive portal login page with a link to their shopping cart for immediate and convenient end user sales on the spot.

wXa Core Features include:

- Local web page caching plus over the air web compression are combined to dramatically increase web browsing performance and reduce airtime expense.
- Captive portal pincodes control time or data used by user. Detailed activity logs help eliminate unwanted usage.
- Web site controls such as black/white listing.
- Firewall filtering by MAC address, TCP/IP address, and/or TCP port number.
- Automatic transparent failover from a primary link to a secondary link assuring smooth service backup delivery with no disruptions.
- Bandwidth shaping QoS for high priority data.
- Efficient support through IT remote network access via VPN for maintenance and support.
- Option for new revenue generation by selling voucher pincodes to crew and passengers.
- Works with any broadband satellite device such as Fleet Broadband, BGAN, VSAT, Iridium OpenPort, and Thuraya DSL.
- Can be configured to be a Wi-Fi hotspot.

---

## 2.2 Applicable Systems

There are several models of the wXa available. These include:

- 19" 1U wired rack mount with 1 LAN and 2 WAN ports.
- Wired wall mount or desktop unit with 1 LAN and 2 WAN ports.
- Wi-Fi wall mount unit with 802.11 a/b/g interface, 1 LAN, and 2 WAN ports.
- Small desktop unit with 1 LAN and 1 WAN port, WiFi capable

---

## 2.3 Technical Specifications

wXa-300 and wXa-500 Series

Dimensions:

- Wall mount units 7.9" x 6.3" x 2.4" (200mm x 160mm x 60mm)
- 19" 1U rack mount enclosure

Weight: 0.99 lbs (0.45 Kg)



Operating Temperature: 32°F to 122°F (0°C to 50°C)

Internal Drive: 8Gb SLC SSD

Ram: 512 Mb

Certifications: FCC, CE, and RoHS

Wi-Fi: 802.11 a/b/g

Power: 12VDC - 2A (Operating range 9-18V DC)

wXa-200 Series

Dimensions: 5.5" x 6.3" x 1.2" (140 x 160 x 30 mm)

Power: 12VDC

---

## 2.4 Manufacturer Contact Information

RedPort wXa routers are manufactured by:

**Global Marine Networks, LLC**

2668 Jericho Rd,

Maryville, TN 37803

Tel: +1.865.379.8723

Fax: +1.865.681.5017

Web: [www.globalmarinenet.com](http://www.globalmarinenet.com)

Email : [info@globalmarinenet.com](mailto:info@globalmarinenet.com)

Internal components manufactured in Germany, Taiwan, and USA.

Assembled in the Netherlands.

---

## 2.5 Warranty

RedPort routers are warranted for a period of 12 months. If the product malfunctions within 12 months of purchase the product is eligible for RMA (Return Material Authorization) replacement or repair at the manufacturer's discretion. No units will be accepted without an RMA. Units received without an RMA number will be returned unopened.

This warranty does not cover:

- Units damaged by environmental conditions such as operating in excessively humid, hot, cold, or salty environments
- Direct exposure to water, sunlight, or elements
- Reverse electrical polarity or operating with improper voltage or current
- Physical damage to the case or any of its internal components
- Inappropriate electrical connections to any of the devices physical ports
- Exposure to strong microwave or other EMF radiation such as that caused by lightning or other radio transmitting equipment
- Any other environmental, electrical, or mechanical exposure deemed inappropriate by the manufacturer

## 2.5.1 RMA Request

To request an RMA send an e-mail to [support@globalmarinenet.com](mailto:support@globalmarinenet.com) with the following information:

- Name and address
- Original order number and/or copy of the order receipt
- Description of the problem

## 2.5.2 Shipping

Shipping costs and insurance from origin to Global Marine Networks is the responsibility of the end user. Global Marine Networks will cover return costs via UPS Ground to any USA location. Customers are responsible for covering international shipping costs.

Items with RMA approval should be shipped to the manufacturers address listed in section 2.4. The RMA number should be clearly marked on the outside of the package, the packing slip, and shipping label.

## 3 Setting up Your RedPort wXa Router

---

### 3.1 Inventory

The following parts are **included** with the purchase of your RedPort wXa Router:

- RedPort router
- DB-9 NULL modem cable (except wXa-200 series models)
- US or EU compatible external power supply (except wXa-200 series models)
- wXa documentation DVD

### 3.2 Quick Start

A Quick start guide is included in Appendix A of this manual and on the DVD included with your purchase of the RedPort wXa Router. A link to the Quick start guide in Appendix A is included here for convenience:

[Quick Start Guide for wXa](#)

### 3.3 Connecting Your System

wXa comes in several configurations which include a 19" 1U rack mount, a wired desktop/wall mount unit, and a Wi-Fi hotspot. All configurations come with at least one RJ45 ethernet connector. The Wi-Fi versions supports 802.11 a/b/g protocols and can be configured as an access point for a wireless network.

Interfaces are defined as:

- LAN - marked externally as ETH0
- WAN - marked externally as ETH1
- WAN2 - marked externally as ETH2, aka OPT1
- WLAN - Wi-Fi Hotspot, aka OPT2
- VOIP – Voice Over IP (available on wXa-503 model only)

Port	Purpose
ETH0	Connect this port to your Local Area Network (LAN)
ETH1	Connect this port to your Primary Satellite Unit
ETH2	Connect this port to your Backup Satellite Unit (if applicable)
Console Port	Connect to laptop or PC with DB-9 NULL modem cable (Note: USB adapter may be needed for your laptop or PC)

### 3.3.1 ETH0

The LAN port (ETH0) should be connected to your local area network. If your network has only one PC then it can be directly connected to the LAN port on the router. If, however, more than one PC is to be connected on the local LAN then a hub or switch should be connected to the LAN port. Any hub or switch will do. These are readily available at many computer retail stores.

### 3.3.2 ETH1

The primary broadband satellite link should be connected to ETH1 or the WAN Port. This could be a VSAT, FleetBroadband, or Iridium OpenPort for example. ETH2 (WAN2) should be left disconnected for a single satellite installation.

### 3.3.3 ETH2

Installations with redundant satellite systems should connect the backup unit to ETH2 or the WAN2 port. Note that special setup is required to configure automatic failover from the primary unit on WAN to the backup unit on WAN2. See [Configuring Failover from Primary to Backup Satellite Link](#) for details on configuring automatic failover.

### 3.3.4 Serial Port (Console Port)

A DB9 serial port is provided for access to the wXa's console for maintenance. Under normal operating conditions there should be no need to ever access the console port. The console provides detailed status messages on system boot up and is used for specialized system maintenance. The console can be used, for example, to recover from a lost **Web Administrator** password. Details on how to access the console are found in [Appendix B](#).

## 3.4 Power-up

Most wXa routers are supplied with either a US or EU power adapter. Alternately, the unit can be powered by any DC source with voltages between 9-18V. Plugging the unit into the power source will cause it to start up.

---

**Note:** There is no power on/off switch on the wXa.

---

Under normal conditions, it should take between 1 and 3 minutes to fully boot up the router. However, if power has been removed from the unit without properly shutting it down and the internal disk has a lot of data on it, then it could take considerable more time to startup the system.

**Best practice:** Do not configure the system until it is fully operational. The system run status can be monitored on the **Web Administrator** System Overview page as described in [Power-On/Off Procedures](#).

---

## 3.5 Power-down

wXa has an internal solid state disk drive (SSD) used to cache web pages under normal operation. (Exception: the wXa-202 has a CF card.) As with all such SSD systems, care should be taken to properly shutdown the unit before power is removed. Removing the power without proper shutdown can result in lost files. Additionally, on re-start, a full file system check and disk rebuild must take place before the unit begins its normal power-up sequence.

To power-down the unit:

1. login to **Web Administrator**
2. Choose the **Diagnostics** Menu
3. Select **Halt system**

**Best practice:** Wait one full minute before removing power from the unit. See [Power-On/Off Procedures](#) for details.



## 4 Logging in to the Web Administrator

Your router's internal administrative web page must be accessed to configure the unit. You can access the **Web Administrator** through either the LAN or Wi-Fi port.

---

### 4.1 Using the LAN to Connect

To access the **Web Administrator** through the LAN, connect a PC to the port. The PC should be configured to automatically acquire its network settings via DHCP.

Once connected, start a web browser and enter URL **http://<IP address of wXa LAN >** to connect to the wXa **Web Administrator** page.

---

**Note:** IP address 192.168.10.1 is the default IP address for the wXa LAN.

---

The login for the **Web Administrator** is

Username: admin

Password: webxaccess

The **Web Administrator** page opens:

Global Marine Networks  
webX accelerator  
webxaccelerator.gmn-usa.com

System Interfaces Firewall Services VPN Status Diagnostics

## System Overview

System information	
Name	webxaccelerator.gmn-usa.com
Version	1.2.3.23x-RELEASE built on Mon Mar 12 22:33:29 UTC 2012
Run Status	Operational
Uptime	00:17
Default (WAN)	308299/76146 (301 KB/74 KB) <a href="#">Change default route/interface</a>
State table size	26/10000 <a href="#">Show states</a>
MBUF Usage	261 /645
CPU usage	<div><div></div></div> 1%
Memory usage	<div><div></div></div> 14%
Disk usage	<div><div></div></div> 27%

webXaccelerator is © 2010 by Global Marine Networks LLC. All Rights Reserved. [\[view license\]](#)

## 4.2 Using WLAN (Wi-Fi) to Connect

To access the **Web Administrator** through a Wi-Fi connection, configure your PC to link to the wXa access point.

Password: **wXa**

Once connected, start a web browser and enter URL **http://<IP address of wXa LAN >** to connect to the wXa **Web Administrator** page.

**Note:** IP address 192.168.10.1 is the default IP address for the wXa LAN.

The login for the Web Administrator is

Username: admin

Password: webxaccess

The **Web Administrator** page opens:

Global Marine Networks
webX accelerator
webxaccelerator.gmn-usa.com

System
Interfaces
Firewall
Services
VPN
Status
Diagnostics

## System Overview

System information	
Name	webxaccelerator.gmn-usa.com
Version	<b>1.2.3.23x-RELEASE</b> built on Mon Mar 12 22:33:29 UTC 2012
Run Status	Operational
Uptime	00:17
Default (WAN)	308299/76146 (301 KB/74 KB) <a href="#">Change default route/interface</a>
State table size	26/10000 <a href="#">Show states</a>
MBUF Usage	261 /645
CPU usage	<div><div></div></div> 1%
Memory usage	<div><div></div></div> 14%
Disk usage	<div><div></div></div> 27%

webXaccelerator is © 2010 by Global Marine Networks LLC. All Rights Reserved. [\[view license\]](#)

## 4.3 Changing the Web Administrator Password

The password for the **Web Administrator** should be changed to secure the router. Go to **System->General** to set a new password. Click the **Save** button at the bottom of the form to set the new password.

**Warning:** Changing the user name from **admin** is not recommended.

Username	<input type="text" value="admin"/>
If you want to change the username for accessing the webGUI, enter it here.	
Password	<input type="text"/>
	<input type="text" value="(confirmation)"/>
If you want to change the password for accessing the webGUI, enter it here twice.	

## 5 Initial Interface Configuration

The following sections describe how to initially configure the LAN, WAN, WAN2, WLAN, and VOIP Interfaces.

### 5.1 LAN Setup

By default, the LAN port (ETH0) is setup with IP address 192.168.10.1 serving DHCP IP addresses in the range 192.168.10.10-245. *There should be no need to change the defaults unless these addresses conflict with a network already in place.*

The following steps should be followed if you need to change the IP address of the LAN interface:

1. Login to the **Web Administrator**
2. Select **Interfaces->LAN**
3. Enter < **new IP address**> and < **netmask**>
4. Select **Services->DHCP server**
5. Select the **LAN** tab
6. Modify the DHCP **Range** to match the IP address set in 2 above
7. Verify **Enable DHCP server on LAN interface** is checked
8. Click the **Save** button at the bottom of the form

### 5.2 WAN Setup

By default, the primary WAN port (ETH1) is setup to acquire its configuration via DHCP. For many satellite systems, this default is fine and no further configuration is required.

**Warning:** When configuring WAN with DHCP note that the DHCP server must be fully operational before the wXa is powered on or the unit will fail to obtain DNS entries preventing access to the internet. This is a common problem with BGAN

and FB systems where users power them up for short periods of time and then power them off when done.

## 5.2.1 Assigning a Static IP Address

**Best practice:** It is highly recommended that the WAN be assigned a static IP address.

To configure the WAN interface for static IP addressing use the following steps:

1. Login to the **Web Administrator**
2. Select **Interfaces->WAN**
3. For **Type**, select **STATIC** from the drop-down menu
4. In the Static IP Configuration area, enter < **IP address**> and <**netmask**>. The satellite manufacturer provides this information.
5. Enter < **IP address of Gateway**>. Also provided by the satellite manufacturer.
6. Click **Save** at the bottom of the form.

Interfaces: WAN	
<b>General configuration</b>	
Type	Static
MAC address	<input type="text"/> <a href="#">Copy my MAC address</a> <small>This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank</small>
MTU	<input type="text"/> <small>If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.</small>
<b>Static IP configuration</b>	
IP address	<input type="text" value="96.38.22.218"/> / <input type="text" value="28"/>
Gateway	<input type="text" value="96.38.22.217"/>

## 5.2.2 Configuring the DNS Servers

To configure the DNS servers, follow these steps:

1. Go to **System->General**
2. Enter the DNS addresses provided by the satellite provider

**Note:** If the DNS servers are not known then enter 208.67.222.222 and 208.67.220.220 which belong to [www.opendns.org](http://www.opendns.org), a well known free provider of DNS services.

3. From the **Use gateway** pull-down menu, select the gateway. Selecting **Default** means the default gateway will be used to route traffic to the corresponding DNS server.
4. Uncheck **Allow DNS server list to be overridden by DHCP/PPP on WAN**
5. Click **Save** at the bottom of the form

DNS servers

DNS server	Use gateway
208.67.222.222	default ▼
208.67.220.220	default ▼
	default ▼
	default ▼

IP addresses: these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, select the gateway for each DNS server. You should have a unique DNS server per gateway. DNS servers which are physically or directly connected to an interface should be added to the list with gateway value of "default".

☐ **Allow DNS server list to be overridden by DHCP/PPP on WAN**  
If this option is set, webXaccelerator will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.

Please read [Configuring Failover from Primary to Backup Satellite Link](#) if you intend to operate in a failover environment where the satellite unit in WAN2 takes over if WAN1 fails.

---

## 5.3 WAN2 (Backup WAN) Setup

Backup satellite port, WAN2 (ETH2 aka OPT1) is disabled by default.

To enable the port, login to the **Web Administrator** and then go to **Interfaces->WAN2** to configure it. Follow the instructions in [WAN Setup](#) to configure the interface.

---

## 5.4 WLAN (Wi-Fi) Setup

Wi-Fi is enabled by default on Wi-Fi enabled units. The Wi-Fi (WLAN) interface is configured by default with IP address **192.168.20.1** with DHCP enabled serving IP addresses in the range **192.168.20.10-245**. The default configuration uses WPA2 security.

The default login is

```
SSID: webXaccelerator
Pre-Shared Key (PSK): webXaccelerator
```

**Warning:** At minimum, the Pre-Shared Key (PSK) should be changed to secure the network.

The following steps will guide you through modifying the Wi-Fi settings:

1. Login to the **Web Administrator**
2. Go to **Interfaces->WLAN**
3. Enter a new **SSID**, if desired
4. Enter a new **WPA Pre Shared Key (PSK)**

The screen shots below depict the fields that should be modified when setting the access point **SSID** and the **PSK**.

Wireless configuration	
<b>Standard</b>	802.11g
<b>Mode</b>	Access Point
<b>802.11g OFDM Protection Mode</b>	Protection mode off For IEEE 802.11g, use the specified technique for protecting OFDM frames in a mixed 11b/11g network.
<b>SSID</b>	webXaccelerator
<b>802.11g only</b>	<input checked="" type="checkbox"/> When operating as an access point in 802.11g mode allow only 11g-capable stations to associate (11b-only stations are not permitted to associate).

<b>WEP</b>	<input type="checkbox"/> <b>Enable WEP</b> <div style="display: flex; justify-content: space-between;"> <div> Key 1: <input type="text"/>  Key 2: <input type="text"/>  Key 3: <input type="text"/>  Key 4: <input type="text"/> </div> <div> TX key  <input type="radio"/>  <input type="radio"/>  <input type="radio"/>  <input type="radio"/> </div> </div> <p>40 (64) bit keys may be entered as 5 ASCII characters or 10 hex digits preceded by '0x'.  104 (128) bit keys may be entered as 13 ASCII characters or 26 hex digits preceded by '0x'.</p>
<b>WPA</b>	<input checked="" type="checkbox"/> <b>Enable WPA</b> <div style="display: flex; justify-content: space-between;"> <div>WPA Pre Shared Key</div> <div>PSK: <input type="text"/></div> </div> <p>Passphrase must be from 8 to 63 chars.</p>
<b>WPA Mode</b>	WPA2
<b>WPA Key Management Mode</b>	Pre Shared Key

To change the IP address of the Wi-Fi interface and the DHCP range, follow the steps in [LAN Setup](#).

---

**Warning:** WLAN and LAN must be on different subnets. The reason for this is because the captive portal must have an IP address on the selected interface to function. Bridged networks do not have an IP address; therefore, they are incompatible with the captive portal. The same is true for the web proxy and compression. *Do not bridge the Wi-Fi LAN (WLAN) with the Ethernet LAN even though the user interface will permit it. Doing so will break the compression and captive portal features in wXa.*

---

## 5.5 VOIP Interface (wXa-500 series only)

The RedPort wXa-500 series models include a VoIP system in addition to the wXa router as described in this Administrator Guide. While you will still use the **wXa Web Administrator** to configure your router, a different user interface is used to configure the VoIP system functionality. Access to the VoIP Web Administrator is described below.

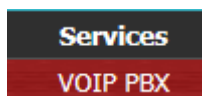
---

**Warning:** Within the **wXa Web Administrator**, there are menu selections for VoIP. One selection is at **Interfaces > VOIP**, the second is **Firewall > Rules > VOIP**. *Do not use these menus for configuring VOIP on your system.*

---

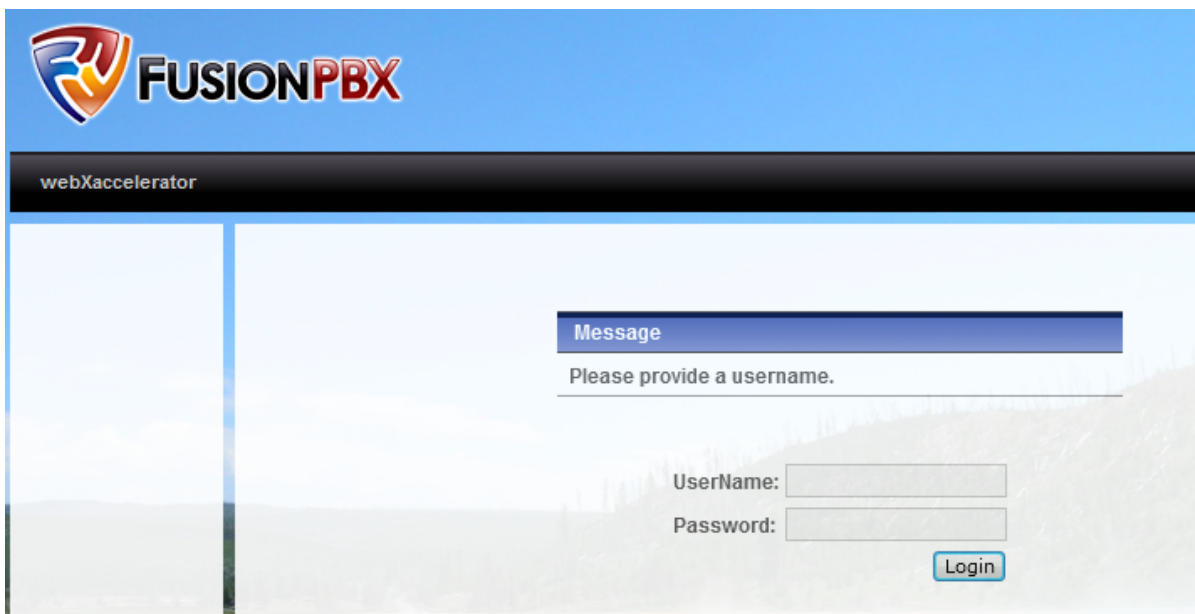
### 5.5.1 Accessing the VoIP Web Administrator from the wXa Web Administrator

If you have the wXa-500 series router, you can access the **VoIP Web Administrator** site from the **wXa Web Administrator** by going to **Services > VOIP PBX**:



The **VoIP Web Administrator** site is opened:





The superadmin login should be used for configuration of the VoIP system. This login displays the full functionality and configuration of your system.

```
Login: superadmin
Password: webxaccess
```

## 5.5.2 Additional information for RedPort VoIP

Additional information for configuring the wXa-500 series models for VoIP can be found in the RedPort VoIP Administrator Guide available from RedPort Global.

## 5.6 Backup/Restore System Configuration

It is highly recommended that you backup your router configuration after completing the initial installation.

To back up the configuration:

1. Login to the **Web Administrator**
2. Go to **Diagnostics->Backup/Restore**
3. From the **Backup Configuration/Backup area** dropdown menu, select **ALL**

## 4. Click **Download configuration**

The screenshot displays two sections of the RedPort Web Administrator interface. The top section, titled "Backup configuration", contains instructions to download the system configuration in XML format. It features a "Backup area:" dropdown menu set to "ALL", an unchecked checkbox for "Do not backup package information.", and a "Download configuration" button. The bottom section, titled "Restore configuration", contains instructions to open a webXaccelerator configuration XML file and click the button below to restore the configuration. It features a "Restore area:" dropdown menu set to "ALL", a "Choose File" button next to the text "No file chosen", and a "Restore configuration" button. A red "Note:" indicates that the firewall may need to be rebooted after restoring the configuration.

**Backup configuration**

Click this button to download the system configuration in XML format.

Backup area: ALL

☐ Do not backup package information.

Download configuration

**Restore configuration**

Open a webXaccelerator configuration XML file and click the button below to restore the configuration.

Restore area: ALL

Choose File No file chosen

Restore configuration

**Note:**  
The firewall may need to be rebooted after restoring the configuration.

To restore the configuration:

1. Login to the **Web Administrator**
2. Go to **Diagnostics->Backup/Restore**
3. From the **Restore Configuration/Restore area** dropdown menu, select **ALL** (or appropriate area)
4. Click **Restore configuration**

## 6 Locking the Console

The console can be password protected for installations where security is a concern.

