



Optimizer

ADVANCED USER GUIDE

FOR MODELS: WXA-203 AND WXA-213

Revision History

Doc Rev	Date	Name	Changes Made
2.0	08JAN2021	Kyle Tuczynski	Issued as version 2.0
2.1.0	19JAN2021	Bethany Headrick	Issued as version 2.1.0

Table of Contents

1.	ABOUT THIS GUIDE	4
2.	INTRODUCTION TO THE REDPORT OPTIMIZER	5
2.1.	OPTIMIZER KEY FEATURES.....	6
2.2.	SERVICES INCLUDED	7
2.3.	PREMIUM SERVICES AVAILABLE.....	7
3.	SAFETY.....	8
4.	THINGS TO KNOW BEFORE GETTING STARTED.....	9
4.1.	MORE THAN JUST A ROUTER	9
4.2.	DESIGNED USE OF THE OPTIMIZER	9
4.2.1.	<i>Single User Environment</i>	9
4.2.2.	<i>Multi-User Environment</i>	10
4.3.	HOW IT WORKS OUT OF THE BOX.....	10
4.4.	DESIGNED USE OF THE OPTIMIZER	ERROR! BOOKMARK NOT DEFINED.
5.	GETTING STARTED – USER INTERFACE (UI) ACCESS.....	12
5.1.	ACCESS THE PORTAL DASHBOARD	12
5.1.1.	<i>Login - Onsite Administrator (Admin)</i>	13
5.1.2.	<i>Installer/Network Administrator Login (Superadmin)</i>	14
5.2.	HOW TO USE WITH DEFAULT SETUP	16
5.2.1.	<i>Email and Web Browsing</i>	16
5.2.2.	<i>Voice Calls</i>	17
5.2.3.	<i>SMS Messaging</i>	17
5.3.	ROUTER SECURITY	17
5.3.1.	<i>How to Secure Your Router</i>	18
6.	SERVICES	19
6.1.	WEB COMPRESSION AND FILTERING.....	19
6.1.1.	<i>Settings</i>	19
6.1.2.	<i>Filters</i>	23
6.2.1.	<i>Web Settings</i>	24
6.2.2.	<i>Configure SIP Extensions to Receive SMS Messages</i>	25
6.2.3.	<i>Settings</i>	26
6.2.4.	<i>SMS Management</i>	27
6.3.1.	<i>Voice PBX Settings</i>	29
6.3.2.	<i>SIP Extensions</i>	30
6.3.3.	<i>How to Make and Receive Voice Calls</i>	31
6.3.4.	<i>FleetBroadband Monitor (FBB)</i>	32
6.4.1.	<i>Configure Optimizer for use with the Halo Wi-Fi Extender</i>	33
6.4.2.	<i>Route Network Traffic through the Halo Wi-Fi Extender</i>	36
6.4.3.	<i>Manage Halo Firewall</i>	37
6.4.4.	<i>Disconnect from the Halo Wi-Fi</i>	38
6.5.1.	<i>Tracking powered by RedPort</i>	39
6.5.2.	<i>SMS Tracking</i>	40
6.6.1.	<i>GPS/NMEA Repeater Equipment Setup</i>	42

7.	STATUS	48
8.	SYSTEM.....	50
9.	NETWORK.....	57
9.2.1.	<i>GSM Configuration in Optimizer</i>	58
9.2.2.	<i>Using GSM</i>	61
9.2.3.	<i>Changing from GSM Service to Satellite Service</i>	62
9.5.2.	<i>Add a Firewall Zone</i>	69
9.5.3.	<i>Port Forwards</i>	71
9.5.4.	<i>Firewall Rules</i>	72
9.5.5.	<i>IP Sets</i>	76
9.5.6.	<i>Allow WhatsApp Configuration</i>	77
10.	STATISTICS.....	81
10.1.	GRAPHS.....	81
11.	PRODUCT WARRANTY AND SUPPORT INFORMATION.....	83
11.1.	PRODUCT WARRANTY INFORMATION	83
11.2.	PRODUCT SUPPORT INFORMATION	84

1. About this Guide

This guide is intended for users of the RedPort Optimizer wXa-203 and wXa-213 routers. It features only those sections of the user interface that require configuration for a specific service or may need to be accessed by the average user.