**Warning:** Once the console is password protected there is no way to reset the system or the **Web Administrator** password should it be lost. If the password is lost, the unit will have to be shipped back to the manufacturer for unlocking. Please make certain that the password is stored in a secure recoverable location, should you choose to use this option.

To password protect the console:

1. Login to the **Web Administrator**
2. Go to **System->Advanced**
3. In the **Miscellaneous** section, check **Password protect the console menu**

Miscellaneous	
Device polling	<input type="checkbox"/> <b>Use device polling</b> Device polling is a technique that lets the system periodically poll network devices for new data instead of relying on interrupts. This prevents your webGUI, SSH, etc. from being inaccessible due to interrupt floods when under extreme load. Generally this is not recommended. Not all NICs support polling; see the webXaccelerator homepage for a list of supported cards.
Console menu	<input checked="" type="checkbox"/> <b>Password protect the console menu</b> Changes to this option will take effect after a reboot.

## 7 Time Configuration with NTP

The wXa router can synchronize its time with time keepers on the internet as well as serve time to PCs on a local network using NTP, the Network Time Protocol.

### 7.1 NTP Client

The wXa router is both an Internet time client and a LAN time server. When powering on, the unit will establish a connection to the Internet to synchronize its clock. This happens whether the NTP time client is enabled or not. No further access to the Internet is done if the NTP time client is disabled. The NTP time client is disabled by default on the wXa router.

If the NTP time client is enabled then wXa will routinely access the internet keeping its internal clock synchronized with time keepers on the internet.

To enable the time client:

1. Login to the **Web Administrator**
2. Go to **System->General**
3. Click on **Enable syncing of system time over the Internet**
4. You may change the DNS name of the time keeper with your preferred Host. IP addresses are also acceptable if the time keeper is on an internal network.
5. Click **Save** to start the service

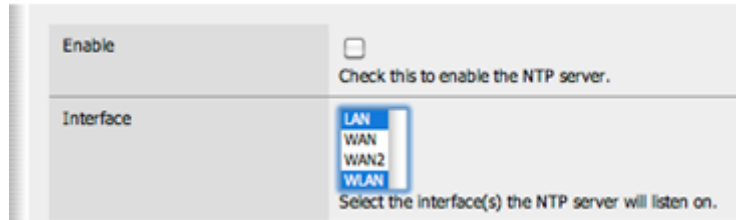
NTP time client	<input type="checkbox"/> <b>Enable syncing of system time over the Internet</b> If this option is set, webXaccelerator will access the Internet to sync time at a dynamically determined polling interval. The polling interval depends on the skew of the system clock. The more stable the system clock the longer the polling interval. Note that enabling the Services->OpenNTPD server forces this option to be set. <input type="text" value="0.pfsense.pool.ntp.org"/> Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here! Note that valid time server must be entered for setting the time at boot up even if time syncing is disabled.
-----------------	--

### 7.2 NTP Server

The wXa router can serve as a time server.

To enable the NTP Time server:

1. Login to the **Web Administrator**
2. Go to **Services->OpenNTPD**
3. Click on **Enable** to turn the NTP service on
4. Select the **Interface(s)**:  
Use CNTL-Click on a PC or OPTION-Click on a Mac to select the desired network interfaces
5. Click **Save** to start the service



**Note:** Enabling the NPTD service will also enable wXa NTP client causing additional network traffic over the WAN.

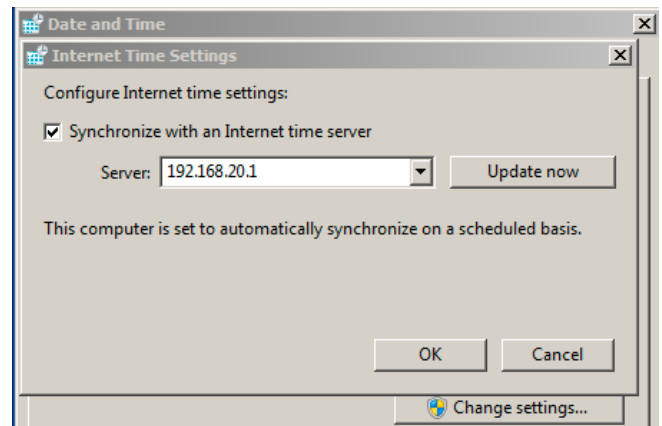
## 7.3 Configuring NTP Time Client on PCs

Both Mac and Windows have native support for the NTP time protocol. This means that the wXa can be configured to serve time to your LAN. Doing so saves airtime since the only device synchronizing time over the internet is the wXa router.

### 7.3.1 Enabling NTP Client on a Windows PC

To enable the NTP client on MS Windows PCs:

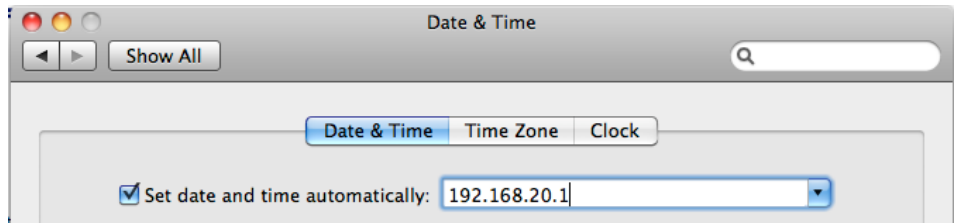
1. Select **Date and Time** from the **Control Panel**
2. Select the **Internet Time** tab
3. Click the **Change Settings** button
4. Check **Synchronize with an Internet Time Server**
5. In the Server field, enter the IP address (or the local DNS name) of the wXa
6. Click **Update Now**
7. Click **OK**



## 7.3.2 Enabling NTP Client on a Mac

To enable the NTP client on a Mac:

1. Select **Date & Time** from **System Preferences**
2. Select the **Date & Time** tab
3. Check **Set date and time automatically**
4. Enter the IP address (or local DNS name) of the wXa



---

## 7.4 Internet Polling Interval

When enabled, wXa's NTP client will periodically poll the internet to synchronize its internal clock. The polling frequency is based on a complex algorithm that takes the clock jitter and wander into account. Stable clocks require less access to the internet while unstable clocks will generate more traffic. The algorithm is designed to reduce network load. Initially on startup the wXa will access the internet frequently until the jitter and wander parameters are determined. Then it will fall back and only access the internet periodically.

---

**Warning:** Caution should be used when enabling the NTP client over a FleetBroadband or BGAN unit. Inmarsat's billing increment is 50Kbytes up/down. This means that there are 10 billing increments per Mbyte. Since billing is done by the Megabyte a time synchronization cycle will cost 1/10th of a Mbyte or about \$1 over FleetBroadband if no other traffic is happening when NTP accesses the internet time server. This is not an issue over Iridium OpenPort or VSAT where the billing increments are small or nonexistent.

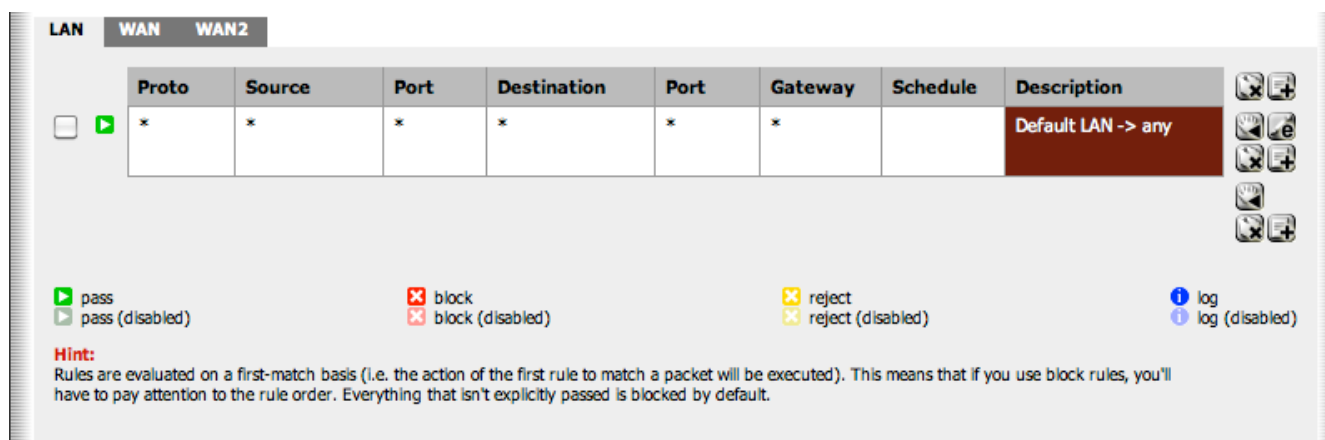
---

## 8 Firewall Rules - Block Unwanted Traffic to/from the Internet

The wXa router has a powerful firewall feature allowing the creation of Firewall rules to permit only certain kinds of traffic to/from the Internet. Firewall rules are executed in a first come first serve fashion. When creating firewall rules you should keep in mind that the very first rule on the list gets executed first and all of the rules are executed in order until a rule is found to match. Once a match is found the data is allowed to pass or it is blocked, based on the rule action.

**Warning:** By default, wXa is distributed with **Open** firewall rules on all interfaces. This means that all traffic originating from the LAN or WLAN ports is allowed to flow unhindered onto the internet and vice-versa. *This is not a very secure setup and should be modified before placing the router into production.*



The following default rule on the LAN port, for example, specifies that data matching any network protocol, originating from any source IP address and port number, destined to any IP address and port number, through any gateway, is allowed to pass.



For obvious reasons, this might be a poor choice for users wanting to protect themselves from downloading, for example, a windows update when paying \$14 per Mbyte over a FleetBroadband System.

## 8.1 Configuring Firewall Rules

To configure Firewall Rules:

1. Login to the **Web Administrator**
2. Select **Firewall->Rules**
3. Select the interface to configure
4. Click on the  next to a rule to remove it
5. Click on the  to add a new rule

The order of the rules is important:






Click the top  to insert a rule **before** the current rule;

Click the bottom  to insert **after** the current rule.

## 8.2 Example of Firewall Rule Configuration

For this example, we want to have all WAN access disabled (i.e. traffic originating from the internet should not be let through the router) and that users on the LAN should only have access to web browsing on ports 80 (HTTP) and 443 (HTTPS).

Follow this sequence to implement this set of firewall rules:

1. Login to **Web Administrator**
2. Select **Firewall->Rules**
3. Select the **WAN** tab
4. Click the  next to the existing rule to disable it  
(OR) Click the  to the right of the rule to edit, check **Disable this rule** and click **Save**
5. Select the **WAN2** tab
6. Disable the existing rule by clicking the  next to the rule
7. Click on the **LAN** tab
8. Disable the **Default LAN -> any** rule by clicking the  next to the rule
9. Click on the  to add a new rule
10. Use the following configuration for the new rule (leaving the Gateway as Default unless configuring failover, see [Configuring Failover from Primary to Backup Satellite Link](#))



## Firewall: Rules: Edit








<b>Action</b>	<input type="button" value="Pass"/> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
<b>Disabled</b>	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<input type="button" value="LAN"/> <p>Choose on which interface packets must come in to match this rule.</p>
<b>Protocol</b>	<input type="button" value="TCP"/> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
<b>Source</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match.  Type: <input type="button" value="any"/> Address: <input type="text" value=""/> / <input type="button" value=""/>  <input type="button" value="Advanced"/> - Show source port range
<b>Source OS</b>	OS Type: <input type="button" value="any"/> Note: this only works for TCP rules
<b>Destination</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match.  Type: <input type="button" value="any"/> Address: <input type="text" value=""/> / <input type="button" value=""/>
<b>Destination port range</b>	from: <input type="button" value="HTTP"/> <input type="text" value=""/> to: <input type="button" value="HTTP"/> <input type="text" value=""/>  Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port
<b>Log</b>	<input type="checkbox"/> <b>Log packets that are handled by this rule</b> Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the <a href="#">Diagnostics: System logs: Settings</a> page).
<b>Advanced Options</b>	<input type="button" value="Advanced"/> - Show advanced options
<b>State Type</b>	<input type="button" value="Advanced"/> - Show state
<b>No XMLRPC Sync</b>	<input type="checkbox"/> HINT: This prevents the rule from automatically syncing to other CARP members.
<b>Schedule</b>	<input type="button" value="none"/>  Leave as 'none' to leave the rule enabled all the time.  <b>NOTE: schedule logic can be a bit different. Click <a href="#">here</a> for more information.</b>
<b>Gateway</b>	<input type="button" value="default"/>  <b>Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.</b>
<b>Description</b>	<input type="text" value="Allow all HTTP access"/> You may enter a description here for your reference (not parsed).

11. Click **Save**
12. Repeat steps 9-11 selecting HTTPS for the destination ports
13. Click **Apply changes** to enable the new rules

LAN

WAN

WAN2

		Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	TCP	*	*	*	443 (HTTPS)	*		Allow all HTTPS access	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	TCP/UDP	*	*	*	80 (HTTP)	*		Allow all HTTP access	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	*	*	*	*	*	*		Default LAN -> any	

Note that although the **Default LAN -> any** rule still appears in the list, it is disabled (grayed out) and will be ignored.

**Note:** When selecting **default** for the **Gateway**, the router will use the default routing table to route traffic. This is fine when only one WAN connection is available. *However, selecting **default** is not a good idea when using two satellite systems in a failover configuration.* The reason for this is that the default routing table is not updated during the failover process and traffic matching the rule cannot be routed since the primary WAN is offline. To use failover, policy-based routing must be used. Under these conditions, select either the desired WAN interface or the **Failover** pool. See [Configuring Failover from Primary to Backup Satellite Link](#) for information on configuring automatic failover.

**Warning:** Every interface has its own firewall rule set. This means that on Wi-Fi routers the **WLAN** tab must be selected to create rules for the wireless LAN. *Rules created under **LAN** do **not** apply to the **WLAN** interface.*

## 8.3 System vs. User Generated Firewall Rules

System generated firewall rules take precedence over user created rules. This means, for example, that the transparent proxy rule that automatically routes HTTP traffic on port 80 when the proxy server is enabled will take precedence over any HTTP allow/deny firewall rule created by the user. This has implications for administrators wishing to create firewall rules to prevent some users from accessing the Internet through port 80 and the proxy server. When transparent proxy is enabled there is no way to prevent a specific IP client from using the Internet through port 80 using firewall rules. *To block these users, transparent proxy must be disabled.*

Another example is the anti-lockout rule under **System->Advanced** in the **Web Administrator**. This rule is designed to prevent any PC on the LAN network from being locked out of the **Web Administrator**. *Administrators wishing to disable access to the **Web Administrator** using firewall rules must disable anti-lockout.*

## 9 VPN access through WAN

The wXa router implements three different VPN protocols (OpenVPN, IPsec, and PPTP). Since most installations will use PPTP, this chapter covers how to enable this protocol. PPTP is easy to setup and has the added advantage that both Microsoft Windows and Mac OS X come with VPN clients that use this protocol.

**Note:** PPTP will only work when connecting through the **WAN** port. If VPN connections through WAN2 are required then IPsec or OpenVPN must be used.

### 9.1 Enabling PPTP

To enable the PPTP service:

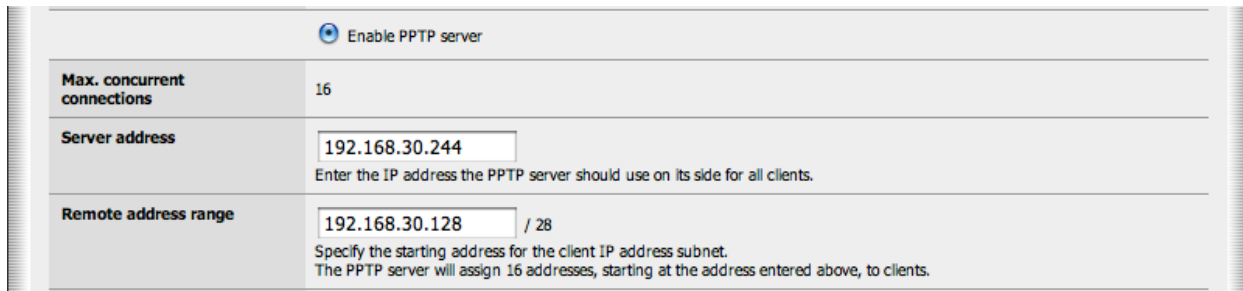
1. Login to the **Web Administrator**
2. Select the **VPN** menu
3. Select **PPTP**
4. Select the **Users** tab
5. Enter a **Username** and **Password** for each user that will login through this service.  
The **IP address** field should be left blank.
6. Click **Save**

#### VPN: PPTP: User: Edit

Username	<input type="text" value="testaccount"/>
Password	<div><input type="password" value="••••"/></div> <div><input type="password" value="••••"/> (confirmation)</div>
IP address	<div><input type="text"/></div> <div>If you want the user to be assigned a specific IP address, enter it here.</div>
<input type="button" value="Save"/>	

7. Select the **Configuration** tab
8. Click **Enable PPTP server**
9. Enter the **Server address**

10. Enter an IP address range in **Remote address range**



<input checked="" type="checkbox"/> Enable PPTP server	
Max. concurrent connections	16
Server address	<input type="text" value="192.168.30.244"/> <small>Enter the IP address the PPTP server should use on its side for all clients.</small>
Remote address range	<input type="text" value="192.168.30.128 / 28"/> <small>Specify the starting address for the client IP address subnet. The PPTP server will assign 16 addresses, starting at the address entered above, to clients.</small>

11. Leave the default options in all other fields
12. Click **Save**

Enabling the PPTP server automatically adds firewall rules permitting TCP port 1723 and GRE traffic into the WAN IP so there is no need to edit the WAN firewall rules to add these. Additionally, traffic from connected PPTP users is controlled via rules under the **PPTP VPN** tab in **Firewall>Rules**. (This tab will be selectable after PPTP is enabled.) Rules should be added to allow VPN users access to internal network resources on the LAN. Until these rules are added, all traffic initiated from connected PPTP clients will be blocked. See [Configuring Firewall Rules](#) for instructions.

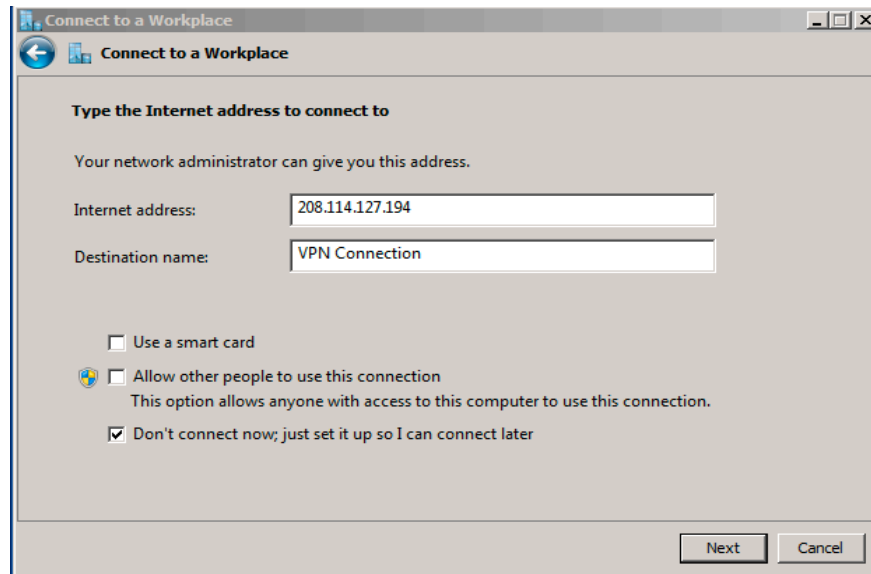
**Note:** Regarding Security - If your PPTP clients originate from known IP addresses then it may be better to disable the automatic generation of PPTP firewall access rules for the WAN port. This is done under the **System->Advanced** menu using **Disable Auto-added VPN rules**. Once the auto-added rules are disabled, new specific rules must be manually added to the WAN firewall list.

---

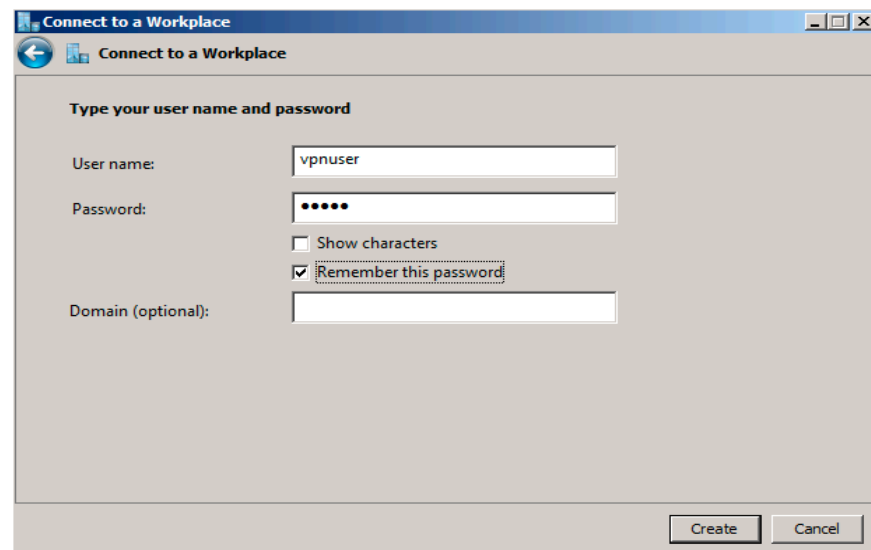
## 9.2 Windows 7 PPTP Client Setup

To setup a Windows 7 PPTP VPN connection, follow these steps:

1. Open the **Control Panel**
2. Select the **Network and Sharing Center**
3. Select **Setup a new connection or network**
4. Select **Connect to a workplace**
5. Click **Use my Internet connection (VPN)**
6. Enter the **Internet address** for the VPN connection
7. Enter a description for the connection in **Destination name**



8. Click **Next**
9. Enter the VPN **User name** and **Password** created during the server PPTP VPN setup
10. Click **Create**



11. Connect to the VPN by selecting **Connect to a network** from the Network Sharing center under the windows control panel

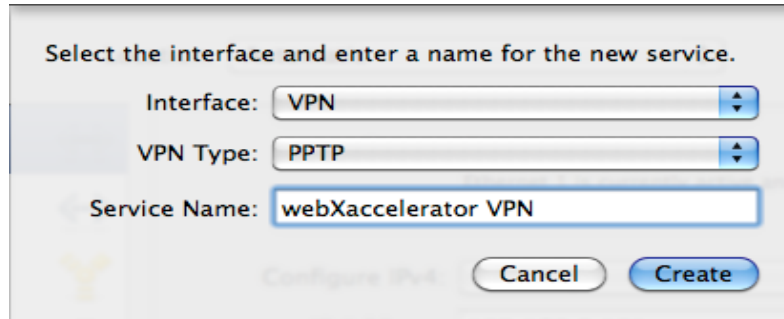
---

## 9.3 Mac OS X Client Setup

To configuring a Mac to connect to a VPN/PPTP server, follow these steps:

1. Open **System Preferences**
2. Select **Network**

3. Click on the "+" (bottom left of window) to add a new connection.
4. Select VPN for the **Interface**
5. Select PPTP for the **VPN Type**
6. Add a description for the connection in the **Service Name:** field



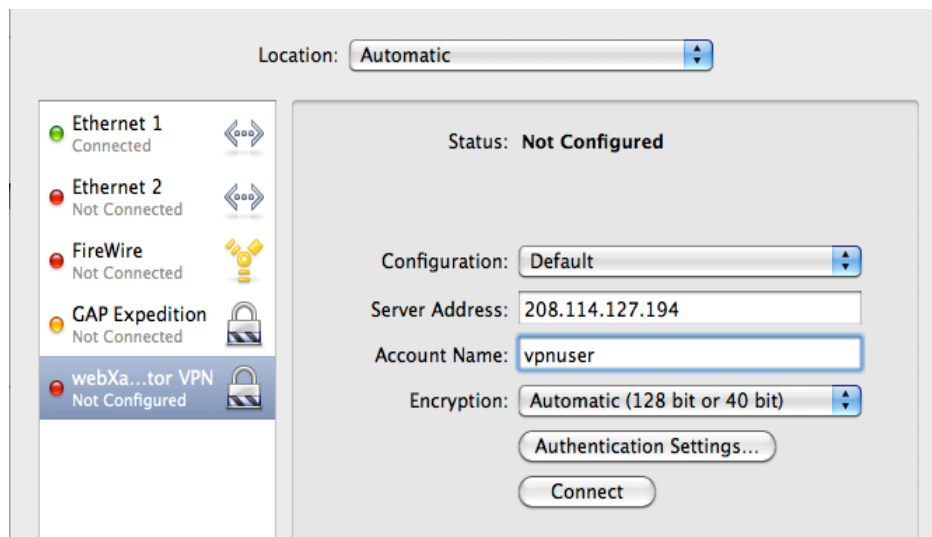
Select the interface and enter a name for the new service.

Interface:

VPN Type:

Service Name:

7. Click **Create**
8. Click on the new interface and enter the server IP address in the **Server Address** field
9. Enter the **Account Name**. The account name is the username created on the router during the PPTP VPN server setup.



Location:

Status: **Not Configured**

Configuration:

Server Address:

Account Name:

Encryption:

10. Click on **Authentication Settings** and enter the VPN user's assigned password in the **Password** field. The password is the password that was entered for the user when creating the user account during the PPTP VPN server setup.
11. Click **Connect** to connect to the VPN

## 10 Captive Portal

The captive portal feature in the wXa router allows administrators to restrict access to the internet on a per user basis. When enabled, the captive portal directs users to a login page when they try to access the internet using a web browser. Users are required to enter a valid pincode before access is allowed. Once the pincode is entered, the user can use the internet for browsing and other applications (such as file transfer, instant messaging, gaming, etc.) within the constraints set by firewall rules and the pincode itself.



The screenshot shows the webX accelerator captive portal interface. At the top, there is a header with the text "Global Marine Networks" and "webX accelerator" in a stylized font. Below the header, a grey bar contains the text "Voucher Login - enable browser popup windows for logout and status". The main content area has a white background. It features a label "Enter PIN number:" followed by a text input field. To the right of the input field is a "Continue" button. Below the input field, there is a link that says "Click to [BOOKMARK the STATUS PAGE] (allows you to review account and session information when you are logged in.)". To the right of this link is a yellow box with the text "PIN: 3786imx3", "BUY PINCODE", and "NOW" in a large, bold font. At the bottom of the page, a dark brown bar contains the text "webXaccelerator is © 2010 by Global Marine Networks, LLC. All Rights Reserved."

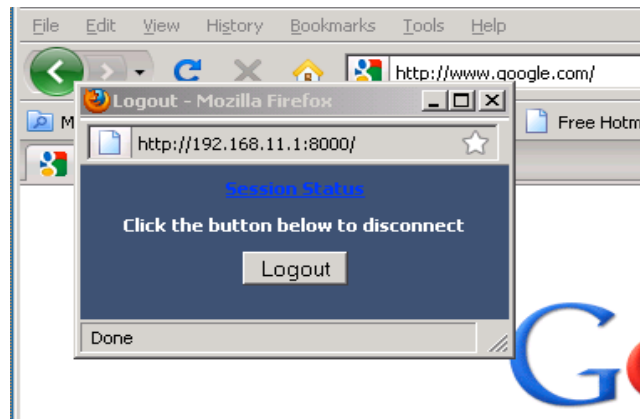
Pincodes can restrict access to the internet in several key ways:

1. Time - Users are allowed a total number of minutes before their connection is terminated.
2. Data volume - Users are allowed a total number of bytes transferred before their connection is terminated.
3. Time of day - Users can be restricted to internet access during a certain period of the day.
4. Bandwidth - Users can be restricted to a fixed bandwidth channel such as 64kbps. Data cannot be transferred up or down faster than the maximum specified bandwidth allocated

to the pincode.

When a user tries to access the internet, he is presented with a login screen requesting a pincode. Entering an invalid pincode will redirect the user to an error page. The user then has the option to return to the login page or, if the Buy Now feature is enabled, to click on a link which allows the purchase of a pincode on the spot. After acquiring a pincode, the user can then return to the login screen to access the internet.

Upon entering a valid pincode, the user is redirected to the original page that was requested and (if popups are not blocked by the browser) a popup window appears.

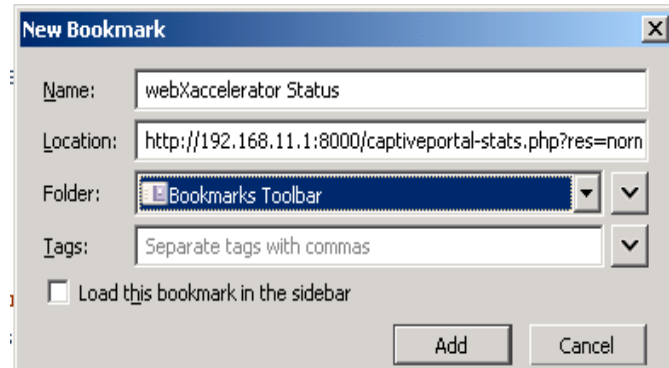


The popup window allows the user to either logout or click on a status link that provides real-time status for the internet connection and pincode usage. To end a session, the user clicks on the **Logout** button.

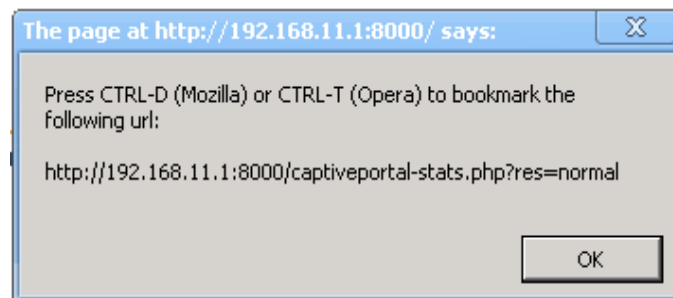




The status window is available for mobile devices and browsers that disallow popup windows via the use of a bookmark link on the login page. Users who do not have access to popup windows should pay close attention to the bookmark link since this link provides valuable session information.



To use the bookmark, users should click on the bookmark link before entering their pincode. With Firefox or Internet Explorer browsers, a dialog will pop up to confirm the action and the location to store the bookmark. For other browsers, a window will pop up displaying the URL for the bookmark. Users will need to copy the URL from the popup window and then manually store the bookmark.



Users should take care to logout when done with their session. To logout, click the **Logout** button in the popup window that appeared after login or on the status page. As stated previously, the status page can be viewed by using the bookmark or by clicking on the status link in the popup window.

Sessions are set to timeout after a fixed amount of time. This is done to protect users from wasteful usage of their pincodes. This is especially true for users who walk away from their sessions without logging out.

Time based pincodes will end a session after 5 minutes of idle time and every 30 minutes. This means that if no network traffic happens within a period of 5 minutes the session will be timed

out and the user forced to log back in. Users are forced to login regardless of their usage every 30 minutes.

For data based pincodes the idle timeout is set for 10 minutes and the hard timeout is 1 hour.

Every session is logged for time and usage. Administrators can access call logs from the Call Details Records (see [The CDR and Pincode Call Logs](#)). Such records may be used for accounting purposes or to settle disputes with users.

## Call logs for "123456-64" from "2010-07-27 00:00:00" to "2014-12-31 23:59:59"

user	date_time	session_time	in_bytes	out_bytes	total_bytes
123456-64	2010-07-29 23:49:40	173	11195	120348	131543
123456-64	2010-07-30 00:03:08	66	5441	79419	84860
123456-64	Totals	239	16636	199767	216403

## 10.1 Limitations

The captive portal implementation on wXa can only be run on one interface. This means that on Wi-Fi units, the captive portal can be configured to use the WLAN or LAN interface but **not** both.

## 10.2 Setting up the Captive Portal

When the captive portal is enabled, users are redirected to a login page when trying to access the internet via a web browser. After following the setup steps below, test the captive portal by entering a website URL in a browser. You can obtain pincodes from your wXa provider. For more information about pincode restrictions and authentication methods, refer to [Pincode Restrictions](#) and [Pincode Authentication](#).

To set up the Captive Portal, use the following steps:

1. Login to the **Web Administrator**
2. Enable the traffic shaper if desired:
  - Go to **Firewall->Traffic Shaper**. Click **Enable traffic shaper**, then click **Save**

**Note:** The traffic shaper is only required if per pincode bandwidth restrictions are to be implemented. As stated previously, pincodes have the ability to limit users to

maximum bandwidth usage. Enforcement of bandwidth limitations is done with the traffic shaper.

---

3. Go to **Services->Captive portal**
  4. Click **Enable Captive portal**
  5. Select the **Interface**: Select **LAN** to enable the captive portal for wired users. Select **WLAN** to enable the captive portal for Wi-Fi users.
- 

**Note:** Note that the captive portal can only be enabled on one interface. WLAN is selected by default for Wi-Fi routers and LAN for the wired version.

---

6. Enter **maximum concurrent connections**. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time. Default is 4 connections per client IP address, with a total maximum of 16 connections.
  7. Enter **Idle timeout**. The default is 5 minutes. Note that this field is overridden by the pincodes. The field is only used for users who have been whitelisted to bypass the captive portal or pincodes with no limits defined.
  8. Enter **Hard timeout**. The default is 60 minutes. Note that the field is overridden by the pincodes. The field is only used for users who have been whitelisted or have pincodes with no defined limit.
  9. Check **Enable logout popup window**.
- 

**Warning:** Browsers on the network should be configured to allow popups initiated from wXa. After login, a popup window is displayed on the client's computer which allows him to logout and view important real time status information. See above for details.

---

10. Check **Enable per-user bandwidth restriction**. This is required if pincodes are to be used for bandwidth limitations. You will **need** to enable the traffic shaper for this to be effective (see number 2).
  11. Select **Radius authentication** and enter the following values:
    - The **Primary Radius Server IP address** is **204.109.60.96**
    - **Port** field should be left blank
    - **Shared secret** is **xgate**
  12. **Secondary Radius Server IP Address** is **208.86.227.138**
  13. Check **Send RADIUS accounting packets**
  14. Check **Reauthenticate connected users every minute**
- 

**Warning:** If steps 13 and 14 are omitted, then the pincodes will not work.

---

15. Leave all other values set to their defaults
16. Click **Save**


## 10.3 Bypassing the Captive Portal

For some installations it might be desirable to bypass the captive portal for some special users or for all users accessing a specific website. For example, company policy may require users to enter a pincode for personal browsing but none to access the corporate website. Another example might be for the owner of the vessel (i.e. the guy who pays the airtime bills) to have full access to the internet while restricting access to the crew with pincodes.


The captive portal can be bypassed using two different methods: Either by the MAC address or the IP address of the computer. The term *whitelist* is used to refer to the list of addresses that are bypassed using one of these two methods.

**Note:** By default, wXa comes configured with whitelist rules for the GMN mail and weather servers. This allows XGate and WeatherNet users to access the services without having to enter pincodes into the captive portal login screen. These rules should be removed if the policy is not compatible with your operation.

To whitelist by MAC address:

1. login to the **Web Administrator**
2. Select **Services->Captive portal**
3. Select the **Pass-through MAC** tab
4. Click on the 
5. Enter the **<MAC address>** and **<computer description>** in the appropriate fields
6. Click **Save**

To whitelist by IP address:

1. Login to the **Web Administrator**
2. Select **Services->Captive portal**
3. Select the **Allowed IP addresses** tab
4. Click on the 
5. Select the direction (from/to)

**Note:** IP addresses can be whitelisted as **any-> IP address** or **IP address -> any**. In **any -> IP address**, any computer on the local LAN (or WLAN) is allowed unrestricted

access to the specified external IP address. In **IP address** -> **any**, the specified internal IP address has unrestricted access to the internet.

6. Enter the **<IP address>** and **<computer description>** in the appropriate fields
7. Click **Save**

**Services: Captive portal**

Captive portal Pass-through MAC Allowed IP addresses Users File Manager

IP address	Description
any ► 204.109.60.97	XGate Server TX
any ► 208.86.225.107	WxNet Server NC
any ► 208.86.227.175	XGate Server NC
any ► 216.157.143.52	XGate Server FL

**Note:**  
Adding allowed IP addresses will allow IP access to/from these addresses through the captive portal without being taken to the portal page. This can be used for a web server serving images for the portal page or a DNS server on another network, for example. By specifying *from* addresses, it may be used to always allow pass-through access from a client behind the captive portal.

any ► x.x.x.x All connections **to** the IP address are allowed  
x.x.x.x ► any All connections **from** the IP address are allowed

## 10.4 Setting up for the Buy Now links

It is possible for wXa reseller's to configure the captive portal login page with a customizable **Buy Now** link which will redirect retail users to a shopping cart website for the purchase of a pincode. By default, this feature is disabled. This section describes how to enable the feature and customize the look and the links to the shopping website.

The following resources can be found on the DVD included with the wXa under the captive portal folder. These files include:

- *captiveportal-vendor.inc* - a vendor specific configuration file (discussed below)
- *captiveportal-mbuynow.gif* and *captiveportal-buynow.gif* - sample buy now icons to be displayed on the login page. The first icon is formatted for small screens on mobile devices. The second icon is for normal computer screens. Vendors are free to use this graphic or to design their own, keeping the same dimensions.
- *captiveportal-header.gif* - banner which appears on the login screen. Vendors are free to use this banner or design their own as long as the image dimensions are maintained.
- *captiveportal-header\_mobile.gif* - banner for smaller login page used for mobile

devices.

To add a personalized "Buy Now" icon and link to the shopping cart website, do the following:

1. (Optional) Create Buy Now icons that have the same dimensions as *captiveportal-buynow.gif* and *captiveportal-mbuynow.gif* icons
2. (Optional) Create replacement images for *captiveportal-header.gif* and *captiveportal-header\_mobile.gif*
3. Edit *captiveportal-vendor.inc* and modify it so that **\$vendor\_buy\_now\_url** contains the link to the shopping cart and the **icon\_fields** contain the name of the appropriate **Buy Now** images.

Here is a sample:

```
<?php
$vendor_buynow_url="http://www.globalmarinenet.com/catalog"
$vendor_buynow_icon="captiveportal-buynow.gif";
$vendor_mbuynow_icon="captiveportal-mbuynow.gif";
?>
```

4. Login to the **Web Administrator**
5. Go to **Services->Captive portal**
6. Select the **File Manager** tab
7. Upload the files created in steps 1-3 above

Once completed the screen should look like this:

Captive portal   Pass-through MAC   Allowed IP addresses   Users   File Manager		
Name	Size	
captiveportal-buynow.gif	2 KB	
captiveportal-header.gif	20 KB	
captiveportal-header_mobile.gif	12 KB	
captiveportal-mbuynow.gif	2 KB	
captiveportal-vendor.inc	82 bytes	
<b>TOTAL</b>	<b>36 KB</b>	

8. Select the **Allowed IP addresses** tab
9. Add an **Any to** rule for the IP address of the server hosting the shopping cart. This will allow users access to the shopping cart without having to enter a valid pincode in the login and error pages. See **Error! Reference source not found.** [Bypassing the Captive Portal](#) for detail on creating rules to bypass the captive portal.

The customized Buy Now icons and links should now appear on the captive portal login and error pages.

## 10.5 Pincode Restrictions

There are several restrictions to pincodes that need to be noted before ordering them from your wXa supplier. These restrictions are:

1. Time-based pincodes cannot be activated with more than 24 hours. 24 hours is the maximum amount of time that can be allocated to any pincode.
2. Data-based pincodes can limit 1Mb up to 100Mb of data transfer units. 100Mb is the maximum amount of data that can be allocated to any given pincode.
3. Pincodes must be activated within 24 months of purchase. Pincodes that are not activated within this period expire. There is no way to carry over the time/data allocations to a new pincode.
4. Pincodes become active on first use and are good for 1 year. The content of the pincode must be used within one year of first use. As long as the first use is within the initial 24 month purchase (see #3 above) the user will have one full year to use the pincode.
5. Pincodes can be locked to a specific wXa. If locked, once activated, pincodes can only be used on the captive portal hosted by the specific wXa. If unlocked, pincodes can be used on any wXa. Unlocked pincodes might be used, for example, by a shipping company with many vessels allowing the crew to use their pincodes on any of the vessels.

## 10.6 Pincode Authentication

When pincodes are requested, administrators can specify local or remote authentication for the pincodes. There are advantages and disadvantages to each of these authentication methods. Thus it is important to understand the difference between these methods to know which will work best for your system.

The RedPort wXa routers come configured with an installed local Radius server. One exception to this is the wXa-202 that does not have a local Radius server.

### 10.6.1 Remote Authentication

**Remote authentication** means that once every minute, authentication information is sent to a central server for every user who is logged into the system.

#### **Advantages:**

1. The information is stored in a database at a central location making it possible for the pincodes to be used on a number of vessels.
2. Administrators have easy shore side access to the call records since the database is maintained on the shore side of the link.

#### **Disadvantages:**

1. Additional traffic overhead is generated for the authentication to the remote server.
2. Users can be logged out if the Radius server fails to authenticate due to slow satellite links with long latencies.

## 10.6.2 Local Authentication

**Local authentication** means that authentication packets are verified locally on the local Radius server.

### Advantages:

1. No additional traffic overhead is generated for the authentication, which means no additional airtime overhead is consumed.
2. For slow satellite links with long latencies, users are not logged out when the Radius server authentication fails.
3. CDRs are kept locally for easy access by the administrator on the vessel.

### Disadvantages:

1. CDRs are kept locally on the vessel and are not easily available to shore personnel. Shore side administrators have to login remotely to view the CDRs.
2. Pincodes can only be used on the particular vessel for which they are generated. Crew/Pax cannot use the pincodes on a different ship.

---

## 10.7 The CDR and Pincode Call Logs

The Captive Portal Menu provides access to the Call Detail Records (CDR) from the CDR tab.

When you select the CDR tab, you can enter a pincode value and view the call logs for this pincode.

To access the CDR and the Pincode call logs:

1. Login to the **Web Administrator**
2. Select **Services->Captive portal**
3. Select the **CDR** tab
4. Enter the pincode in the **Pincode** field
5. Click **Submit**



## Services:Captive portal

Captive portal
Pass-through MAC
Allowed IP addresses
Users
File Manager
Pincodes
CDRs

### Pincode Call Records

Enter pincode to query

Pincode

Start Date Year: 2010 Mon: 1 Day: 1

End Date Year: 2030 Mon: 12 Day: 31

Submit Reset

Records for the pincode will be displayed:

Pincode details											
pincode	attr_group	active	start_time	end_time	data_limit	time_limit	nas_lock	data_to_date	time_to_date	agent	timestamp
43-6038325-3411	data128kbps	0	0	0	104857600	0	1	105973338	33003		2012-02-16 11:52:40


Call logs from "2010-1-1 00:00:00" to "2030-12-31 23:59:59"

user	date_time	session_time	in_bytes	out_bytes	total_bytes
43-6038325-3411	2012-02-11 23:59:23	862	565130	4957271	5522401
43-6038325-3411	2012-02-12 12:50:37	3243	1837539	10248825	12086364
43-6038325-3411	2012-02-12 16:53:30	3639	1741553	8827107	10568660
43-6038325-3411	2012-02-12 23:59:11	1492	1054588	9053253	10107841
43-6038325-3411	2012-02-13 11:07:56	34	15049	170084	185133
43-6038325-3411	2012-02-13 11:36:43	2336	1363723	9384544	10748267
43-6038325-3411	2012-02-13 20:38:19	1555	863090	5100606	5963696
43-6038325-3411	2012-02-14 11:53:14	1178	798494	8226918	9025412
43-6038325-3411	2012-02-15 11:58:41	3649	2145905	13479723	15625628
43-6038325-3411	2012-02-15 13:05:54	3628	273437	2683840	2957277
43-6038325-3411	2012-02-15 14:20:38	1046	413790	1527526	1941316
43-6038325-3411	2012-02-15 18:16:13	2863	1030230	5556353	6586583
43-6038325-3411	2012-02-15 23:36:54	3647	2934238	9887650	12821888
43-6038325-3411	2012-02-16 00:42:49	3652	132536	223600	356136
43-6038325-3411	2012-02-16 11:49:41	179	224186	1252550	1476736
43-6038325-3411	Totals	33003	15393488	90579850	105973338

## 11 Assigning Static IP addresses to PCs on the LAN/WLAN

At times it is necessary to assign static IP addresses to client PCs on the LAN or WLAN networks. This might be needed, for example, when whitelisting a PC to bypass the captive portal. There are 2 different ways to assign a static IP address to a client computer referred to as Method 1 and Method 2 below.