The following chapter references will help you in administering the most-used features of the Optimizer:

Chapter 4 Getting Started

Chapter 5.4 Halo Wi-Fi Extender

Chapter 7.1 Change the Router Admin Password

Chapter 7.3 Update Firmware

Chapter 7.4 Reboot the Router

Chapter 8.3 Restrict Wireless Network (Add or Change Network Password)

Chapter 8.4 Rename the Wireless Network (Change SSID Name)

Other useful information can be found in the following chapters:

Chapter 5.5 GPS Tracking Service

Chapter 5.6 GPS/NMEA Repeater Settings

Chapter 5.7 Remote Support

Chapter 8.2 GSM Capability

Chapter 8.5 Firewall

Chapter 10 Corporate Contact Information

2. Introduction to the RedPort Optimizer

RedPort, 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.

Ship to shore network management solutions are sold by Pivotel under the RedPort brand name at redportglobal.com and as white-label solutions for the world's premier satellite data service providers.

Optimizer is a satellite Wi-Fi router that combines a powerful satellite data router with voice capabilities, including a full PBX. It is more than just a voice device. It gives you everything you need to create a local voice and data network with your satellite device. You can manage your usage, protect against accidental airtime usage, accelerate your data speeds, enable web compression, track your location via GPS, and provide routing, filtering and security.

2.1. Optimizer Key Features

Designed specifically for use with satellite phones and satellite terminals:

- Replaces a standard router that is typically added to any satellite broadband installation.
- Powerful firewall accommodates any common installation scenario, with features including block or allow any range of port, IP address and protocols.
- Proxy Server enables HTTP filtering: whitelist/blacklist of URL's, domains, and rudimentary content filtering.
- Logging/Reporting to keep track of usage.
- Wi-Fi hotspot makes setup and use easy for crew with compatible computers and tablets.
- Supports Shared Web Compression.
- GSM Compatibility with optional GSM modem and your own SIM card.
- GPS NMEA Repeater reads the built-in GPS in any satellite broadband terminal and rebroadcasts via Wi-Fi.
- Supports voice calling and SMS messages using smartphones connected to the local network.
- Compatible with any IP-based satellite phone and satellite broadband terminal.
- Powerful firewall stops all unwanted data traffic. Optimizer blocks all traffic except XGate-compressed email, web and weather data.
- Works with XGate for email, web, weather and social media services.
- GSM support to switch between satellite and GSM when available.
- Track GPS locations from compatible GPS-enabled devices.
- Compatible with optional RedPort Halo Wi-Fi Extender for access to external Wi-Fi networks, when available.

NOTE: XGate service and Tracking service are not included with the Optimizer and must be purchased separately. Contact your satellite service provider for details.

2.2. Services Included

Voice PBX - allows smartphones to send/receive calls to others on the local area network for free, or over the satellite link at standard satellite airtime rates. Requires a supported satellite terminal.

SMS Messaging - allows smartphones to send SMS messages to others on the local area network for free, or over the satellite link at standard satellite airtime rates. Requires a supported satellite terminal.

GPS NMEA Repeater – allows other devices onboard/on-site to read your GPS location. For example, a navigation program running on an iPad could be used on your boat, or you could get weather information tailored to your location.

GSM Compatibility - allows Internet connectivity via your GSM modem or cell phone with your own SIM card.

File Sharing - Network Shares allows the sharing of files among Windows and Mac computers via Wi-Fi, without the requirement of a wired local network of computers.

2.3. Premium Services Available

The following additional services are available. Contact your RedPort dealer to purchase.

Shared Web Compression – routes all web traffic through a proxy service that works with an onshore server to deliver 3-5 times average web compression, along with virus detection and ad blocking.

GPS Tracking - Using a GPS-enabled device, submit position reports to a central database for viewing on the tracking website.