### Method 1:



1. Login to **Web Administrator**
2. Go to **Services > DHCP server**
3. At the bottom of the form is a table that maps MAC addresses to IP addresses. Click on the  button at the bottom of the form to map a MAC address to an IP address adding the appropriate values.
4. Click **Save**

### Method 2:


1. Login to **Web Administrator**
2. Go to **Status > DHCP Leases** to display a list of hosts that have been granted DHCP leases. Here is an example:

**Diagnostics: DHCP leases**

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.20.245	00:26:bb:11:4c:c1		2010/07/31 17:02:08	2010/07/31 19:02:08	online	active

Show all configured leases

3. Click the  button next to the computer that is to be assigned a static IP address. This brings up the DHCP static mapping dialog used in the first method.

**Note:** When invoked from the DHCP leases status function, the form is automatically populated with the MAC address of the PC. Leaving the IP address field blank

causes the system to reserve the IP addresses currently assigned to the PC for use exclusively by this client.

**Services: DHCP: Edit static mapping**

MAC address	<input type="text" value="00:26:bb:11:4c:c1"/> <a href="#">Copy my MAC address</a> Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
IP address	<input type="text"/> If no IP address is given, one will be dynamically allocated from the pool.
Hostname	<input type="text"/> Name of the host, without domain part.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

4. Enter a **Hostname** to automatically add the IP address and Hostname mapping to the DNS forwarder's table. This allows users on the local LAN or WLAN to access the host via its name rather than its IP address.
5. Click **Save** to configure the static IP entry

## 12 Caching Proxy Server

The RedPort wXa router contains a caching web proxy server that, by default, is enabled and configured to cache any/all HTTP and FTP requests from the local LAN (WLAN for Wi-Fi units). As users access pages from the internet, the proxy server caches these pages locally. When a user makes a request for a page on the internet, the request is first passed to the wXa's proxy server. The proxy server looks in its cache to see if a local copy of the page exists. If it does, then it checks the timestamp of the local copy against the original page on the internet. If the page has not changed, it then serves the client the local copy. If the original page is newer, then it downloads it, stores it in the cache, and serves the page to the client. Caching of pages locally can dramatically improve satellite link performance; since depending on the cache hit ratio, pages are served to local clients over the LAN (or WLAN) and not fetched over the satellite link.

The proxy cache therefore improves performance (and saves users money) by reducing the amount of data that must be transferred over the WAN links.

wXa's caching proxy server is based on the popular Open Source Squid project. This guide documents common Squid configuration settings. Advanced users requiring information beyond the scope of this manual should refer to the Squid project home page at <http://www.squid-cache.org> for full documentation.

---

### 12.1 Limitations

The caching proxy server is enabled, by default, and configured for the LAN interface on wired routers and the WLAN interface on the Wi-Fi version. Like the captive portal, the proxy server can be configured for one, and only one, network interface port.

---

### 12.2 Customizing the Proxy Server

The proxy server is enabled by default. The default settings should be good for most installations so little customization is required. However, under special circumstances, it might be necessary to modify the proxy settings.

To customize the proxy server:

1. login to the **Web Administrator**
2. Select **Services->Proxy server**

## 12.2.1 General Settings

The **General** tab allows access to common proxy server settings:

**Proxy Interface** is used to select the interface the proxy is to act on. WLAN should be selected for Wi-Fi installations and LAN should be used for wired ones.

General	Compression	Cache Mgmt	Access Control	Traffic Mgmt	Auth Settings	Local Users
<div> <div>Proxy interface</div> <div> <div>LAN</div> <div>WAN</div> <div>WAN2</div> <div>VOIP</div> </div> </div> <div>The interface(s) the proxy server will bind to.</div>						

The proxy is enabled or disabled using **Allow users on interface**. This setting should be checked on the proxy server. Checking this option automatically adds the primary subnet for the interface to the **Allowed Subnets** table under the **Services > Proxy Server > Access Control** tab. Note that the primary interface does not show up in the table although it has been configured. Additional subnets should be added to the **Services > Proxy Server > Access Control > Allow Subnets** table for installations with multiple subnets on one interface.

<div>Allow users on interface</div> <div><input checked="" type="checkbox"/></div>	<p>If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.</p>
--	--

Enabling **Transparent proxy** causes all http requests on the network to be redirected to the proxy server. Unchecking this option effectively disables the proxy server.

<div>Transparent proxy</div> <div><input checked="" type="checkbox"/></div>	<p>If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.</p>
---	---

Logging is required for web access report generation. See [Web Logging](#) for generating and analyzing web access. This option should be left enabled and the path to the log should be left unmodified.

<div>Enabled logging</div> <div><input checked="" type="checkbox"/></div>	<p>This will enable the access log. Don't switch this on if you don't have much disk space left.</p>
<div>Log store directory</div>	<div>/var/squid/log</div> <p>The directory where the log will be stored (note: do not end with a / mark)</p>
<div>Log rotate</div>	<div></div> <p>Defines how many days of logfiles will be kept. Rotation is disabled if left empty.</p>

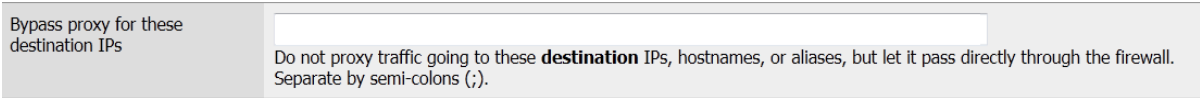
## 12.2.2 Bypassing Proxy for access to Satellite Terminals

Users using Iridium OpenPort or Inmarsat Broadband Terminals (Such as FleetBroadband and BGAN) for their WAN will want to bypass the proxy when accessing the control panels on the terminals. This is especially true if XWeb compression is enabled using the forward proxy which forwards all HTTP traffic to the compression server on the internet. Unless the terminals are bypassed errors will occur since the XWeb server has no way to access them from the Internet side of the link.

By default the proxy server is configured to bypass all addresses in the Private Address Space defined by RFC 1918. This means that if your terminal has an IP address in the range of 192.168.X.X, 172.16.X.X, or 10.X.X.X then nothing needs to be done to bypass access to the terminal. If, however, your terminals use a public address then intervention is required.

There are two additional ways to bypass the proxy server. Method 1 is the simplest.

**Method 1:** Enter the IP address of the terminal in **Bypass proxy for these source add IPs**

Multiple IP addresses can be entered separated by ';'.  


**Method 2:** Create a custom rule for an Access Control List (ACL) and enter it into Custom Options (see [Custom Options](#) for additional detail). An example is below:

```
acl    satellitenet    dst    229.200.21.0/24
optional_additional_ip_addresses/netmaks;
always_direct    allow    satellitenet;
never_direct    allow    all;
```

Where **229.200.21.0** is the **network address of subnet** and **24** is the **subnet mask**. Additional IP address/netmask can be added by separating them with whitespace. *You will need to change these to match your network topology.*

---

**Warning:** When entering multiple ACL lists make sure that the **never\_direct allow all;** statement is the very last one. One of these is required.

---

## 12.2.3 Custom Options

Custom squid options are added to **Services->Proxy server > General** under **Custom Options**. Options are entered one line at a time separated by a semi-colon.

## Custom Options

```
refresh_pattern guru.avg.com/*\.(bin) 4320 100% 43200 reload-into-ims;refresh_pattern windowsupdate.com/*\.(cab|exe) 4320 100% 43200 reload-into-ims;refresh_pattern download.microsoft.com/*\.(cab|exe) 4320 100% 43200 reload-into-ims;refresh_pattern au.download.windowsupdate.com/*\.(cab|exe)
```

You can put your own custom options here, separated by semi-colons (;). They'll be added to the configuration. They need to be squid.conf native options, otherwise squid will NOT work.

By default, options for caching windows updates and AVG antivirus virus signature updates are added to the customs option text edit box. The default options are listed below.

```
refresh_pattern guru.avg.com/*\.(bin) 4320 100% 43200 reload-into-ims;
refresh_pattern windowsupdate.com/*\.(cab|exe) 4320 100% 43200 reload-into-ims;
refresh_pattern download.microsoft.com/*\.(cab|exe) 4320 100% 43200 reload-into-ims;
refresh_pattern au.download.windowsupdate.com/*\.(cab|exe) 4320 100% 43200 reload-into-ims;
range_offset_limit -1;
```

In some cases it might be necessary to bypass the XWeb compression for specific pages (see [XWeb Compression](#) for information on web compression with XWeb). To do this, custom rules must be added.

Say, for example, that access to any website in the domain *gmn-usa.com* should not be compressed. (This means that access to *http://www.gmn-usa.com* is to bypass the compression engine as well as *http://webmail.gmn-usa.com*).

For this example the following rules should be added to **Custom Options**:

```
acl noxweb    dstdomain    .gmn-usa.com .optional_additional_domain.com;
always_direct    allow    noxweb;
never_direct     allow    all;
```

The first line defines an access control list (ACL) called `noxweb` that contains a list of domains. In this case, the list contains one item which is `.gmn-usa.com`. Additional domains can be added by separating them with white space. The list can contain any number of domains. The second line specifies that access to any domain in ACL `noxweb` should bypass the forward XWeb compression agent and go directly to the source. The third line indicates that all other requests should be passed forward to the XWeb compression agent (and should therefore go directly to the internet).

---

**Warning:** When entering multiple acl lists make sure that the **never\_direct allow all** statement is the very last one. One of these is required.

---

When your custom options are complete, click **Save** to restart the proxy service.

## 12.2.4 Caching Options

Caching options control the way cache is managed and can be found under the **Caching** tab at **Services->Proxy server**. The parameters in this form have been customized to meet the internal disk requirements for the wXa hardware. *Under normal circumstances, no changes to this form should be required.* However, there might be two exceptions; Use of **Enable offline mode** and the **Do not cache** list.

<b>Enable offline mode</b>	<input type="checkbox"/>
Enable this option and the proxy server will never try to validate cached objects. The offline mode gives access to more cached information than the proposed feature would allow (stale cached versions, where the origin server should have been contacted).	

Checking **Enable offline mode** turns off cache validation. This means that pages in the cache will be served to clients whether they are current or older than the source on the internet. Enabling this option basically turns wXa into a local web server. Once the cache is loaded, it serves pages out of the cache and never checks the internet for newer pages. This greatly increases the efficiency of the cache, and hence increases satellite bandwidth efficiency, at the cost of serving stale pages. If, for example, users on the local network are restricted, to say a local corporate website which rarely changes its content then setting this option will greatly enhance the satellite link usage.

<b>Do not cache</b>	<div><div></div></div>
Enter each domain or IP address on a new line that should never be cached.	

There may be times when pages should never be cached. It is, however, difficult to imagine when this might be needed. Entering the IP address of the remote server in the **Do not cache** list prevents the proxy server from caching pages from this source. Note that this does not disable compression (if it is enabled). The squid custom options, see [Custom Options](#), must be used for this.



## 12.2.5 Traffic Management

Traffic management controls how bandwidth is to be allocated globally to users using the proxy server. These controls are applied on top of any bandwidth management instituted by the traffic shaper and [Captive Portal](#). The default settings should suffice for most installations.

## 12.2.6 XWeb Compression

Web compression is disabled by default. Enabling web compression is desirable since, on average, the service compresses web pages by a factor of 3-5x, i.e. with compression enabled, access speed over the satellite link is increased by up to a factor of 5x, on average. This results in much faster performance while decreasing costs.

RedPort wXa uses Global Marine Networks XWeb proxy compression service. The service does the following to accelerate web links.

- Compress text pages to gzip streams (reduces size by up to 75%)
- Compress images to 10% jpeg (reduces size by up to 95%)
- Removes advertising
- Removes background images
- Caches filtered pages and images
- Uses keep-alive if possible

## 12.2.7 Requirements

To use compression, the following requirements must be met:

1. RedPort wXa must be registered with your provider who provides you with an XWeb username and password
2. Monthly subscription fee must be up to date
3. The satellite provider must allow access to the xweb server at *xweb.gmn-usa.com* via port 3120

## 12.2.8 Limitations

Only http pages can be compressed. Https, ftp, and other protocols are passed through unmodified. By definition, SSL encrypted pages such as those used in the https protocol are randomized and therefore cannot be compressed. Data streams that cannot be compressed are passed through without modification. However, many websites which use https (such as hotmail and gmail) have links to many http URLs on them that are compressible. So, it is rare to have a web page that does not benefit from XWeb compression.

## 12.2.9 Configuration

XWeb compression is configured into the proxy server using the following steps:

1. Login to the **Web Administrator**
2. Go to **Services > Proxy server**

3. Select the **Compression** tab
4. Select **Enable web compression**
5. Enter your assigned **Username** and **Password**
6. Select the **Compression Type**. Maximum compression yields faster connections while sacrificing picture quality.

If no compression is desired then **Enable web compression** should be unchecked.

Enable web compression	<input checked="" type="checkbox"/> This option enables the proxy server to forward requests to an upstream compression server.
Primary proxy server	<input type="text" value="xweb.gmn-usa.com"/> Select primary proxy server.
Username	<input type="text" value="test"/> Compression proxy requires a username, specify it here.
Password	<input type="password" value="*****"/> Compression proxy requires a password, specify it here.
Compression Type	<input type="text" value="Standard"/> Select compression level. Higher compression sacrifices picture quality for speed.

## 12.3 Transparent vs. Manual Proxy

Transparent proxy, which is enabled by default, takes any traffic through port 80 and redirects it to the proxy server for caching and optional compression. *Transparent proxy is recommended for normal operation since nothing has to be done on the client PCs to enable proxy based caching and compression.*

**Note:** Only HTTP traffic on port 80 is redirected. HTTPS traffic on port 443, for example, is not redirected and passed straight through to the internet.

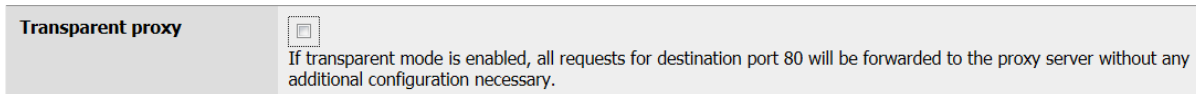
At times it might be advantageous to configure the client PC web browsers to access RedPort wXa's proxy server directly. Some of these advantages include:

- The ability to block *all* (including HTTPS) traffic through the router permitting access to the internet only through the RedPort wXa. This might be required to block point-to-point applications such as Skype and instant messaging.
- Allowing users to dynamically enable/disable compression on a per web page basis.
- Allowing HTTP based firewall rules to take precedence. When transparent proxy is enabled all HTTP traffic on port 80 is routed before firewall rules for this port are evaluated. At times it might be advantageous to create firewall filtering rules for port 80. This requires disabling transparent proxy.

To disable transparent proxy:

1. Login to **Web Administrator**
2. Go to **Services > Proxy server**

3. Select the **General** tab
4. Uncheck **Transparent proxy**



## 12.3.1 Configuring Client Browsers for Manual Proxy

Caching and compression are available only when accessing the internet through the RedPort wXa proxy server. Client web browsers must be manually configured to allow these services. Disabling transparent mode is usually accompanied by creating firewall rules that block access to HTTP (port 80) and HTTPS (port 443) forcing users to reconfigure their browsers to access the Internet.

The user will need to know the **<IP address of wXa>** (default 192.168.10.1 for wired networks and 192.168.20.1 for Wi-Fi) and the **<proxy port number>** (default 3128). RedPort wXa can be configured to automatically serve this information to the client web browser making it easier for the user to enable manual proxy settings. Instructions for configuring wXa for automatically serving the settings are discussed below.

### Configuring Firefox

1. On Windows, go to **Tools->Options**  
On Mac, go to **Firefox->Preferences**
2. Click on the **Advanced** icon
3. Click on the **Network** tab
4. Click on the **Settings...** button
5. Select **Manual proxy configuration**:
6. Enter the **<IP address>** and **<port number>** of the proxy server
7. Select **Auto-detect proxy settings for this network** if using automatic proxy configuration as described in [Automatic Proxy Configuration](#)
8. Optionally enter any hosts or networks that should be accessed directly bypassing the proxy server

### Configuring Internet Explorer

1. Select **Tools->Internet Options**
2. Click on the **Connections** tab
3. Click on **LAN Settings**
4. Enable **Use a proxy server for your LAN**
5. Enter the **<IP address>** and **<port number>** of the proxy server

9. Select **Automatically detect settings** if using automatic proxy configuration as described in [Automatic Proxy Configuration](#)
6. Optionally enter any hosts or networks that should be accessed directly bypassing the proxy server

## Configuring Safari

1. Select **Safari->Preferences**
2. Select **Advanced**
3. Click on Proxies: **Change Settings...**
4. Enable HTTP, HTTPS, and FTP proxies
5. Enter the **<IP address>** and **<port number>** of the proxy server
10. Select **Automatic Proxy Configuration** if using automatic proxy configuration as described in [Automatic Proxy Configuration](#)
11. Optionally enter any hosts or networks that should be accessed directly bypassing the proxy server

### 12.3.2 Automatic Proxy Configuration

To use this feature, client web browsers will need to be configured to enable automatic proxy configuration. See the previous section for instructions on configuring client PCs.

The following steps are required to configure RedPort wXa to automatic proxy configuration settings.

1. Login to the **Web Administrator**
2. Go to **Diagnostics->Edit File**
3. Enter the following in the body of the form

```
function FindProxyForURL(url,host)
{
    return "PROXY 192.168.10.1:3128;
}
```

where 192.168.10.1 is the **<IP address of the wXa>**

---

**Note:** Note WI-FI configurations should use 192.168.20.1 or **<IP address of the wXa WLAN>**

---

4. Save this file 3 times to the following filenames

```
/usr/local/www/wpad.dat
/usr/local/www/wpad.da
/usr/local/www/proxy.pac
```



Saved text to `/usr/local/www/wpad.dat`

Save/Load from path:

Load

Save

```
function FindProxyForURL(url,host)
{
    return "PROXY 192.168.10.1:3128;
}
```

5. Confirm that you can access this file from a web browser by entering **`http://<IP_ADDRESS_OF_WXA>/wpad.dat`** replacing the appropriate IP address. Also test that `wpad.da` and `proxy.pac` are also accessible.
6. Go to **System->General Setup** and note the domain. The default is *gm-n-usa.com*.
  1. Go to **Services->DNS forwarder** and add the following host

```
host: wpad
domain: gm-n-usa.com or whatever the domain was in (5) above
ip: 192.168.10.1 or the IP address of wXa; Use 192.168.20.1 for WI-FI setups
comment: auto proxy settings
```

7. Click **Save**
8. Set your client browser settings for auto proxy as described in the previous section for your browser
9. From a client PC execute the Ping command to make sure that *wpad.gm-n-usa.com* (or *wpad.whatever\_domain.com*) is available
10. Use a web browser to access *http://wpad.gm-n-usa.com/wpad.dat* (or *http://wpad.whatever\_domain.com*) to make sure it is accessible

### 12.3.3 Dynamically Disabling Web Compression

Users are able to dynamically enable/disable web compression once their browsers are configured to use RedPort wXa's proxy server directly.

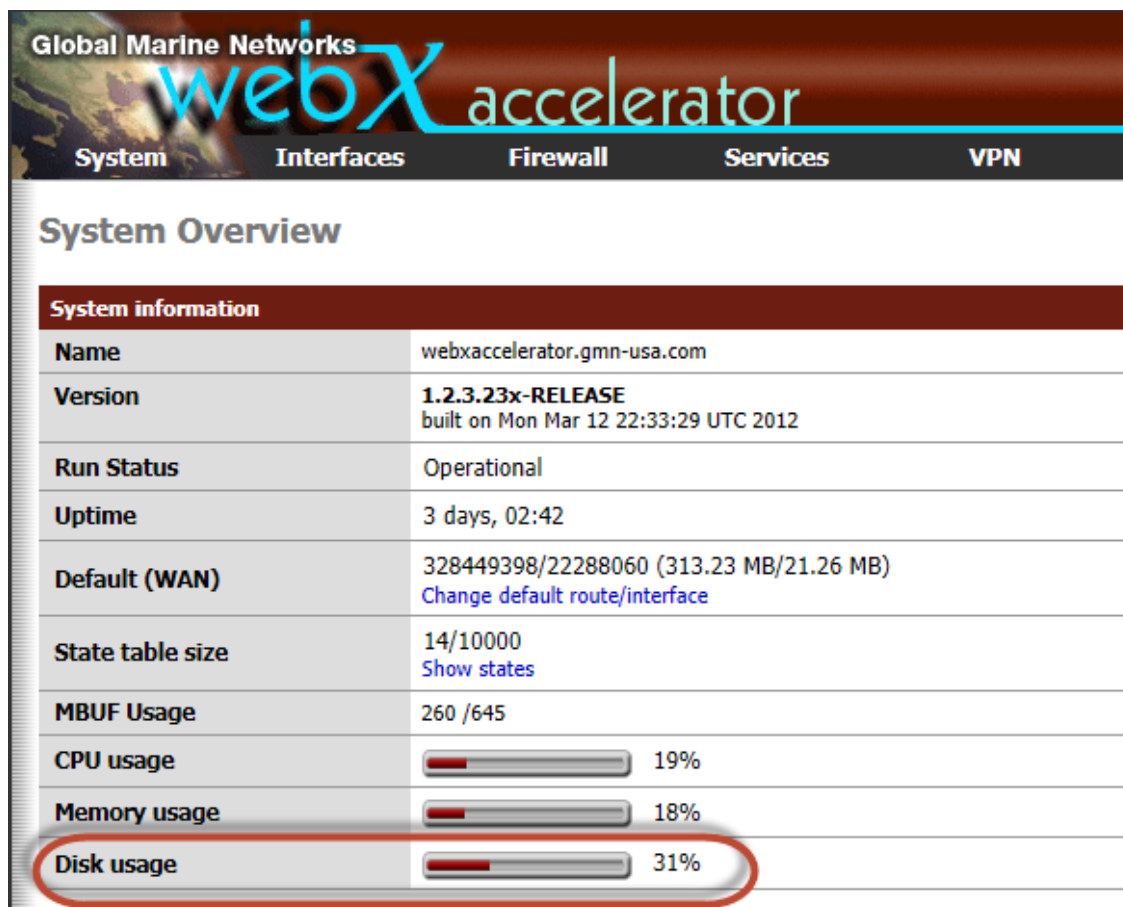
Prepending `noproxy` to any URL will disable compression for that page. So to view the uncompressed version of `http://www.globalmarinenet.com` enter `http://noproxy.globalmarinenet.com`.

**Warning:** This feature does not work with transparent proxy. When using transparent proxy DNS look ups occur on the client PC. Since noproxy.domain.com is never a valid DNS name the lookups fail causing *Server not found* errors.