RedPort VoIP Service - Transform your satellite device into a multi-user unit. Up to four users can send/receive phone calls and/or SMS (text) messages simultaneously. Experience significant price reduction in outbound calls when using VoIP in lieu of standard satellite airtime rates. Requires a supported satellite terminal.

3. Safety



Shock Hazard

The Optimizer is a sealed device and is not meant to be opened for repair in the field by operators or technicians. The enclosure must remain in place at all times on the router to maintain the warranty terms. Make sure the system is correctly grounded and power is off when installing, configuring and connecting components.



Passive POE Port(s)

The Optimizer has a SAT (WAN) and LAN port that are Passive POE. Connecting any device such as a laptop or switch with a Gigabit ethernet, 1000Mbps speed NIC will cause your device or port, at the minimum, damage or burn out. RedPort does provide coverage or warranty for this damage. Connect any device of this nature at your own risk.



Proposition 65

This product can expose you to Acrylonitrile, which is known to the State of California to cause cancer. For more information go to www.P65Warnings.ca.gov.

4. Things to Know Before Getting Started

As the onboard/onsite administrator, under normal operating conditions, you will seldom have a need to interact with the user interface of the router. However, should you find yourself in a position that requires you to login to the router, this Guide is designed to help you.



4.1. More Than Just A Router

The Optimizer is more than just a router. It has some enhanced proxy services in addition to basic routing capabilities.

Proxy Server(s) - when Transparent proxy is enabled, all traffic on port 80 (http port) is redirected through the internal proxy server. This allows URL and DNS filtering (whitelist and blacklist sites), some content filtering (i.e. remove flash video) and you can turn on http logging to see what URLs are

Firewall - A full-featured firewall is included. Block or allow IP address/ranges, port ranges, different protocols. Rules can be applied to any path in and out of the router.

4.2. Designed Use of the Optimizer

This router is suitable for two distinctly different audiences:

4.2.1. Single User Environment

For the single user that wants the convenience of BYOD (bring your own device) for email, web browsing, SMS and phone calls. All that is required is a RedPort-certified compression email account like XGate and/or compression web-browsing service like XWeb. By adding the XGate Phone app, a smartphone can be used to place and receive voice calls and/or SMS messages over the satellite network. With the optional RedPort VoIP service, the costs of those voice calls can be kept to a minimum

4.2.2. Multi-User Environment

This is a single-user router that can be configured for use in a multi-user environment. The idea is that you, as the installer or network administrator, will configure the router, using these guidelines, before installing it at its ultimate destination.

Once installed, the onsite administrator will log in and land on the Home page. The Home page has the common tasks that will be used locally just as creating and managing crew accounts.

The onsite administrator does not have access to the full user interface and therefore does not have the ability to re-configure the router. There is a separate user guide for the onsite administrator: Optimizer Onsite Administrator Guide.

4.3. How It Works Out of the Box

We ship the router ready for use with a RedPort-certified compression email and/or web browsing account.

This default setup allows anyone with a RedPort-certified email or web account (with a Primary Account username and password) to use the router, as is, to send and receive email and to browse the Internet.

This out-of-the-box configuration works well for single broadband users.

This configuration is also suitable for the multi-user environment where each person has a separate primary email and/or web browsing account. While you have the benefit of email and web compression on each primary account, all users have unlimited access to the Internet.

If you are in a multi-user environment, we recommend enabling Transparent proxy. With Transparent Proxy enabled, all traffic on port 80 (http port) is redirected through the internal proxy server. This allows URL and DNS filtering (whitelist and blacklist sites), some content filtering (i.e. remove flash video) and you can turn on http logging to see what URLs are being accessed by the users. You also have the option to communicate upstream to a compression proxy server. For savings on voice calls consider RedPort VoIP service. You may realize further savings by enabling shared web compression (see Section 5.1).

Best Practice is to have a knowledgeable technician (someone who knows about proxy servers and routers) go through and generate a custom configuration. In a fleet environment, this custom configuration can be recorded and used on other Optimizer routers within the organization.

4.4. Navigating the User Interface

Access to the UI depends upon how you login to the router. There are two logins available: admin and superadmin.

The user interface is divided into sections; use the tabs to access the required service or information.

On most pages in the user interface you will see three buttons in the lower right corner:



Reset: Returns the page to its previous saved state.

Save: Saves the changes but does not yet apply the changes.

Save & Apply: Saves the changes and applies them to the router configuration. In some cases, the router must reboot to apply the change. If reboot is required, it will be noted on the page.

5. Getting Started – User Interface (UI) Access

In a typical situation, the Optimizer router arrives to you with the following services enabled:

- Closed Firewall allowing email and web access via RedPort-certified services only.
- GPS/NMEA Repeater.

There are also services available that are disabled:

- Internal Transparent Proxy for Web Filtering.
- SMS for compatible satellite devices.
- Voice Capability for compatible satellite devices.
- Web Compression (additional fees may apply).
- GPS Tracking (additional fees may apply).
- RedPort VoIP for multi-user calls and SMS (additional fees may apply).

5.1. Access the Portal Dashboard

To access the router's Dashboard, you must login to the router. This can be accomplished in several ways however the most popular method is to:

1. Connect to the Wi-Fi Hotspot created by the router using a PC. Connect to the Wi-Fi Hotspot just like you would any other Wi-Fi connection: On a Windows PC, go to: Windows Start > Control Panel > Network Connections.

On a MAC, go to: Apple > System Preferences > Network.

The Network Name will look something like: 'wXa-203-XXXX' where 'XXXX' is the last four digits of the Optimizer's Mac address.

2. Open any web browser on the computer and enter the URL: <http://192.168.10.1>

The next sub-section outlines the login process. The Optimizer ships with two existing accounts:

- **Admin** - for normal day-to-day operation.
- **Superadmin** - for configuration and maintenance.

5.1.1. Login - Onsite Administrator (Admin)

Onsite Admin Default User Credentials:

Username: admin

Password: webxaccess

This login gives the user access to portions of the user interface and the ability to perform common tasks such as:

- Monitor the system status.
- Reboot the router, if necessary.
- Change the router password for the admin account, if necessary.

5.1.2. Installer/Network Administrator Login (Superadmin)

Installer/Network Administrator Default User Credentials:

Username: superadmin

Password: webxaccess

This login provides full access to the user interface for configuration and maintenance of the router. Once logged in, you will see the router's Home page (Super Administrator login shown):

The screenshot shows the Optimizer Home page with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.08 1.02 1.01 | Changes: 0
- Top Navigation:** Home, Services, Status, System, Network, Statistics, Logout
- Left Sidebar:** Tasks
- Main Content:**
 - WiFi Extender Setup:**
 - Step 1: Connect (Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.)
 - Step 2: Enable WiFi Extender (WiFi Extender Status: OFF. Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi Extender first (see Step 1).)
 - Step 3 (Automatic): Disable Firewall (Firewall Status: ON. Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution and only when connected to land based WiFi.)
 - System Status:**
 - System status overview
 - Realtime bandwidth usage over satellite link
 - Historic bandwidth usage over satellite link
 - System message log
 - Local WiFi setup:**
 - SSID and Security: WiFi setup (Change hotspot name and/or add security and set password)
 - System:**
 - Router password
 - Reboot router
- Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

NOTE: The Wi-Fi Extender Setup section only displays when the optional RedPort Halo Wi-Fi Extender is physically connected to the Optimizer and powered ON.

This Home Page is the onsite administrator's gateway to the most used features. From the Home Page you have access to the remaining sections of the user interface.