## 12.4 Rebuild Proxy Cache

### 12.4.1 Disk Usage and Monitoring

The RedPort wXa (except the wXa-202) uses an internal solid state silicon disk drive (SSD) to store its configuration, cached web pages, and reporting log files. The SSD is 8 GB in size with the following allocations: 3 GB for cache management, 3 GB for reporting logs, and 2 GB for system software and configuration.



It is always a good idea to monitor your system's disk usage on the **System Overview** screen. If your disk usage reaches 100%, compression is essentially disabled because the caching capability is needed to do compression.

---

**Warning:** If your system reaches 100% full disk usage state, it is a combination of the 3 GB allocated for cache is full and the 3 GB allocated for the logs is also full. To immediately open up disk space on your system, use the **Rebuild Proxy** menu option detailed in the section below to flush the cache. **You should be aware that flushing the cache will treat the symptom but will not prevent the problem from reoccurring. The problem being that the log rotation does not occur frequently enough.** So in addition, you will need to re-configure your logging options as described in [Web Logging](#).

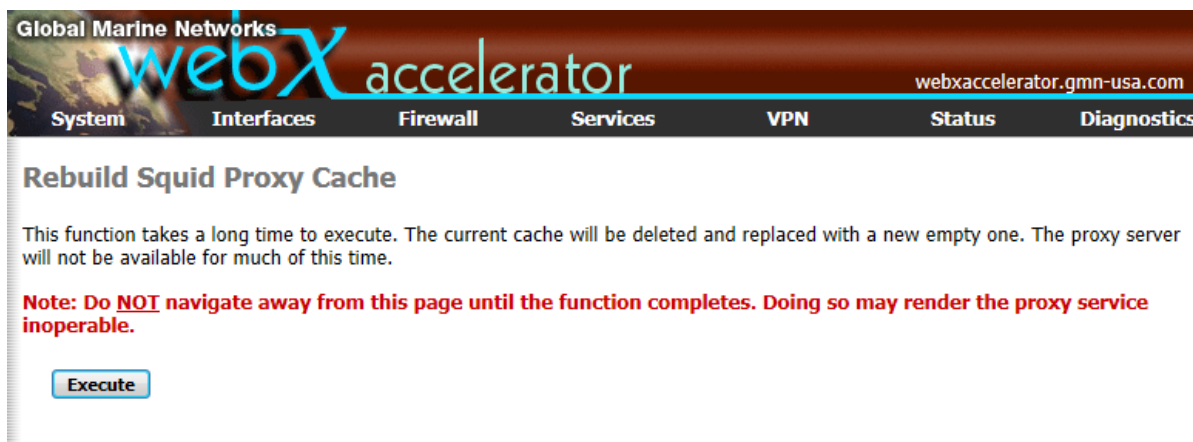
---

## 12.4.2 Flushing the Cache

If your disk usage on your system reaches 100%, you can immediately free up disk space on your system by rebuilding the Proxy cache. However, you will also need to re-configure your logging options as noted in the Warning above. See [Disk-Full issues](#) for additional information.

To rebuild your Proxy cache:

1. Login to Web **Administrator**
2. Go to **Diagnostics**
3. Select **Rebuild Proxy**
4. Click **Execute** on the **Rebuild Squid Proxy Cache** page



The screenshot shows the webX accelerator interface. At the top, there's a header with 'Global Marine Networks' and 'webX accelerator' logo, and the URL 'webxaccelerator.gmn-usa.com'. Below the header is a navigation bar with tabs: System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The 'Diagnostics' tab is selected. The main content area is titled 'Rebuild Squid Proxy Cache'. It contains a warning message: 'This function takes a long time to execute. The current cache will be deleted and replaced with a new empty one. The proxy server will not be available for much of this time.' Below this is a red note: 'Note: Do NOT navigate away from this page until the function completes. Doing so may render the proxy service inoperable.' At the bottom of the content area is a blue 'Execute' button.

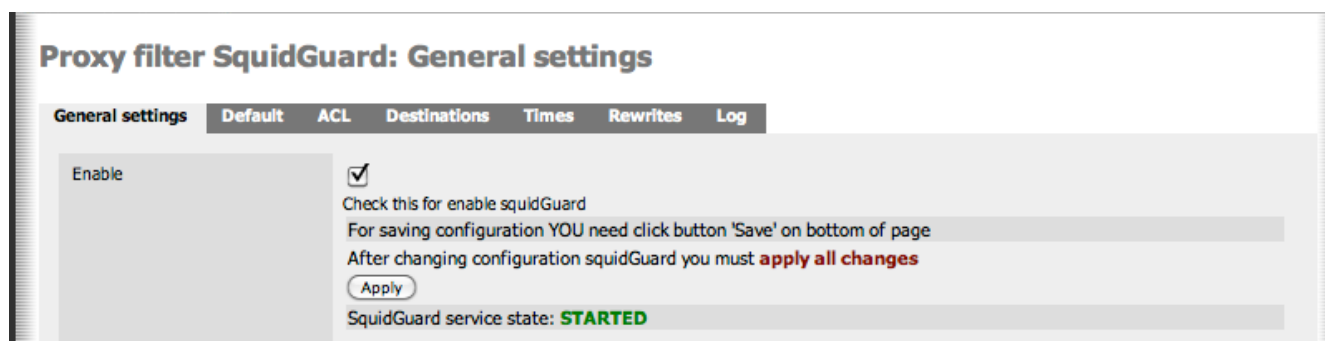
## 13 Controlling Access to the Web

One way to control access to the Internet is by creating firewall rules as described in [Firewall Rules - Block Unwanted Traffic to/from the Internet](#) . However, firewall rules are very specific and do not lend themselves well to blocking access to specific websites. A better approach to controlling access is to use the proxy filter included with RedPort wXa.

RedPort wXa's proxy filtering is based on the SquidGuard open source project. This user guide touches on very basic configuration of the proxy filter. Users requiring additional information should refer to the project's website at <http://www.squidguard.org>.

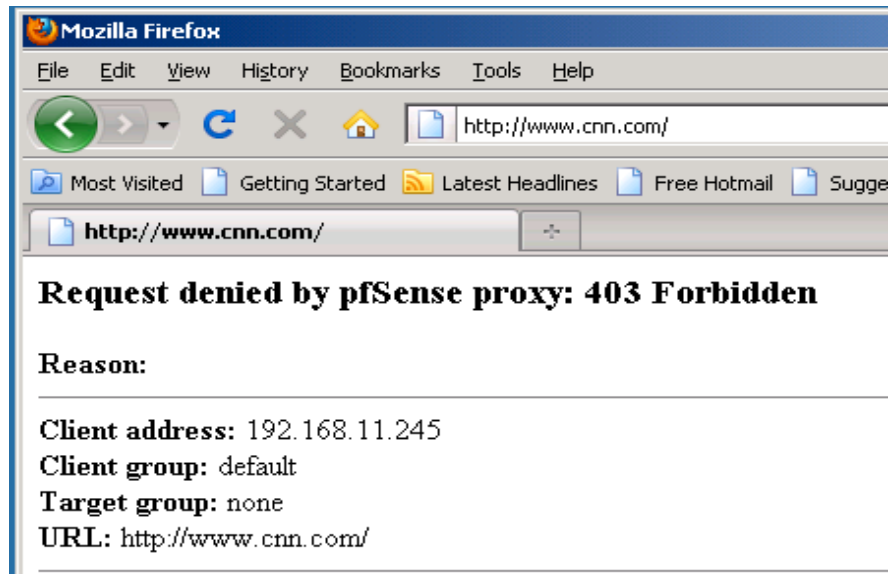
To enable the proxy filter:

5. login to the **Web Administrator**
6. Go to **Services > Proxy filter**
7. Click **Enable**
8. Click **Save** to enable the server
9. Click **Apply** to start the service



All access to the Internet will be barred as soon as the service is started. Users wanting to access the Internet will see an error message similar to the following.





Rules must now be defined that allow access to the Internet. There are several methods available to define the access rules. These methods are discussed in the remaining sections of this chapter.

## 13.1 Blacklists

A list of prohibited websites (such as porn sites) can be uploaded. One popular list can be found at <http://www.shallalist.de/>; it contains over 1.7 million entries. Commercial lists containing more than 2M entries, covering many different categories, can be purchased from [URLBlacklist.com](http://URLBlacklist.com).

A list of SquidGuard compatible lists can be viewed at <http://www.squidguard.org/blacklists.html>

Note that these lists are large and it can take time (30 minutes or more) to download and install them.

To Upload a Blacklist,

1. Enter the URL in the **Blacklist URL** field

A screenshot of a web form titled 'Blacklist URL'. It features a text input field containing the URL 'http://www.shallalist.de/Downloads/shallalist.tar.gz'. Below the input field, there is a small text label that reads 'Enter FTP, HTTP or LOCAL (pfSense) URL blacklist archive, or leave blank.' At the bottom of the form, there are two buttons: 'Upload Url' and 'Restore last'.

2. Click **Upload Url**
3. After the list has uploaded, click **Check this for enable blacklist**



4. Click **Apply** for changes to take effect

Once the blacklist is enabled, enable/disable the categories in the list with these steps:

1. go to the **Default** tab
2. Click on **Destination ruleset**
3. Click **deny** or **allow** access for the desired categories.

**Note:** Rules are executed in a first come first serve basis so if all the rules are blocked except for the very last **all** rule then access will be allowed to any website not in the list.



## 13.2 Dynamic Content Filtering

Although RedPort wXa does not directly support dynamic content filtering, there is a simple trick that can be used to enable this type of service. Like blacklisting, described in the previous section, dynamic content filtering is used to block unwanted access to the Internet. Unlike blacklisting, dynamic content filtering management is done off site, i.e. someone else takes care of keeping the lists up to date. Keeping the list on shore makes it simpler for administrators to configure and manage the settings.

To implement dynamic content filtering:

1. Go to [www.opendns.com](http://www.opendns.com) and signup for a free account


2. Add your WAN network to the account (you will need to get this information from your satellite air time provider)
3. Configure the category restrictions
4. Setup wXa to use **208.67.220.220** and **208.67.220.222** for the DNS servers as discussed in [WAN Setup](#)

---

## 13.3 Custom Destinations

At times it might be desirable create custom rules that allow/deny access to specific websites or domains. For example, say we want to bar access to all Internet sites except for any website that belongs to Google. The first step in the process is to create a custom destination for all Google hosts.

Implement this example to create a custom destination for all Google hosts using the following steps:

1. Login to **Web Administrator**
2. Select **Services > Proxy filter**
3. Select **Destinations** tab
4. Click on the  button to add a new destination
5. Name the rule; In this example we will call it google
6. Enter **google.com** in the domain list

*This list contains all the domains that apply to the destination. In this example only one domain is required. However, multiple domains can be specified, if required.*
7. Leave the **Expressions** list blank

*This list contains word fragments that appear in URLs for the domain. Word fragments are separated by "|" as in **mail|casino|game**. If a word in the list is in the URL then there is a match to the rule.*
8. Leave the **URL list** blank

*This list contains the URLs that apply to the domain. An example of this might be **www.google.com/news** or **www.google.com/imghp**. URLs matching the list are considered a match to the rule.*
9. Enter **none** for the redirect mode


*Enter a redirection mode if a user is to be taken to an external URL or an error message is to be displayed when the destination rule is matched. Leave **none** if the default rule is to be used to allow access.*
10. Enter the redirect rule or error text in the **Redirect** box. Leave blank for this example.
11. Enter **google servers** as a description for the rule
12. click **Save**

Here is our defaults destination rule:

General settings	Default	ACL	Destinations	Times	Rewrites	Log
Destination name	Domain list	URL list	Expressions	Redirect	Description	
google	google.com				google servers	 
						

13. Select the **Default** tab

14. click on **Destination ruleset**

Default destination	<input type="text" value="google !all"/>
Destination ruleset (click)  	
ACCESS: 'white' - always pass; 'deny' - block; 'allow' - pass, if not blocked.	
<b>Destination rules</b>	
google servers [google]	access <input type="button" value="allow"/>
Default access [all]	access <input type="button" value="deny"/>

15. Allow access to the google servers and deny access to all

16. Click **Save** to make the new selections effective

17. Go to **General Settings**

18. Click **Apply** to make the rule change effective


You will now be able to browse google.com but nothing else.

## 13.4 Access Control Lists (ACL)

ACL rule sets are used to create rules that apply to unique users. When creating ACL rules the IP address or network address for the allowed machine is specified in the Source IP address field. Each ACL rule has a unique rule set that can be enabled or disabled for the IP addresses in question.

Times can be applied to the ACL rules. A time slot is defined under the **Times** tab. Once defined, the time appears under the **Time** field in the ACL entry form. Select the time name that applies to the rule. Select the access mode for both the in time and overtime rules. Note that if no time is defined then overtime rules are ignored.

For example, we want everyone on the WI-FI LAN to have access to the Internet except the user on PC with IP address 192.168.20.20. Use the following steps to block the user:

1. Go to **Web Administrator**
2. Select **Services > Proxy Filter**
3. Define what is allowed or disallowed. If unrestricted access to the web is what is wanted then set the **Default access** to **allow**.
4. Click **Save** to record the settings
5. Click on the **ACL** tab
6. Click  to add an ACL rule
7. Name the rule
8. Select the order in which this rule fits into the rule scheme. Note that rules are evaluated on a first come first serve basis. For this example you can leave the default **Blank**.
9. Enter the source IP address that is to be blocked. In this example, **192.168.20.20**.  
*Networks can be specified by entering a network address followed by a netmask. As in 192.168.20.0/24 which would block access from any PC on the WI-FI LAN.*
10. Click on **Destination rule set**
11. Select **deny** for the default rule (or set access for any custom rules that have been defined)
12. Set **redirect mode** appropriately (none in this example)
13. Enter a **comment** if desired
14. Click **Save**
15. Go to **General Settings**
16. Click **Apply** to make the rule change effective

Users on PC at IP address 192.168.20.20 are now blocked from the Internet.

---

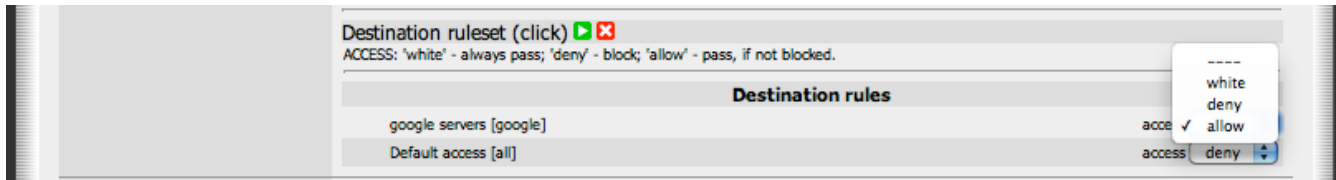
## 13.5 Whitelists

So far, all the rules we have examined are either **allow** or **deny**. As stated earlier, rules are executed in the order they are matched. Say for example we have a blanket rule that denies access to a whole group of domains and URLs. For example: 'cars'. But we want to create a **Destination** rule that overrides the **deny** behavior of one specific website in this category.

To do this, we create a Destination rule that matches the exception and then we select **white** for the access mode.

Any rules that are whitelisted have priority over the deny/allow rules that match the rule set. This is true no matter the order of the list. In other words, whitelist is used to override the default

behavior of a more general matching rule. Looking at our previous example we see that although **white** was not selected it was an option.



## 13.6 Apply your Configuration

**Warning:** Don't forget to click the **Apply** button under **General Settings** after any changes to the **Default, ACL, Destination, Times or Rewrite** lists.

## 14 Web Logging

RedPort wXa includes a powerful web based URL analyzer and logging facility. The facility allows the examination and analysis of all URLs fetched by every client on the system. This allows administrators to know what websites were accessed, who accessed them and when they were accessed.

To access Web logging:

1. Login to **Web Administrator**
2. Select **Status**
3. Select **Proxy report**

---

### 14.1 Configuration

The **Settings** tab controls the look and feel of the reports. It also controls the frequency of caching proxy log rotation and the report refresh rate.

By default, reports are generated every two hours. The administrator can, at anytime, push the **Refresh now** button to get up-to-the-minute logging. Otherwise, reports are updated based on the **Refresh scheduler**. If changes to the default schedule are needed, select the desired **refresh scheduler** value and click **Save**.

Ten copies of the caching proxy logs are maintained on the system at any given time. By default, the logs are rotated once a week so at any given time there are 10 weeks' worth of web access logs on the system. The frequency of log rotation and the specific day can be selected in the **Squid rotate log scheduler** pull down menu. Note that every **X** day corresponds to log rotation once per month on day **X**. The default is to rotate the logs on Sunday.

---

### 14.2 Disk-Full issues

If you are experiencing disk-full issues (see [Disk Usage and Monitoring](#)), it is likely that it is a combination of the cache disk area being full **and** the reporting log area on the disk is also full. If you experience this issue, it is recommended that you change the frequency of your log rotation.

**To change the frequency of your log rotation, follow these steps:**

1. Login to **Web Administrator**

2. Select **Status > Proxy report**
3. Go to **Squid rotate scheduler**
4. Using the pull down menu, select a new rotation schedule. If you have a large number of users (e.g. 200 per day), it is recommended that you change the log rotation to every day. For systems with a smaller number of users, you may need to experiment for which is the best log rotation schedule for your system.

**Warning:** For your system to properly generate logs, the **Log rotate** field under **Services->Proxy Server->Log rotate** *must* be left blank. This field will be removed in a later firmware version.

## 14.3 Reports

To view the web logging reports,

1. Login to **Web Administrator**
2. Select **Status**
3. Select **Proxy report**

**Warning:** The **Proxy report Refresh scheduler** option is by default set to run every 3 hours to incorporate new log changes into the reports. This frequency can be changed. However, it takes CPU cycles to do this so it is recommended to



accept the default value or to set it to a longer period. Also, care should be taken before modifying the **Squid rotate log scheduler** default time period. The squid log rotation should happen on a period which is slower than the **Refresh scheduler** rate. If the squid logs are rotated too quickly some of the reports can be missed since they will not be built if the logs are rotated before the reporting process has a chance to access them.

4. Select the **Lightsquid Report** tab
5. On the calendar that is displayed, select a date to view the logs

## Squid user access report

Work Period: Jul 2010

Calendar											
2010											
01	02	03	04	05	06	07	08	09	10	11	12

Top Sites	Total	Group
<a href="#">YEAR</a>	<a href="#">YEAR</a>	<a href="#">YEAR</a>
<a href="#">MONTH</a>	<a href="#">MONTH</a>	<a href="#">MONTH</a>

Date	Group	Users	Oversize	Bytes	Average	Hit %
<a href="#">31 Jul 2010</a>	grp	1	0	400 288	400 288	0.14%
<a href="#">30 Jul 2010</a>	grp	1	0	2.3 M	2.3 M	0.00%
<a href="#">19 Jul 2010</a>	grp	1	0	1.8 M	1.8 M	3.66%
<a href="#">17 Jul 2010</a>	grp	1	0	76 379	76 379	0.93%
<a href="#">16 Jul 2010</a>	grp	1	0	3.7 M	3.7 M	29.80%
<a href="#">13 Jul 2010</a>	grp	1	0	92 336	92 336	1.57%
<a href="#">11 Jul 2010</a>	grp	1	1	10.9 M	10.9 M	13.39%
Total/Average:		1	0	19.2 M	2.7 M	7.07%

[LightSquid v1.7.1](#) (c) Sergey Erokhin AKA ESL


In this example, clicking on 11 Jul 2010 shows a list of all the clients that accessed the internet that day.

## Squid user access report

Date: 11 Jul 2010 (update :: 22:00 :: 11 Jul 2010)

[Top Sites](#) Report

Big Files Report

#	Time	User	Real Name	Connect	Bytes	%	Group
1		<a href="#">192.168.11.245</a>	?	1 669	10.9 M	100.0%	<a href="#">?</a>

[LightSquid v1.7.1](#) (c) Sergey Erokhin AKA ESL

One client computer accessed the internet on this day. Clicking on the IP address of the client shows all the websites visited on that day.

Date: 11 Jul 2010					
					
Total		10.9 M			
#	Accessed site	Connect	Bytes	Cumulative	%
1	<a href="http://i.cdn.turner.com">i.cdn.turner.com</a>	285	3.2 M	3.2 M	29.3%
2	<a href="http://ds.serving-sys.com">ds.serving-sys.com</a>	7	1.2 M	4.4 M	10.7%
3	<a href="http://cache.gawkerassets.com">cache.gawkerassets.com</a>	195	1.1 M	5.5 M	9.9%
4	<a href="http://hyperion.zih.tu-dresden.de">hyperion.zih.tu-dresden.de</a>	2	600 943	6.0 M	5.2%
5	<a href="http://v18.lscache3.c.youtube.com">v18.lscache3.c.youtube.com</a>	1	385 932	6.4 M	3.3%

Clicking on the clock generates an hour-by-hour listing with the access time and the amount of data transferred during that hour.

Squid user access report

User: 192.168.11.245 (?)

Date: 11 Jul 2010

#	Accessed site	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Total
	Total	.	.	.	.	.	.	.	9.4	0.0	.	.	.	.	.	.	.	.	.	0.2	1.4	.	.	.	.	10.9 M
1	i.cdn.turner.com	.	.	.	.	.	.	.	2.6	.	.	.	.	.	.	.	.	.	.	0.6	.	.	.	.	.	3.2 M
2	ds.serving-sys.com	.	.	.	.	.	.	.	1.2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	1.2 M
3	cache.gawkerassets.com	.	.	.	.	.	.	.	1.1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	1.1 M
4	hyperion.zih.tu-dresden.de	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0.6	.	.	.	.	.	600 943
5	v18.lscache3.c.youtube.com	.	.	.	.	.	.	.	0.4	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	385 932
6	www.cnn.com	.	.	.	.	.	.	.	0.3	.	.	.	.	.	.	.	.	.	.	0.0	.	.	.	.	.	366 814

Web logging along with proxy web filtering make a powerful combination for controlling access to Internet websites.

## 15 GPS Tracking

GPS tracking is available on your wXa system for Inmarsat's FleetBroadband service and Iridium's OpenPort service that have GPS built in to their satellites. To use GPS tracking, registration is required at [www.RedPortGlobal.com/gsattrack](http://www.RedPortGlobal.com/gsattrack) for GSatTrack. There is a fixed monthly fee for the tracking service and the user is responsible for any additional airtime charges. The airtime amount is considered negligible though, with an estimation of 500 bytes for one position report. Please see details below for enabling GPS tracking on your wXa system.