The screenshot shows the Optimizer Home page with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.09 1.02 1.01 | Changes: 0
- Top Navigation:** Home, Services, Status, System, Network, Statistics, Logout
- Left Sidebar:** Web Compression and Filtering, Settings, Filters, Log, Help
- Main Content:**
 - Web Compression and Filtering:** SMS, GPS Tracking, Remote Access, WiFi Extender, GPS/NMEA Repeater, Voice PBX, FBB Monitor

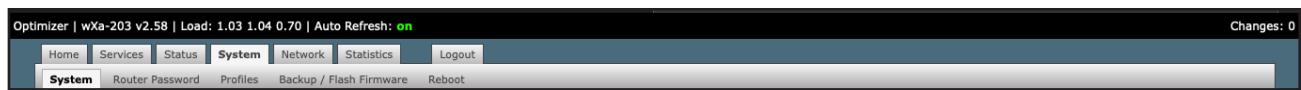
Each service is contained in its own tab under the Services section. This is where you will enable/disable the services and configure them for use.

Status: displays how much memory the router is using, who is connected via Wi-Fi and other information you may find useful.



The System Log contains detailed information of the router's performance. It will report error messages and can be useful when troubleshooting connection issues. Realtime Graphs report how much data is being using by the different interfaces. All Status information is Read Only.

System: contains some of the router's basic settings for you to configure plus a few maintenance functions.



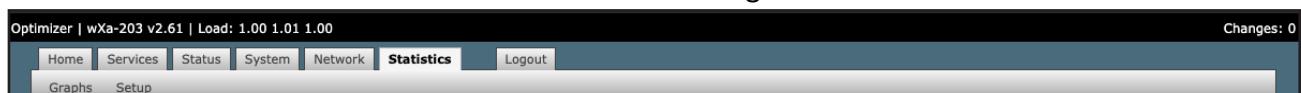
Use this section to set your time zone, change the 'admin' and/or 'superadmin' password, flash new firmware to the router, reboot the router if necessary. Profiles is a way to 'clone' the router configuration for use on another Optimizer router.

Network: contains access to the network interfaces and the firewall.



Use this section to configure network interfaces, run diagnostics, or modify the firewall.

Statistics: contains information about resource usage.



Use the tabs to navigate through the user interface. You will see that the information represented in the user interface can be quite technical. This Guide will cover only those sections of the user interface that require configuration for a specific service or may need to be accessed by the average user.

5.2. How to Use with Default Setup

We ship the router ready for use with Voice and SMS ready to be enabled for use with compatible satellite devices using standard satellite airtime.

This out-of-the-box configuration works well for single broadband users. This configuration is also suitable for the multi-user environment where each person has a separate primary email and/or web browsing account.

While you have the benefit of email and web compression on each primary account, all users have unlimited access to the Internet.

BEST PRACTICE: If you are in a multi-user environment, we recommend enabling Transparent proxy. With Transparent Proxy enabled, all traffic on port 80 (http port) is redirected through the internal proxy server. This allows URL and DNS filtering (whitelist and blacklist sites), some content filtering (i.e. remove flash video) and you can turn on http logging to see what URLs are being accessed by the users. You also have the option to communicate upstream to a compression proxy server. For savings on Voice calls consider RedPort VoIP service. You may realize further savings by enabling shared web compression.

5.2.1. Email and Web Browsing

This default setup allows anyone with a RedPort-certified email account (such as XGate) or web account (such as XWeb), with a Primary Account username and password, to use the router, as is, to send and receive email and to browse the Internet.

Here are the basic instructions:

1. Power the Optimizer ON.
2. Turn your satellite phone ON.
3. Connect the Optimizer to your satphone with the appropriate cable.
4. On your computer, iOS or Android device, connect to the wireless network created by the Optimizer. The name of the wireless network will be something like: wXa-203-xxxx, where xxxx may represent the last four digits of the Mac address of the Optimizer.
5. Once connected to the wireless network, open the RedPort-certified email program (such as XGate) and go to Settings > Connection > and set the Connection Type to “Optimizer xxxxxx” where xxxxxx represents your satphone connection. Click [OK].
6. Wait for a strong satphone signal.
7. Start an email or a web browsing session.

5.2.2. Voice Calls

Voice is disabled by default but can be enabled for use with compatible satellite devices using standard satellite airtime.