To enable GPS Tracking on wXa system, use the following steps:

1. Login to **Web Administrator**
2. Go to **Services > GPS Tracking**

General Tracking Parameters	
Tracking Interval	<input type="text" value="60"/> Specify the tracking interval in minutes
Tracking powered by GSatTrack	
Please visit <a href="http://www.RedPortGlobal.com/gsattrack">www.RedPortGlobal.com/gsattrack</a> for registration information	
FleetBroadband	<input checked="" type="checkbox"/> Enable a connected FleetBroadband
OpenPort	<input type="checkbox"/> Enable a connected Iridium OpenPort
<input type="button" value="Save"/>	

3. Specify a **Tracking Interval** in minutes
4. Select your system
5. Click **Save**

**Note:** Registration information for **GSatTrack** can be found at <http://www.RedPortGlobal.com/gsattrack>

## 16 Disabling Skype and other P2P Applications

Skype and instant messaging programs such as MSN Instant Messenger fall into a class of software called peer-to-peer or P2P applications. These applications are designed to circumvent firewalls allowing users to communicate and share data. For satellite administrators this class of program is very problematic. P2P programs consume a lot of satellite airtime resources and are very difficult to block. Fortunately, RedPort wXa is one of the few devices in the market place that can block P2P applications.

Use the following procedure to block P2P programs from accessing the Internet:

1. Configure RedPort wXa's proxy server and test it (See [Caching Proxy Server](#))  
*You can configure either transparent or manual mode. In transparent mode users will only be able to access regular HTTP URLs. HTTPS and FTP will only be available to users using manual proxy configurations.*
2. Enable the proxy filter and block numeric IPs. (See [Controlling Access to the Web](#))  
*If the proxy is used only to block numeric IP addresses then enable it and set the default destination rule set access to **allow**. This step is necessary because Skype is able to negotiate traffic through the proxy server otherwise. Note that as soon as this feature is enabled access to satellite terminals by URLs containing IP addresses such as `http://192.168.0.1` will be forbidden. Create ACL rules in the proxy filter or configure the client proxy settings to not use the proxy server for access to these hosts.*
3. Delete all firewall rules for the LAN and/or WI-FI (WLAN).
4. Add firewall rules that allow the LAN to access 192.168.10.1 and the WLAN to access 192.168.20.1 or the users will not be able to do DNS, DHCP and other RedPort wXa services.
5. Set the network settings on the PC to either use DHCP with automatic DNS settings or manually set the DNS servers to point to the RedPort wXa.
6. Add appropriate firewall rules if access to external DNS servers is required.
7. From a client PC ping the RedPort wXa and make sure that DNS lookups work.
8. Configure the proxy settings on the PC (See [Transparent vs. Manual Proxy](#)) and test access to the web.
9. Run Skype and confirm that it can't reach the internet.

## 17 Configuring Failover from Primary to Backup Satellite Link

RedPort wXa routers (except wXa-202) can be configured to automatically route traffic through a backup link (WAN2) if the primary satellite (WAN) connection fails.

On the surface this seems like an easy problem to solve, however it is not so simple to accomplish. The obvious thing to do when the WAN fails is to have wXa reconfigure the routing tables so that all Internet bound traffic is rerouted through WAN2. This is exactly what is done. However, the complication lies with DNS. DNS servers fail unless some site-specific configurations are done.

The reason for this is due to RedPort wXa using internal routing tables to reach the configured DNS servers. This means that without static routes configured, it will only use the primary WAN connection to reach DNS servers. Static routes must be configured to access DNS server(s) on the WAN2 interface. Without static routes, the alternate DNS servers cannot be reached which will cause internet access failure.

The way DNS is routed depends on the way the WAN and WAN2 (OPT1) ports are configured. See [Initial Interface Configuration](#) for configuration steps.

**There are three possible scenarios to consider:**

1. Both WAN and WAN2 have static IP addresses (RECOMMENDED)

In this case there is nothing to worry about as long as one DNS server from each WAN is assigned to the DNS server list under **System->General setup**. Since each server is bound via a static route through the appropriate interface, only the DNS server for the active link will be used.

2. Primary WAN uses DHCP and WAN2 uses static IP address

This again is not an issue. All traffic is routed through WAN when it is active. Since access to the dynamically assigned DNS server is routed through the WAN there are no issues reaching it during normal operation. On a failover, the dynamically assigned DNS, however, is not available. Under these conditions, the secondary DNS server is used. Since WAN2 is a static IP address, a static route has been added which allows the router to route traffic to the secondary DNS server.

- Both primary WAN and secondary WAN2 connections use DHCP; or primary WAN is static and the WAN2 uses DHCP

Under these conditions, routes to the DNS servers are lost when the primary connection goes down. Since the router uses the WAN connection to route all its internal default traffic, access to the DNS servers is lost. Traffic from the client is routed correctly through WAN2, however, DNS lookups in the router and those of the client's (if using the DNS forwarder which is on by default) fail causing the internet to be inaccessible.

**Best practice:** When configuring failover and/or load balancing it is best to use scenario 1 above where both WAN and WAN2 are configured with static IP addresses.

Unfortunately, scenario three is the most common and therefore, special setup is required to make failover work.

**For scenario 3, there are two ways to address the problem.** The first one is a simple but less efficient method that moves DNS resolution to the clients. The second is a more complex approach that preserves the caching efficiency of RedPort wXa's DNS forwarder. The second approach is recommended but we include the first for completion.

---

## 17.1 Scheme 1 - Client Based DNS Lookups

Under this scheme, publicly available Internet DNS servers are pushed to the clients during their DHCP configuration. Since DNS queries are done directly by the client and not the router, traffic is passed through directly to the backup link. DNS lookups therefore succeed and Internet access continues to be available. This scheme works because traffic from inside the network is policy routed by the router and it is therefore not bound to the internal router DNS usage limitations.

---

**Warning:** One side effect of Scheme 1 is that internet functions initiated by the router itself will fail (e.g. Captive Portal). If you are running in a configuration which requires router based DNS server to continue working during a failover, then consider using Scheme 2.

---

Following are the configuration changes required for scheme 1:

1. Login to the **Web Administrator**
2. Go to **System > General Setup**
3. In the **DNS Servers** field, enter the IP addresses of two publicly available DNS servers; A good choice would be to use servers provided by opendns.com at **208.67.222.222** and **208.67.220.220**
4. Uncheck **Allow DNS server list to be overridden by DHCP/PPP on WAN** on the same form

5. Click **Save** to save the configuration
6. Go to **Services > DNS forwarder**
7. Uncheck **Enable DNS forwarder** to disable the DNS forwarder
8. Click **Save** to save the configuration

## 17.2 Scheme 2 - Static Routes to DNS Servers

Scheme 2 is a bit more complex since it requires the creation of static routes to DNS servers on each interface. This configuration requires local knowledge of the gateway IP addresses for each WAN connection. The IP addresses will be unique to each installation.

**Best practice:** Creation of static routes for DNS servers can be bypassed if the DNS servers are used as the link monitors when configuring the failover or load balancing pools. When selecting DNS servers as monitors wXa automatically creates the static routes.


The advantage of this scheme over the previous one is that the DNS forwarder is preserved allowing DNS caching and more importantly access to DNS by the internal wXa services such as the captive portal.

1. Login to the **Web Administrator**
2. Go to **System > General Setup**
3. In the **DNS Servers** field, enter the IP addresses of two publicly available DNS servers; A good choice would be to use servers provided by opendns.com at **208.67.222.222** and **208.67.220.220**

4. Uncheck **Allow DNS server list to be overridden by DHCP/PPP on WAN** on the same form
5. Go to **Status > Interfaces** to determine the address of the gateway for each WAN interface. Below is an example for the primary WAN on our development system. The

WAN interface (em0)	
Status	up
DHCP	up <input type="button" value="Release"/>
MAC address	00:0c:29:7c:c3:b6
IP address	192.168.0.9
Subnet mask	255.255.255.0
Gateway	192.168.0.1
ISP DNS servers	208.67.222.222 208.67.220.220
Media	1000baseTX <full-duplex>
In/out packets	69139/32517 (5.73 MB/4.03 MB)
In/out errors	0/0
Collisions	0

gateway in this case is 192.168.0.1.

6. Go to **System > Static routes** to configure static routes to each DNS server through the gateway on each WAN interface
7. Click on the  to add a new route
8. Select the appropriate **<WAN interface>**
9. Enter the **<IP address for the DNS server>** for the interface
10. Enter the **<gateway>**
11. Enter a **<description>** as a reminder
12. Click **Save**
13. Repeat steps 7-12 for your second WAN interface
14. Go to **Services > DNS forwarder**
15. confirm that **Enable DNS forwarder** is checked

## Services: DNS forwarder

☒ **Enable DNS forwarder**

Following is an example where DNS server 208.67.220.220 is to be accessed through WAN2 with gateway 172.16.225.2 and DNS server 208.67.222.222 is accessed through WAN using its gateway at 192.168.0.1



## System: Static Routes

Interface	Network	Gateway	Description
WAN2	208.67.220.220/32	172.16.225.2	Route to DNS2 on WAN2
WAN	208.67.222.222/32	192.168.0.1	Route to DNS1 on WAN



Continue the configuration in the next section on [Configuring Failover Pool](#).

## 17.3 Configuring Failover Pool

The following steps describe how to configure and enable the failover pool:

1. Login to the Web Administrator
2. Select **Services->Load balancer**
3. Select the **Pools** tab
4. Click the button to add a new pool
5. Enter a **<name>** such as Failover
6. (Optional) Enter a **<description>** for the pool
7. From the **Type** dropdown menu, select **Gateway**
8. For **Behavior**, select **Failover**

### Load Balancer: Pool: Edit

<b>Name</b>	<input type="text" value="Failover"/>
<b>Description</b>	<input type="text" value="Failover from WAN to WAN2"/>
<b>Type</b>	<input type="text" value="Gateway"/>
<b>Behavior</b>	<input type="radio"/> Load Balancing <input checked="" type="radio"/> Failover Load Balancing: both active. Failover order: top -> down. NOTE: Failover mode only applies to outgoing rules (multi-WAN).

9. Configure the pools in steps 10-13
10. From the **Monitor IP** pull down menu, select **DNS Server 1**
11. For **Interface Name**, select **WAN**
12. Click **Add to pool**
13. Repeat steps 10-12 again for **DNS Server 2** and **WAN2**

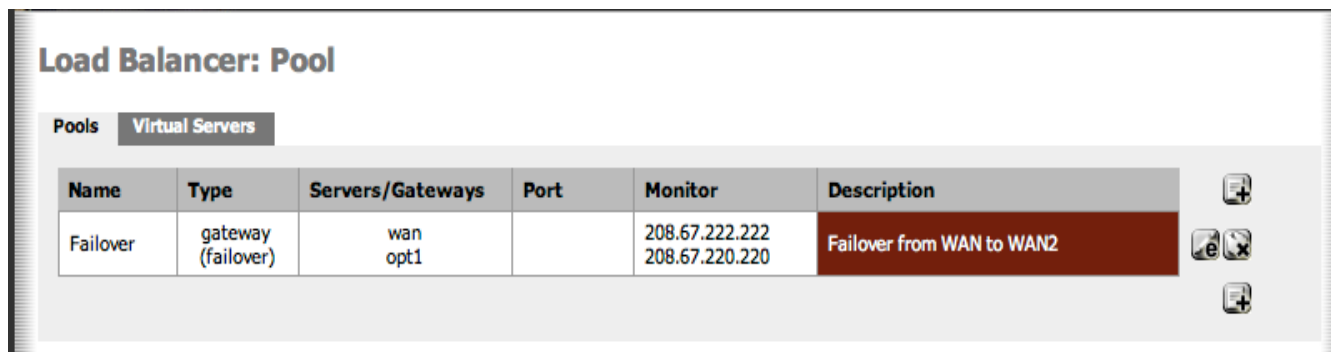
**Note:** Static routes to DNS servers are created automatically when selecting the monitor IP hosts.

14. Confirm that the both **WAN** and **WAN2(OPT1)** have been added to the list

**Note:** The order is important. The first item on the list is considered to be the primary interface. The second is the backup.

15. Click **Save**

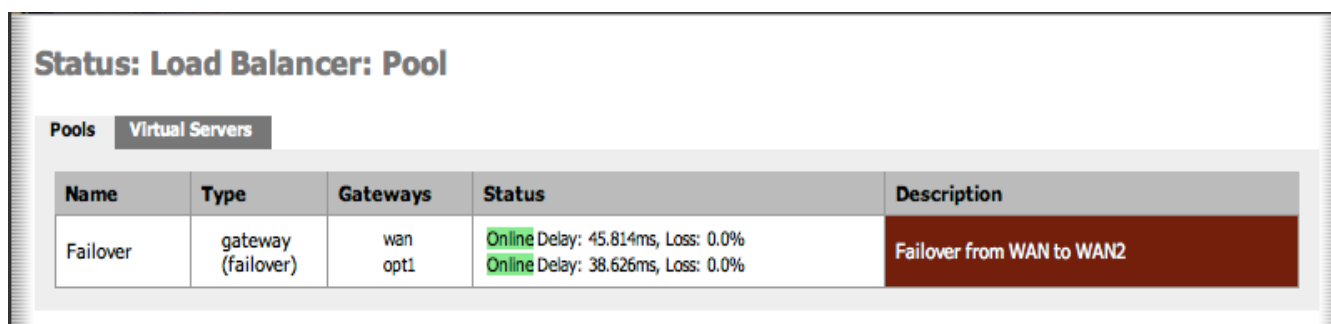
The load balancer pool should look similar to the following:



Pools Virtual Servers					
Name	Type	Servers/Gateways	Port	Monitor	Description
Failover	gateway (failover)	wan opt1		208.67.222.222 208.67.220.220	Failover from WAN to WAN2

16. Go to **Status->Load Balancer**

17. Confirm that the failover pool is active and operating properly. The display should look similar to the following:



Pools Virtual Servers				
Name	Type	Gateways	Status	Description
Failover	gateway (failover)	wan opt1	Online Delay: 45.814ms, Loss: 0.0% Online Delay: 38.626ms, Loss: 0.0%	Failover from WAN to WAN2

The load balancing and failover software on the RedPort wXa pings the monitoring IP every 10 seconds. A failover occurs 10-15 seconds after a ping failure is detected.

**Warning:** Note that monitoring the DNS servers as recommended above incurs satellite traffic. On some systems it might be undesirable to generate airtime traffic on the back up unit. If this is the case then the WAN2 gateway can be selected for monitoring. Monitoring the gateway for the backup WAN causes no airtime traffic since this unit is local. Since the unit is a backup unit to be used only if the primary is off-line it really does not matter if the unit is operational or not. If

there is no satellite connectivity the ping monitor will still indicate that the unit is on-line and ready to pass traffic. If the backup unit is down then no traffic will pass making irrelevant that a false positive is being reported by the monitor.

---

Note that static routes to the DNS servers are not created when a gateway is selected as the ping host. DNS failure will occur on failover unless static routes are manually created to the DNS hosts as described above in [Scheme 2 - Static Routes to DNS Servers](#).

Continue the configuration in the next section on [Policy Based Routing](#).

---

## 17.4 Policy Based Routing

There is one final step in enabling failover. This is to change the system firewall to use policy routing instead of the default system table.


---

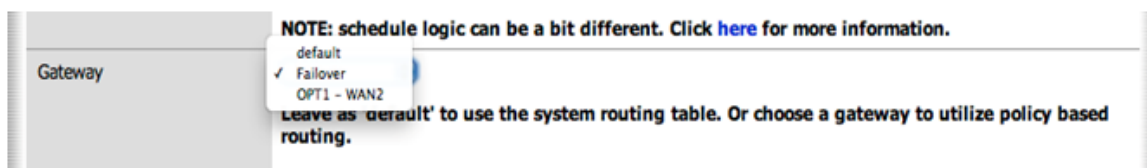
**Warning:** The failover will not work unless this step is completed.

---

By default, all firewall rules are configured to use the system's default routing table. As previously discussed, this kind of routing does not work during a failover since the default routing table uses WAN as the default interface. In order for traffic to be routed to the correct WAN port during a failover, all firewall rules for the LAN and WLAN (Wi-Fi) must be modified to use policy routing.

To configure the system to use Policy Based Routing:

1. Login to the Web Administrator
2. Go to **Firewall->Rules**
3. click on the **LAN** and/or the **WLAN** tab
4. Click on the  button next to a rule
5. On the **Gateway** pull down menu, select **Failover** (or your failover pool name)



6. Click **Save**

- Repeat steps 3-6 for every firewall rule for the LAN and WLAN

## 17.5 Failover and Firewall Rules

Most installations implementing failover consist of a primary satellite link with higher (and less expensive) bandwidth and a slower more expensive backup link. It is therefore reasonable to want to restrict the kinds of traffic that flow through the backup link when a failover occurs. For example, users might be allowed to browse the Internet when the primary link is up but only allowed to do e-mail when in failover mode.

The hierarchical nature of the firewall rules in RedPort wXa makes it simple to implement this sort of scheme. As stated previously in [Firewall Rules - Block Unwanted Traffic to/from the Internet](#) rules are implemented in order from top to bottom. As soon as a rule is matched, filtering is stopped and the corresponding action is taken.

**To implement the above scheme, 3 rules are required on the LAN interface:**

**Rule 1: All HTTP bound traffic should be routed to the WAN interface**

**Rule 2: All POP traffic should be routed to the Failover pool**

**Rule 3: All SMTP traffic should be routed to the Failover pool**

When the system is fully operational HTTP, SMTP, and POP traffic is routed through the WAN port. On failover, however, HTTP traffic is blocked (because there is no WAN interface) while POP and SMTP traffic continue to flow through the backup interface defined in the Failover pool.

**Alternate implementation:** An alternate implementation allows *all* traffic through the WAN but only POP/SMTP traffic through the failover rule would have the first 2 rules in the list route the mail while the default or last “catch all” rule routes traffic through the default gateway (i.e. WAN).

LAN WAN WAN2									
	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<input type="checkbox"/>	TCP	*	*	*	25 (SMTP)	Failover		SMTP to Failover pool	
<input type="checkbox"/>	TCP	*	*	*	110 (POP3)	Failover		POP3 to Failover pool	
<input type="checkbox"/>	*	*	*	*	*	*		Everything else to WAN	

## 17.6 Failover and Captive Portal

Special care must be taken when configuring failover on systems that use Captive portal. Since the Captive portal service runs on the router, like DNS, it depends on the system routing table to reach its Radius servers. Since the default route is lost during a failover, static routes must be used to define routes to the Radius servers. Fortunately this is simple to do.

1. Login to the **Web Administrator**
2. Go to **Services->Captive portal**
3. For the Primary RADIUS server, select an **Interface** from the dropdown menu (e.g. WAN)
4. For the Secondary RADIUS server, select an **Interface** from the dropdown menu (e.g. WAN2)

**Note:** Typically WAN is bound to the primary server and WAN2 to the secondary server although the assignment is not important just as long as each RADIUS server is bound to different interfaces. The default is to *not* bind the RADIUS servers to any interface which means that the system default route (i.e. WAN) is used to route the traffic.

Authentication	<input type="radio"/> No authentication <input type="radio"/> Local user manager <input checked="" type="radio"/> RADIUS authentication
Primary RADIUS server	
IP address	<input type="text" value="204.109.60.96"/> <small>Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.</small>
Port	<input type="text"/> <small>Leave this field blank to use the default port (1812).</small>
Shared secret	<input type="text" value="xgate"/> <small>Leave this field blank to not use a RADIUS shared secret (not recommended).</small>
Interface	<input type="button" value="WAN"/> <small>Choose which interface to route traffic through for this RADIUS server. Hint: use default unless implementing failover or load balancing. In multi-WAN configurations WAN is usually the desired choice.</small>
Secondary RADIUS server	
IP address	<input type="text" value="208.86.227.138"/> <small>If you have a second RADIUS server, you can activate it by entering its IP address here.</small>
Port	<input type="text"/>
Shared secret	<input type="text" value="xgate"/>
Interface	<input type="button" value="WAN2"/> <small>Choose which interface to route traffic through for this RADIUS server. Hint: use default unless implementing failover or load balancing. In multi-WAN configurations WAN2(opt) is usually the desired choice.</small>

---

## 17.7 Failover and Proxy Web Services

Unfortunately, the proxy web service is not compatible with multi-WAN configurations such as Failover or Load balancing. The reason for this is that all services that run on the router such as the proxy server, Captive portal, DNS forwarder, etc. use the system routing tables that define the default route through the WAN port. When the WAN port is not available there is currently no way to traffic through WAN2.

Many onboard services such as DNS and the Captive portal can be made to work by defining static routes to the servers with which they interact. The proxy server, however, only supports one forward proxy server that, by default, is accessed through the WAN port.

Fortunately, there is a work around solution. Proxy services can be made to work, if all of the following are true:

1. wXa has been registered with a provider
2. A wXa username and password has been assigned
3. The wXa account is in good standing
4. XWeb compression is enabled

---

**Note:** In a failover state, access to websites that has been configured to bypass compression (see [Custom Options](#)) will fail since the request to the internet page is generated locally and the request fails because the route through the default interface is down.

---

To configure Proxy failover:

1. Login to **Web Administrator**
2. Go to **Services->Proxy server**
3. Select the **Compression** tab
4. Click the box to **Enable Failover or Load balancing**
5. Select the **Secondary proxy server** (i.e. the back up XWeb server). The secondary proxy server must be different than the primary.
6. Select **Service Type** required - either Failover or round-robin load balancing
7. Click the box to bind proxy servers to interfaces

---

**Note:** The primary proxy is normally bound to the WAN and the secondary to WAN2 although in practice it doesn't matter.

---

8. Click **Save** to enable

<b>Enable Failover or Load balancing</b>	<input checked="" type="checkbox"/> <p>This option enables proxy failover or load balancing. NOTE: Don't forget to create static routes for proxy hosts when configuring multi-WAN load balancing or failover. Static routes are configured below in "Bind proxy servers to interfaces".</p>
Secondary proxy server	<input type="text" value="xweb2.gmn-usa.com"/> <p>Select secondary proxy server. Must differ from the primary server.</p>
Service Type	<input type="text" value="Failover"/> <p>Select load balancing or failover mode.</p>
<b>Bind proxy servers to interfaces</b>	<input checked="" type="checkbox"/> <p>Bind routes to primary and secondary compression proxy servers to network interfaces.</p>
Primary proxy interface	<input type="text" value="WAN"/> <p>The interface the primary proxy server will bind to. Hint: usually WAN.</p>
Secondary proxy interface	<input type="text" value="WAN2"/> <p>The interface the secondary or backup proxy server will bind to. Hint: usually WAN2 (or OPT1).</p>

Failover and load balancing can be done without binding the proxy servers to specific interfaces. When the servers are not bound to specific interfaces all traffic is routed through the default route (i.e. WAN). If one of the servers is inaccessible then the second one will fill in. This provides redundancy at the server level but not the local interface level.