CAUTION: When you enable the Voice PBX it is listening on all ports. Without further configuration, this could leave you vulnerable to unwanted traffic.

5.2.3. SMS Messaging

SMS is disabled by default but can be enabled for use with compatible satellite devices using standard satellite airtime.



CAUTION: When you enable the SMS service it is listening on all ports. Without further configuration, this could leave you vulnerable to unwanted traffic.

5.3. Router Security

If you modify the default settings of the firewall you may have WAN ports open.

If you enable the Voice PBX or SMS messaging, all ports are listening.

Any of these changes could leave you vulnerable to unwanted traffic. Note that ports open to the Internet on satellite systems that have public IP addresses are vulnerable to attackers that run dictionaries trying to guess usernames and passwords on the router. These dictionary attacks, at best, can result in large amounts of accounted traffic; and, at worst, they are a security breach that could endanger communications on the vessel. Systems open to the public Internet must take special precautions to secure the router from intrusion.

Web Proxy is not a problem, by default, unless you make changes since the software, by default, only listens to traffic on the LAN.



CAUTION: Before you block the WAN ports, read the next chapter. **Blocking the WAN ports at this stage may lock you out of the router.** We've built in some measures to help minimize that possibility, but please pay special attention when making router configuration modifications.

5.3.1. How to Secure Your Router

First, confirm that the Disable anti-lock rule setting is “Unchecked” in System > System Settings. If it is checked, you want to uncheck it to Enable the anti-lock rule. The anti-lock rule prevents the administrator from inadvertently locking him/herself out of the router when programming firewall rules.

Confirm that in Network > Firewall > Firewall Rules that the first rule “BLOCK WAN” is disabled. If you Enable (check) this rule you will lock yourself OUT of the router, unless the antilock rule is enabled (unchecked). If you lock yourself out of the router you must perform a factory reset.

Confirm that in Services > Web Compression and Filtering > Advanced that Listen Interfaces is set to LAN. Do not change this to WAN unless you desire proxy service through the WAN port. If changing the default configuration to listen on the WAN then firewall rules must be created to allow access to the proxy listen port (port 3128 by default).

Go to System > Router Password and change the router password for both the “superadmin” and the “admin” access.

NOTE: The BLOCK WAN firewall rule, if enabled, will prevent access to these ports.

If Voice PBX is enabled, it is listening on all ports. You can specify the Interface to Listen (such as LAN) in Services > Voice PBX > Settings OR, you can leave it to listening on all interfaces and use a firewall rule to restrict traffic Network > Firewall.

NOTE: The BLOCK WAN firewall rule, if enabled, will prevent access to these ports.

If planning to access the web user interface over the WAN port then create firewall rules with higher precedence than the BLOCK ALL rule that allow traffic from your Internet IP address to the router.

NOTE: Ports 80, 443 and 22 are open, if not disabled.

When you have completed and tested your configuration and are confident that it is working as desired, you can remove the Anti-Lock rule in System > System Settings. Now you can Enable the BLOCK ALL from WAN firewall rule in Network > Firewall > Firewall Rules.

6. Services

6.1. Web Compression and Filtering

This section is used to:

- Configure filters for the internal proxy server when compression is not enabled.
- Enable compression so that traffic is passed to the upstream proxy server.
- Configure filters for the proxy server (internal or upstream).
- View traffic logs.

6.1.1. Settings

The screenshot shows the Optimizer web interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 1.00 | Changes: 0
- Top Navigation:** Home, Services (selected), Status, System, Network, Statistics, Logout
- Sub-Header:** Web Compression and Filtering, SMS, GPS Tracking, Remote Access, WiFi Extender, GPS/NMEA Repeater, Voice PBX, FBB Monitor
- Sub-Header Buttons:** Settings (selected), Filters, Log, Help
- Section Title:** Web Filtering and Compression Proxy Settings
- Description:** Enable and configure web compression and filtering features.
- Compression Tab:** Selected tab. Sub-tabs: General Settings, Advanced.
- Enable compression:** A checkbox with a tooltip explaining the benefits of web compression.
- Username:** Text input field labeled "Enter_Compression_User_Name_Here".
- Password:** Text input field labeled "Enter_Compression_Password_Here" with a password strength meter.
- Bypass Regex Domain:** Text input field with a tooltip explaining how to bypass compression for specific domains.
- Buttons:** Reset, Save, Save & Apply.
- Page Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

6.1.1.1. Compression

By default, the router is shipped with web compression disabled. Web compression is a premium service that carries an additional charge. Contact your service provider for details and pricing.