**Best practice:** On systems with only one WAN it is recommended that failover be enabled to provide browsing redundancy.




## 17.8 Manual Failover

Manual failover is initiated by the administrator, by selecting which interface the traffic should be routed through.

To view the amount of traffic routed through the currently selected interface since boot up, use the following steps:

1. Login to **Web Administrator**
2. Go to **Status > System Overview**

## System Overview

System information	
Name	webxaccelerator.gmn-usa.com
Version	<b>1.2.3.23x-RELEASE</b> built on Mon Mar 12 22:33:29 UTC 2012
Run Status	Operational
Uptime	1 day, 02:08
Default (WAN)	37956336/5185616 (36.20 MB/4.95 MB) <a href="#">Change default route/interface</a>
State table size	11/10000 <a href="#">Show states</a>
MBUF Usage	273 /525
CPU usage	 0%
Memory usage	 16%
Disk usage	 27%

### 17.8.1 Changing the Default Interface

To Change the default interface:

1. Login to **Web Administrator**
2. Go to **Status > System Overview**
3. Click **Change default route/interface** on the **System Overview** page (or)  
Select **System->Default route**

The **Set Default Route/Interface** page displays the system WANs that have been configured and which have routes defined to an external gateway. The traffic through each interface is also listed and updated every 5 seconds.

4. Click the **Select** button next to your chosen interface



## Set Default Route/Interface

Select default system interface		
Select	<b>WAN - default</b>	159489048/136709583 (152.10 MB/130.38 MB)
Select	<b>WAN2</b>	14874192/12501749 (14.19 MB/11.92 MB)
Select	<b>WAN3</b>	91946045/9481091 (87.69 MB/9.04 MB)

Once selected, all traffic will be routed through this interface unless otherwise specified in the firewall rules as described in the next section.

### 17.8.2 Firewall and Routing

Changing the interface will change the default gateway used by the router. This means that all traffic entering the unit will be routed through this interface unless firewall rules have been created to route otherwise.

**Warning:** When creating firewall rules which are to follow the default route make sure that the selected gateway is set to **default**.

**Example:** The example listed below displays a set of rules that allows users to browse a web server located at IP address 74.125.159.105 through any interface set with manual failover while only allowing general browsing through the WAN port.

## Firewall: Rules

LAN WAN WAN2 WLAN WAN3									
	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<input type="checkbox"/>	TCP	*	*	74.125.159.105	*	*		Access to specific host through manual failover	
<input type="checkbox"/>	*	LAN net	*	*	*	WAN		Default LAN -> any	

---

## 17.9 Swapping WAN/WAN2 Cables

As you have seen, configuring a Failover strategy is quite complex and not for the faint hearted. One strategy that is simple and foolproof has not been discussed. This strategy involves configuring the router with only the WAN port attached to the primary satellite interface using DHCP addressing. When a failure of the primary link is observed, a trained operator removes the Ethernet cable to the main satellite terminal and replaces it with a cable running between the backup satellite unit and the WAN port. No software configuration is required to implement this strategy! This technique is simple and easy to implement and should be given serious consideration.

---

### 17.10 Testing Failover

To test the Failover configuration:

1. Login to **Web Administrator**
2. Go to **Status > Load Balancer**
3. Disconnect the Ethernet cable to the primary WAN and observe the failover on the **Load Balancer** page
4. Verify that the PCs on the LAN/WLAN are able to access the internet through the backup WAN2
5. Plug the Ethernet cable back into the WAN port and observe that the system goes back to normal routing through this port using **Load Balancer** to monitor the status
6. Unplug the WAN2 port
7. Verify that the PCs on the LAN/WLAN are able to access the internet

---

### 17.11 Monitoring Failover Status

The status of the Failover pool can be monitored on the **Web Administrator** at **Status->Load Balancer** as noted in the previous section, [Testing Failover](#). This can be inconvenient since it requires refreshing a web page to check the status of satellite network.

An alternative and more convenient way to monitor the links is to use a free utility called **FreePing.exe** found on the resource DVD. FreePing can be configured to monitor the IP address of the primary satellite link gateway. When the gateway is inaccessible a visual alarm is displayed on the monitoring PC.

---

## 18 Failover to Serial/USB Satellite Terminal

RedPort wXa supports dialing through serial satellite terminals hooked up directly to the USB ports on the unit. Both the Iridium 9555 and the 9505a (via the use of a Prolific PL2303 USB to serial adapter) have been tested although any terminal that supports AT commands should work.

USB devices such as the Iridium 9555 are directly supported by plugging the device into the USB port in the rear of the unit. Serial terminals such as Iridium LBT based phones or Inmarsat Fleet systems will require a USB to Serial adapter. Adapters with Prolific PL2303 chip sets have been tested and found to be reliable.

---

### 18.1 Manual Failover

Manual failover to a dialup terminal hooked up to a USB to serial adapter can be done easily with these steps:

1. Login to the **Web Administrator**
2. Go to **System > PPP Dialup**
3. Enter **PPP Dialup Settings** for **Phone Number** (minimum configuration)
4. Enter additional **PPP Dialup Settings**

---

**Note:** Dialup settings need to be entered into the form before a connection can be established. The parameters are stored in the system configuration.

---

5. Click **Save**
6. Click **Connect** to initiate a dialup PPP session

Once connected all traffic configured to pass through the WAN will be redirected through the dialup connection. Note that the dialup connections uses the firewall rules configured for the WAN.

## PPP Dialup

**Manage Dialup PPP Connection**

Press "Connect" to start PPP session

**PPP Dialup Settings**

ISP username	<input type="text" value="iridium"/> Optional username only if required by ISP
ISP password	<input type="text" value="iridium"/> Optional password only if required by ISP
Extra initialization	<input type="text" value="at+cbst=71,0,1"/> e.g. AT+CBST=71,0,1 for Iridium
Phone number	<input type="text" value="008816000025"/> e.g. 008816000025 for Iridium or **94# for INMARSAT MPDS
Baud rate	<input type="text" value="19200"/> e.g. 19200 for Iridium or 115200 for INMARSAT MPDS
Idle timeout	<input type="text" value="300"/> Idle timeout in seconds. Enter 0 or leave blank to disable timeout

### 18.1.1 Iridium Connection Parameters

Parameter	Value
Phone Number	008816000025
Extra Init	at+cbst=71,0,1
Baud Rate	19200
ISP Username/Password	Optional

### 18.1.2 Inmarsat MPDS Connection Parameters

Parameter	Value
Phone Number	**94#
Extra Init	N/A
Baud Rate	115200
ISP Username/Password	Provided by airtime provider

## 18.2 Manual Failover using Telnet

The following steps will cause a Failover to a serial port-based satellite terminal connected to one of the USB ports on the RedPort wXa:

1. Connect the terminal to a USB port on the wXa

Either USB port will work. Use a Prolific PL2303 based USB to serial adapter for older style serial phones that do not have a direct USB connector. The Iridium 9555 satellite phone can be connected directly to a USB port using the USB cord supplied with the phone. Other serial based satellite terminals such as Mini-M, MSAT, and Globalstar should also work.

2. Open a command window and use the Telnet command to establish a connection to the wXa on port 5454:

**Telnet 192.168.10.1 5454**

The Telnet command is not installed by default on Windows 7/Vista. To install telnet on newer Windows systems go to the **Control panel->Programs and Features** and select **Turn Windows features on or off**. Place a check next to **Telnet Client** and click **OK**.

3. Set the connection parameters by typing:

**AT+DP=<phone\_num>,<baud>,<auth\_name>,<auth\_password>,<extra\_init\_string>**

where **<phone\_num>** is the number to be dialed

**<baud>** is the speed of the serial connection between the phone and the wXa

**<auth\_name>** is the ISP user login name

**<auth\_password>** is the ISP login password

**<extra\_init\_string>** is an optional initialization string

### Example

Enter the following when using Iridium Direct Internet:

AT+DP=0088160000606,19200,iridium,iridium

wXa will respond with ERROR if a syntax error was detected or OK otherwise.

4. Dial the connection by typing one of the following:

**ATDT=IRIDIUM** if connecting to Iridium

**ATDT=GENERIC** for all other connections

wXa will respond with ERROR if the dialup failed otherwise OK.

5. Once **OK** is returned the unit is on line

All traffic from the LAN/WI-FI side of wXa will be routed through the satellite phone until the connection is disconnected or dropped.

6. To disconnect, enter **ATH0**
7. **OK** is returned once the terminal is disconnected

The system log can be viewed for connection details. Access to the system log is on the **Web Administrator** at **Status->System logs**.

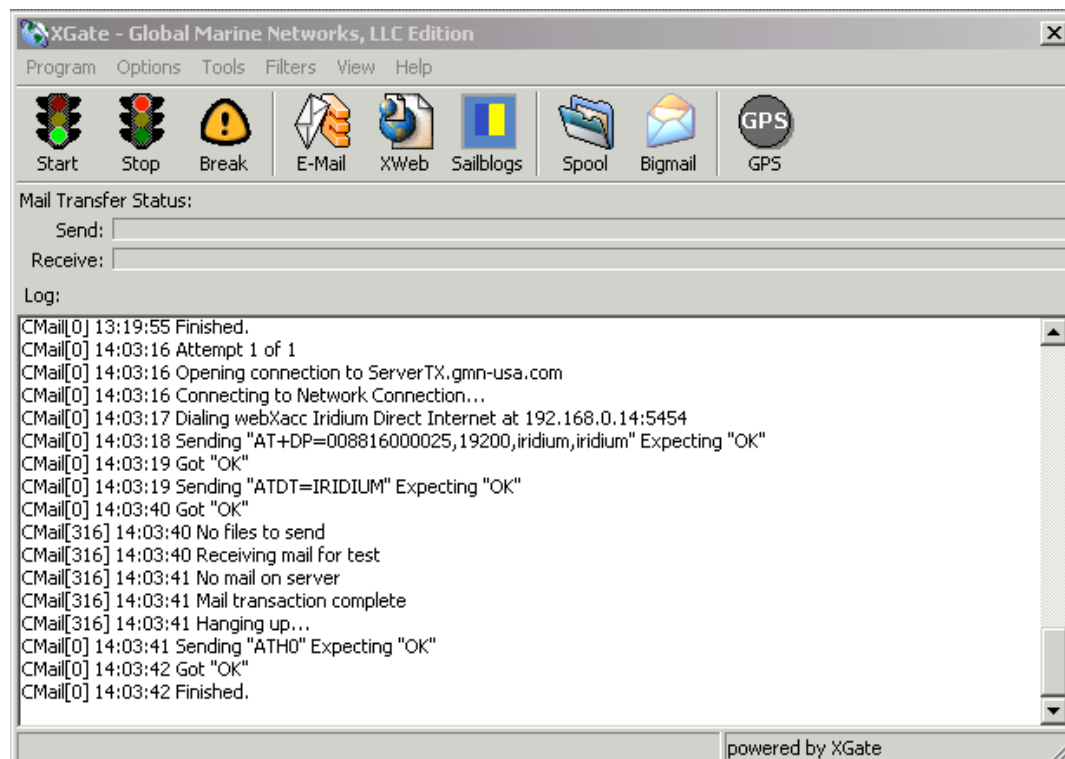
## 18.3 Automatic Failover with XGate

GMN's email client, XGate, can be configured to automatically cause a failover to a USB connected backup terminal when the primary broadband satellite device fails.

To configure XGate for this type of service:

1. Go into XGate's settings under **Connection**
2. Set the default connection to **Network Connection** and then type to **webXacc Iridium Direct Internet**
3. Enable **Use another connection if already open** to allow XGate to use the primary WAN connection for service

**Note:** The failover will then only occur if the primary link is down. Unchecking **Use another connection if already open** will result in XGate causing a failover on every connection.



## 19 Load Balancing

The load balancing functionality in wXa allows the distribution of traffic over multiple WAN connections using round robin scheduling. Load balancing optimizes bandwidth by allowing the concurrent use of two (or more) satellite links while also providing the failover capabilities described above in [Configuring Failover from Primary to Backup Satellite Link](#).

A multi-WAN failover configuration limits use to the primary satellite interface and switches to the secondary interface if the primary fails. Load balancing, on the other hand, allows the use of both satellite systems concurrently effectively doubling the overall bandwidth to the Internet. The actual bandwidth increase depends on a number of factors that include the type of connection being requested and the number of available WAN connections. Like with failover, load balancing will also cause all traffic to be funneled through the remaining channels should one of the satellite interfaces fail.

Load balancing routes traffic over multiple WAN connections using round robin scheduling with sticky connections. This means that when a request is made to a specific server, that request will be channeled through a specific WAN. When a new connection is requested, the wXa will check the instantaneous utilization of each WAN and redirect the request through the least utilized WAN port. Once the connection is established, the open connection will remain on that WAN port until the session completes. This means that when a file download is requested, the download request will be routed through a specific WAN and will remain on that port until the download completes. For single connections, the fastest bandwidth obtained is that of the fastest WAN interface. The connection speed for single sessions is not the sum of the speed of both ports! Increased bandwidth utilization results when multiple sessions are requested at the same time. Under normal circumstances (i.e. a single user browsing the internet) multiple sessions are requested at the same time. A typical webpage (www.cnn.com, for example) has numerous links that are all requested simultaneously. Each request is a separate session that would be routed (in round robin fashion) through an appropriate load balanced WAN port. So under normal web browsing conditions a doubling (or more) of bandwidth is observed (unless sticky connections are enabled as described in [Sticky Connections](#)). This same logic also applies to a multi-user situation where numerous users are accessing the Internet at the same time.

## 19.1 Creating Load Balancing Pool

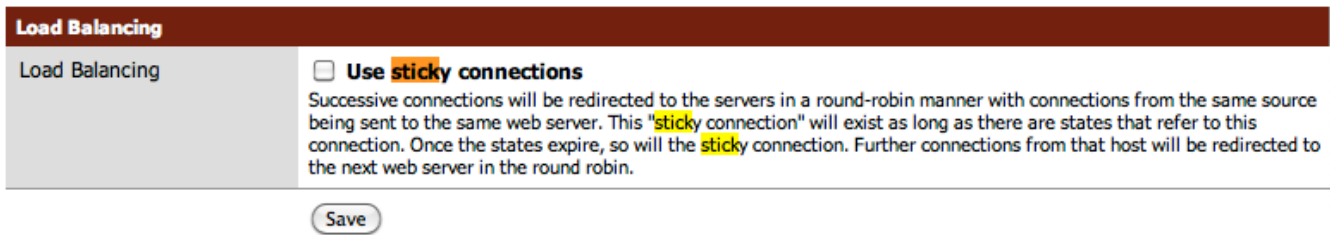
Load balancing pools are created exactly the same way as failover pools. All the same cautions, restrictions, and setup considerations for failover apply to load balancing.

To implement Load balancing, follow the procedures described in [Configuring Failover from Primary to Backup Satellite Link](#) except select **Load balancing** instead of **Failover** when creating the pool in [Configuring Failover Pool](#) and use the **Load balancing** pool (instead of the **Failover** pool) when defining policy based routing in [Policy Based Routing](#).

## 19.2 Sticky Connections

Each time a web page is opened for viewing; new connections to servers coded in the URLs are evaluated and routed by the Load balancer. This can cause problems for some secure websites such as those used for banking. Some secure websites require that the IP address used for a specific banking session be constant. Since load balancing routes traffic through different WANs the originating IP address can change causing the site to close the session with a security warning.

This problem can be addressed in one of 2 methods:



The screenshot shows a web interface for configuring Load Balancing. At the top, there is a dark red header with the text "Load Balancing". Below this, on the left, is a grey sidebar with the text "Load Balancing". The main content area has a white background. It features a checkbox labeled "Use sticky connections" which is currently unchecked. To the right of the checkbox is a detailed explanation: "Successive connections will be redirected to the servers in a round-robin manner with connections from the same source being sent to the same web server. This 'sticky connection' will exist as long as there are states that refer to this connection. Once the states expire, so will the sticky connection. Further connections from that host will be redirected to the next web server in the round robin." At the bottom of this section is a "Save" button.

**Method 1.** The simplest way to resolve this kind of issue is to enable sticky connections when load balancing:

1. Login to the **Web Administrator**
2. Go to **System > Advanced**
3. Under **Load Balancing**, select **Use sticky connections**

Click **Save**



Load Balancing	
Load Balancing	<input checked="" type="checkbox"/> <b>Use sticky connections</b> Successive connections will be redirected to the servers in a round-robin manner with connections from the same source being sent to the same web server. This "sticky connection" will exist as long as there are states that refer to this connection. Once the states expire, so will the sticky connection. Further connections from that host will be redirected to the next web server in the round robin.
<input type="button" value="Save"/>	

When enabled, sticky connections instruct wXa to use the same WAN interface for all connections between a local and remote IP address. Since load balancing is no longer used once a session is established to a remote server, browsing performance may decrease.

**Method 2.** A second alternative for addressing this issue is to define a failover pool (see [Configuring Failover Pool](#)) and then create a firewall rule (see [Failover and Firewall Rules](#)) specific for the destination IP address which uses the failover pool instead of load balancing (see [Load Balancing](#)). This second method allows for better bandwidth optimization while only limiting bandwidth to specific sites.

The first method is simpler but potentially limits bandwidth to all websites while the second method is more difficult to maintain but gives better overall performance.

---

## 19.3 Load Balancing and the Proxy Server

As with failover, the proxy web services are not compatible with multi-WAN configurations. However, as described in [Failover and Proxy Web Services](#), proxy services can be made to work with load balancing if the proper conditions are met. Enable Load balancing in the Web Administrator at **Services > Proxy Server > Compression**. See [Failover and Proxy Web Services](#) for details.

## 20 Power-On/Off Procedures

It takes RedPort wXa about 3 minutes to become fully operational after power has been applied. Note that the **Web Administrator** is available long before the system is fully operational. Administrators should wait until the system is fully operational before they start making changes to the settings. The status of the unit is displayed on the **System Overview** page for the **Web Administrator**. A run status of operational means the unit is ready.

<b>Run Status</b>	Operational
-------------------	-------------

As stated previously in this document, wXa contains an internal solid state disk (except the wXa-202 which is used to store its configuration, logs, and cached web pages. Care must be taken when turning off the unit. Pulling the plug on a mounted file system will cause the machine to shutdown with the file system on the disk in an inconsistent state. Under normal conditions, pulling the plug does not adversely affect the file disk, however, the system must go through a lengthy file system check and rebuild before the disk can be mounted and normal operations resumed.

When powering off the unit care should be taken to follow the correct procedure.

### To shutdown the system:

1. Login to the **Web Administrator**
2. Go to **Diagnostics**
3. Select **Halt System**

#### Diagnostics: Halt system

Are you sure you want to halt the system?

Yes

No

4. Click **Yes** and wait a full minute before removing power

#### Diagnostics: Halt system



The system is halting now. This may take one minute.

5. The unit does not have a power switch; Pull the power plug to turn it off

**To start up the system:**

1. Apply power to the unit to start it up
2. Wait a few minutes for the unit to become fully operational

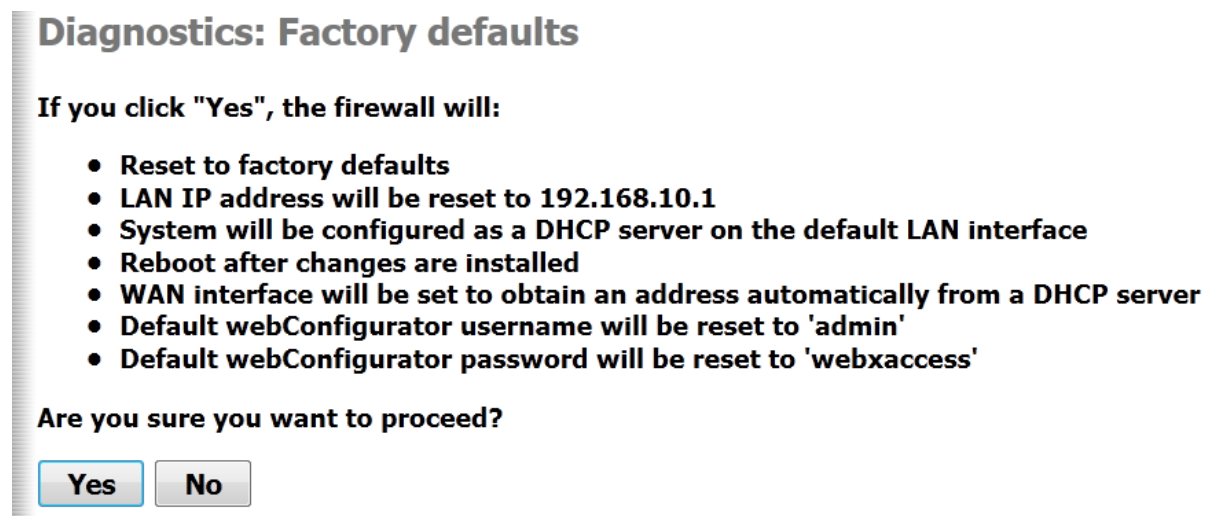
RedPort wXa can be powered by any DC source between 9 - 18V

## 21 Resetting to Factory Defaults

RedPort wXa factory default configuration can be set using one of the two methods described below.

### Method 1:

1. Login to the **Web Administrator**
2. Go to **Diagnostics->Factory defaults**



3. Select **Yes** to proceed
4. Once the defaults are set the unit will reboot to make them effective
5. When you next login to the **Web Administrator** you will be guided through a simple setup procedure

### Method 2:

1. Connect to your system using a Console Window (See [Appendix B: Opening a Console Window](#))
2. Choose Option 4 from the console menu

```
*** Welcome to webXaccelerator 1.2.3.23x-RELEASE on webxaccelerator ***

LAN*          ->  r10      ->  192.168.10.1
WAN*          ->  r11      ->  192.168.1.105 (DHCP)
OPT2 (VOIP) * ->  em0      ->  192.168.77.1
OPT1 (WAN2)   ->  re0      ->  NONE

webXaccelerator console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) webXaccelerator Developer Shell
13) Upgrade from console
14) Disable Secure Shell (sshd)

Enter an option: █
```

3. Once the defaults are set the unit will reboot to make them effective
4. When you next login to the **Web Administrator** you will be guided through a simple setup procedure

## 22 Firmware Upgrade

At times it may be necessary to upgrade the software (firmware) on the wXa. Determine what version of firmware you are currently running using these steps:

1. Login to **Web Administrator**
2. Go to **Status > System** (This is also the default page)
3. Find the software release information in the **Version** section

### System Overview

System information	
Name	webxaccelerator.gmn-usa.com
Version	<b>1.2.3.23x-RELEASE</b> built on Mon Mar 12 22:33:29 UTC 2012

Either the Web Administrator or the system console can be used for Firmware upgrades. Details for each method are included below.

### 22.1 Firmware Upgrade from Web Interface

To access the firmware update screen:

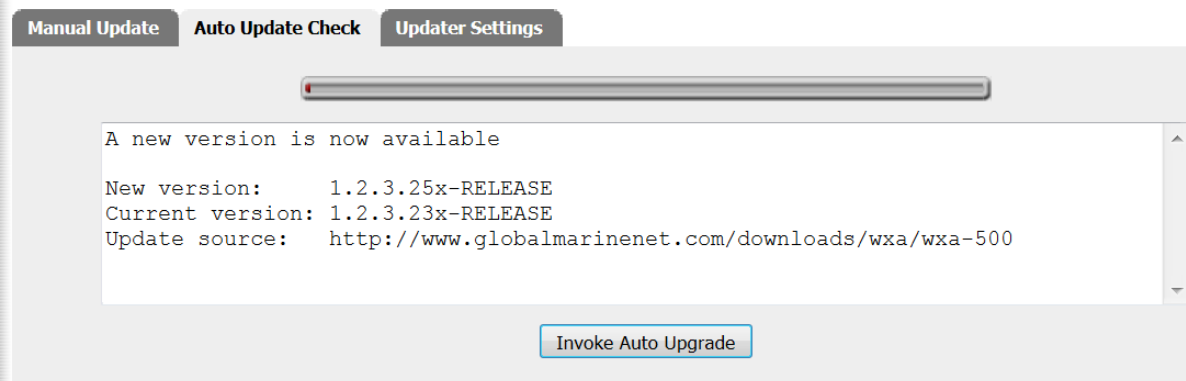
1. Login to the **Web Administrator**
2. Select **System->Firmware**
3. On the tabs, choose between **Manual Update** or **Auto Update**

#### 22.1.1 Auto Update

**Auto Update** is the simplest method to use for updating the firmware. When you select the **Auto Update** tab, the system will open the **Auto Update Check** window that causes the RedPort wXa to check its version of the firmware against the latest on the GMN servers. If there is a newer version on the server than what is currently installed on your system, an option to

invoke an upgrade is given.

## System: Firmware: Auto Upgrade



Click the **Invoke Auto Update** to download and install the latest image over the internet

**Note:** It takes about 15 minutes for the software update to take place. No feedback is provided once the image has been uploaded to the unit. The wXa will eventually reboot with the new version.

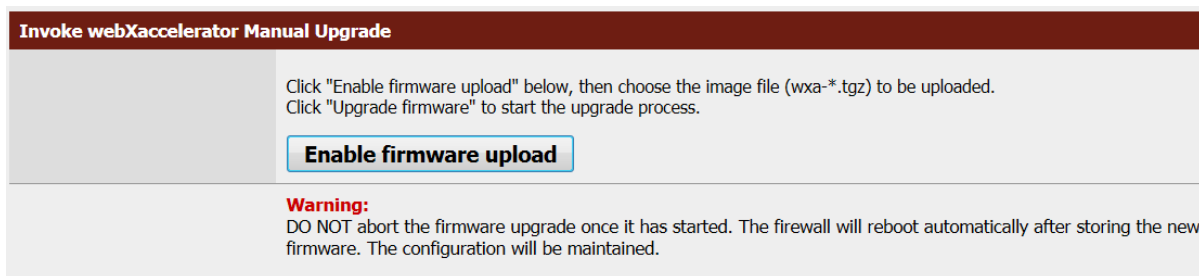
Confirm the upgrade has completed by checking the version number at **Status > System**

## 22.1.2 Manual Update

**Manual update** allows the uploading of firmware image from your local PC.

For a **Manual update**:

1. Download the latest version of the firmware from the wXa documentation and support page at [www.globalmarinenet.com/downloads/wxa](http://www.globalmarinenet.com/downloads/wxa). Select the folder for your wXa model where you will find the latest firmware image named `latest.tgz`. The `ChangeLog.txt` file in the same folder lists the latest version number and the changes made between different versions. Download the `latest.tgz` file to your local system.
2. On the **Web Administrator Manual update** page, click **Enable firmware upload**



3. Click **Browse...** to locate your downloaded `latest.tgz` file

**Invoke webXaccelerator Manual Upgrade**

Click "Enable firmware upload" below, then choose the image file (wxa-\*.tgz) to be uploaded.  
Click "Upgrade firmware" to start the upgrade process.

**Disable firmware upload**

Firmware image file:

**NOTE:** You must upload a .tgz image, not an uncompressed image!

**Upgrade firmware**

**Warning:**  
DO NOT abort the firmware upgrade once it has started. The firewall will reboot automatically after storing the new firmware. The configuration will be maintained.

- Click **Upgrade firmware** to continue or **Disable firmware upload** to cancel

## 22.2 Firmware Upgrade from Console

Upgrading from the console provides more feedback on the progress of the update. Access to the console is required before the firmware can be updated using this method. (See [Appendix B: Opening a Console Window](#))

From the console menu select option 13 to update the firmware.

```
webXaccelerator console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) webXaccelerator Developer Shell
13) Upgrade from console
14) Disable Secure Shell (sshd)

Enter an option: █
```

The following menu is displayed:



```
Starting the webXaccelerator console firmware update system.....

1) Update from a URL
2) Update from a local file
3) Update from USB drive
4) Restore original factory image
5) Create clone/backup image to USB drive
Q) Quit

Please select an option to continue: █
```

Choose menu item **1**, **2** or **3** to update your firmware:

1. Upgrade the system over a live Internet connection. Note that the firmware file is approximately 100Mbytes that could be costly over expensive satellite links. To upgrade to the latest version of the firmware enter the following URL when prompted:

<http://www.globalmarinenet.com/downloads/wxa/<your model>/latest.tgz>

replacing **<your model>** with one of the following values:

**wxa-100, wxa-200, wxa-300, wxa-400, or wxa-500**

Click **Enter** to continue with upgrade.

2. Download the latest version of the firmware from the wXa documentation and support page at [www.globalmarinenet.com/downloads/wxa](http://www.globalmarinenet.com/downloads/wxa). Select the folder for your wXa model where you will find the latest firmware image named `latest.tgz`. The `ChangeLog.txt` file in the same folder lists the latest version number and the changes made between different versions. Download the `latest.tgz` file to your local system. Enter the complete path to the downloaded file when prompted.
3. **Update from USB drive** might be used as an alternative when upgrading systems that are only connected via a satellite link. First download the latest image (see number 2 above) onto a MSDOS (FAT32) formatted USB thumb drive using a land-based Internet connection. Then plug the USB drive into one of the 2 USB ports on the back of the unit. After selecting menu item 3, enter the name of the firmware file to load without a path (e.g. `latest.tgz`). Follow the prompts to complete the installation.

## Appendix A: Resources and Quick Start Guide

---

### DVD Resource

wXa is distributed with a resource CD which contains the following:

- This user guide
- Quick Start guide
- Documentation for main board and a copy of the BIOS
- Supporting software manuals
- Captive portal supporting files and images
- Software Tools
- wXa SSD images

---

## Quick Start Guide for wXa

Congratulations on the purchase of your wXa appliance. With wXa you will increase satellite data transfer efficiency and decrease airtime costs while preventing unwanted costly transmissions. We are confident that wXa will serve you well.

The following information will get you up and running quickly. Please refer to the wXa user guide (on the DVD included with your purchase) for additional information.

### **Port Definitions**

ETH0 is configured as the LAN port with IP address 192.168.10.1.

ETH1 is configured as WAN with DHCP and should be connected to your primary satellite unit.

ETH2 is configured as WAN2 with DHCP and should be connected to your backup satellite unit.

WLAN is configured as the Wi-Fi port (on units with Wi-Fi) with IP address 192.168.20.1.

### **Wi-Fi Hotspot**

Protocol: 802.11g (a and b are disabled by default)

Security: WPA2 (WPA and WEP disabled by default)

SSID: wXa

Secret: wXa

Wi-Fi IP: 192.168.20.1

### **Router Administration Web Page**

IP: 192.168.10.1 - Use a web browser and URL <http://192.168.10.1> on the LAN port or via Wi-Fi.

user: admin

password: webxaccess

### **Configuring WAN and WAN2 Ports**

Both the primary (WAN) and backup (WAN2) ports are configured with DHCP by default. Use the following to configure for use with static IP addressing.

1. Login to the router administration web page
2. Go to **Interfaces->WAN**
3. Set the Type to **Static** (currently DHCP)
4. Enter the IP address for the WAN port and the Gateway then click **Save**.
5. Go to **System->General** and enter the DNS servers in the appropriate boxes
6. Uncheck **Allow DNS server list to be overridden by DHCP/PPP on WAN** and click **Save**

### **Web Compression**

Web compression is disabled by default. The following steps are required to enable compression.

1. Contact your supplier for a wXa account username and password.
2. Login to the router administration web page
3. Go to **Services->Proxy server**
4. Click on **Upstream Proxy**, enable it and enter the information below:

Hostname: xweb.gmn-usa.com

Username: Assigned by your supplier

Password: Assigned by your supplier

Compression level: More compression accelerates the connection sacrificing picture quality

5. Test the compression by viewing an internet website

## **Captive Portal**

The captive portal is disabled by default. The following steps are required to enable it.

1. Login to the router administration web page
2. Go to **Firewall->Traffic shaper** and enable it
3. Go to **Services->Captive portal** and enable it

You will now be taken to a login page every time you try to access the Internet with a web browser. Access to the Internet will be restricted unless a valid pincode is entered. Contact your supplier for pincodes.

## **Captive Portal Wi-Fi Considerations**

Once the captive portal is enabled, access to the **Web Administrator** at <http://192.168.10.1> is lost unless you enter a pincode. The following enables access to the router administration web page without having to enter a pincode.

1. Login to the router administration web page
2. Go to **Services->Captive portal**
3. Click on **Allowed IP addresses**
4. Click on **+** to add a **To** rule for 192.168.10.1, then select **Save**

## **Firewall Considerations**

By default, both WAN and WAN2 are configured to be "Open" allowing unrestricted traffic originating on the Internet. LAN and WLAN (the Wi-Fi interface) are also configured "Open" allowing all traffic to pass through the router onto the Internet. Access rules for all network interfaces should be modified to meet the operational environment. Firewall rules are defined on the router administration web page under **Firewall->Rules**. Click on the tab for the interface that you want to configure. Then add/remove rules to suit your specific environment.

## **Console**

The supplied NULL modem cable can be used to gain console access through the serial port using settings 9600 8N1.

## **Backup/Restore**

On the router administration web page, select **Diagnostics->Backup/Restore** to save a copy of your router's settings.

## **Boot/Halt**

The wXa uses an internal solid-state silicon disk drive (SSD) to store its configuration and cache webpages. Care should be taken when shutting down the unit to prevent loss of data and lengthy disk checks on startup. To properly shutdown the unit, login to the **Web Administrator** and select **Diagnostics->Halt**. Wait one full minute before removing power.

## **In the Box**

The following items are included in every wXa shipment (except the wXa-102):

- ⌘ Base unit. Either rack or wall mount base unit
- ⌘ Wi-Fi antenna for Wi-Fi enabled units
- ⌘ DB-9 NULL modem cable
- ⌘ US or EU compatible external power supply
- ⌘ Resource DVD
- ⌘ This Quick Start guide.

v 1.04



## Appendix B: Opening a Console Window

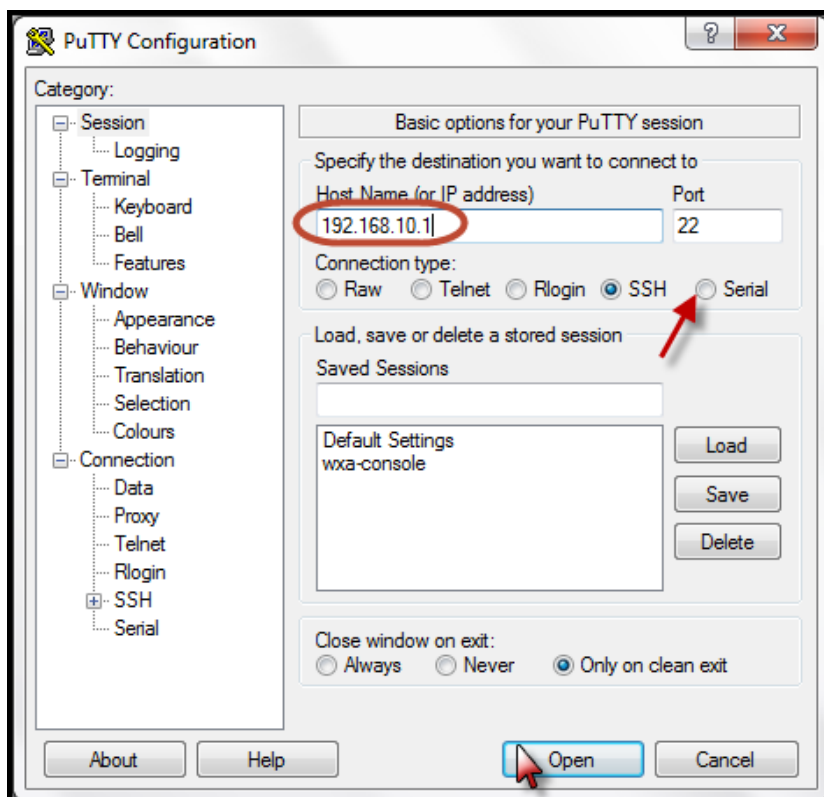
The RedPort wXa system console can be accessed either via the serial console or via a network connection using a Secure Shell Client (SSH) such as putty.exe.

### Console Access via Serial Connection

To access the serial console connect a DB9 NULL Modem cable (provided with the unit) into the serial port on the wXa. Connect one end of the DB9 into the unit and the other into a PC. A generic USB to serial adapter can be used for systems that do not have built-in serial ports.

Opening a console window will require terminal emulator software on your laptop or PC. Various terminal emulators are included on the CD to facilitate access to the console via a serial port. Check the "Tools" folder on the DVD included with wXa.

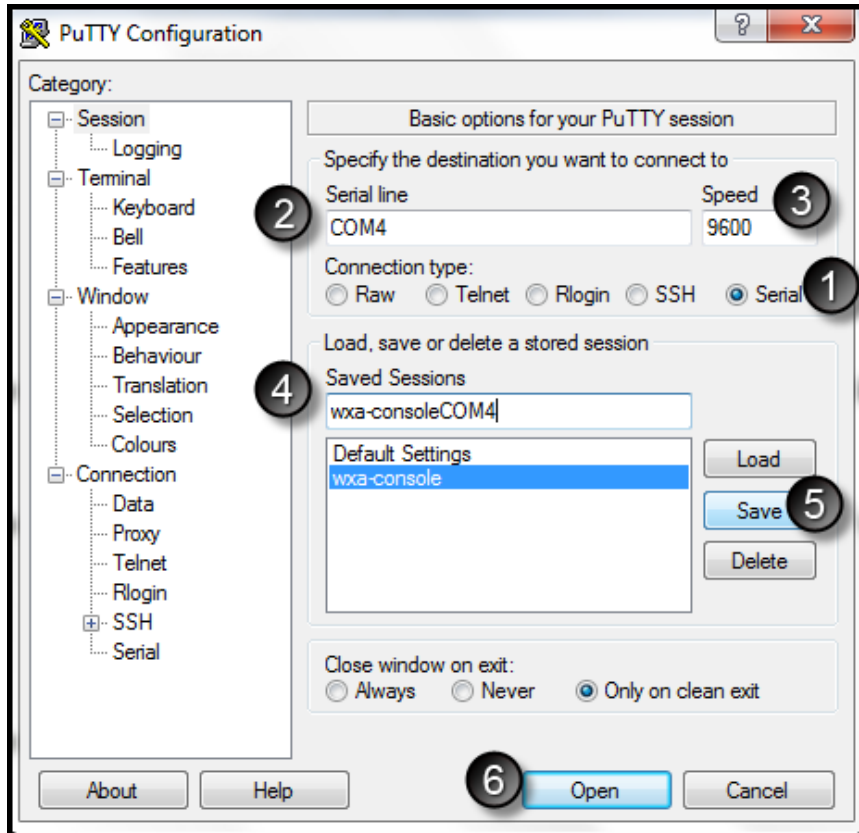
The screenshots below use long-time industry favorite terminal emulator PuTTY.



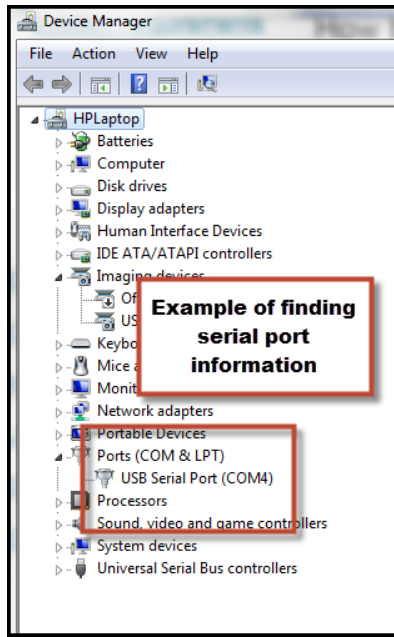
Enter IP address **192.168.10.1** in the highlighted field and then select the **Serial** button.

**Note:** IP address 192.168.10.1 is the default IP address for the wXa LAN port.

A configuration screen will appear similar to the one below. Numbered items are described to help in setting up the console for future use.



1. Verify that the **Serial** button is selected
2. Select the serial line of your PC that is connected to the RedPort VoIP system. Find this information by locating the Device Manager/port information on your PC. In this example, COM4 is used for the connection.



3. Enter **9600** for the **Speed** (Baud Rate).
4. In the **Saved Sessions** field, enter a name for your connection.
5. Click the **Save** button.
6. Click the **Open** button.

For future connections, click on your saved session name and then click **Load** and **Open**.

The console window opens.

**Note:** Press enter if you do not see a menu similar to the screenshot below.



```
*** Welcome to webXaccelerator 1.2.3.23x-RELEASE on webxaccelerator ***

LAN*          ->  rl0          ->  192.168.10.1
WAN*          ->  rl1          ->  192.168.1.105 (DHCP)
OPT2 (VOIP) * ->  em0          ->  192.168.77.1
OPT1 (WAN2) * ->  re0          ->  NONE

webXaccelerator console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) webXaccelerator Developer Shell
13) Upgrade from console
14) Disable Secure Shell (sshd)

Enter an option: █
```

Options on the **Console Menu** can be used to **Halt** and **Reboot** the system, **Reset to factory defaults**, and **Set LAN IP address** should you ever need to do so.

## Console Access via SSH Client

RedPort wXa's console can be accessed over a LAN connection using a Secure Shell Client (SSH). wXa must have been previously configured and in full operating mode before SSH can be used to access the console.

### Console access from Mac, Linux, and UNIX systems

To access the console from an Apple Mac or a system running Linux/Unix:

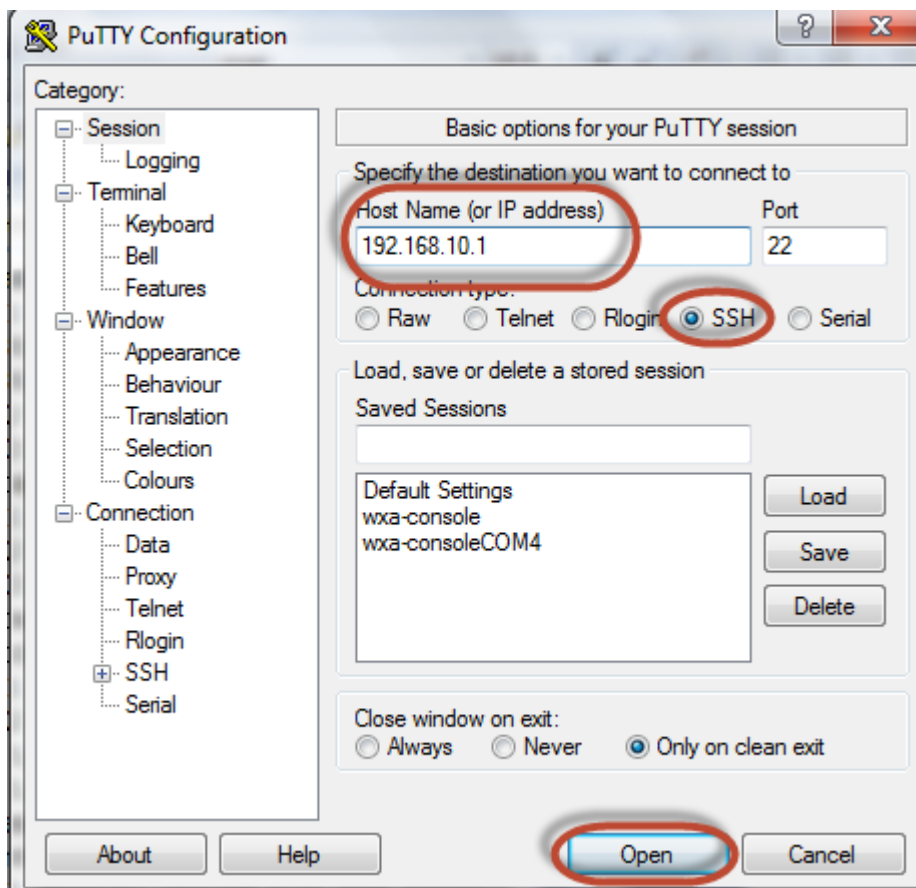
1. Open a terminal window
2. Enter the following command into the terminal window: **ssh -l admin 192.168.10.1**  
where <192.168.10.1> is the **IP address** of the wXa on the local LAN. Note that the IP address may be different for your installation.

## Console access from Windows

Under Windows OS a 3rd party SSH client such as PuTTY must be used. A copy of PuTTY is included on the wXa DVD resource disk. Either download or copy putty.exe onto the windows desktop to install. Putty is a stand-alone executable that does not require an installer.

Double click on the **PuTTY** icon and complete the following:

1. Enter the **<IP address of the wXa router>** (default address is 192.168.10.1)
2. Verify the **SSH** button is selected
3. Click **Open**



You will then be prompted for the wXa administrator username and password:

```
Username: admin
Password: webxaccess
```