Enable Compression: If you have purchased Web Compression service, click the checkbox to Enable compression. The page will expand; see With Compression Enabled below.

Username: Enter the Username given to you by your service provider. This username is specific to the compression service.

Password: Enter the Password given to you by your service provider. This password is specific to the compression service.

Bypass Regex Domain: This is the ‘whitelist’ of sites that should not be compressed. To add a site, click the Add icon . Proper syntax must be used to successfully bypass compression. See the Help tab for guidance and examples of using regular expressions.

With Compression Enabled, the page expands to reveal Proxy Authentication by Client, Server, and Compression Level.

Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 1.00 Changes: 0

Home Services Status System Network Statistics Logout

Web Compression and Filtering SMS GPS Tracking Remote Access WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor

Settings Filters Log Help

Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

Compression General Settings Advanced

Enable compression Web compression will, on average, decrease overall bandwidth usage by a factor of 3-5X while simultaneously increasing overall speed. Don't yet have the incredible airtime savings and optimization of web compression? Contact your dealer for additional information. They can set you up with an account username and password to enable compression for this device.

Proxy Authentication by Client Specifies whether upstream proxy authentication requests are passed through to the client browser. If not, authentication (if required) is done by proxy. **Note:** this feature will not work with transparent proxy. When using transparent proxy you must uncheck this option and enter a valid username and password.

Username

Password

Server

Compression Level

Bypass Regex Domain Bypass compression for listed sites. Enter host regular expression to match. e.g. ".google.com" to bypass any domain containing .google.com. See "Domain Syntax" under Help tab for additional information.

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Proxy Authentication by Client: By default this is unchecked as it does not work with the Captive Portal enabled. In this state, unchecked, the upstream proxy server will login on your behalf. If this is checked, then the authentication happens at the user end, which means that when a user goes to any webpage they will be prompted for a username and password.

Server: Do not change this unless instructed to do so by your service provider.

Compression Level: Set the level of compression that meets your needs. Those on entry level plans should click “Maximum”. Those on high data plans may prefer “Standard” or “Minimum”.

6.1.1.2. Compression

These are the general settings for the internal proxy service. You can use the internal proxy server and enable transparent proxy to redirect all http traffic for filtering.

The screenshot shows the Optimizer web interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 1.00 | Changes: 0
- Top Navigation:** Home, Services, Status, System, Network, Statistics, Logout
- Sub-Header:** Web Compression and Filtering, SMS, GPS Tracking, Remote Access, WiFi Extender, GPS/NMEA Repeater, Voice PBX, FBB Monitor
- Current Tab:** Settings, Filters, Log, Help
- Section:** Web Filtering and Compression Proxy Settings
- Description:** Enable and configure web compression and filtering features.
- Sub-section:** Compression, General Settings, Advanced
- Enable Web Proxy:** Enable/Disable web proxy service.
- Transparent Proxy:** Enable Transparent proxy. i.e. transparently redirect HTTP web traffic to the web proxy for filtering and/or compression without having to modify the end user's browser settings.
Caution: Enabling transparent mode requires opening TCP ports 53 (DNS), 80 (HTTP), and 443 (HTTPS) which can (will) result in high traffic usage.
Note: This mode is not compatible with the captive portal. The captive portal, if enabled, will disable this feature automatically to prevent conflicts.
- Buttons:** Reset, Save, Save & Apply
- Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)



CAUTION: Before enabling Transparent Proxy, refer to section titled Router Security.

6.1.1.3. Advanced Settings

Under normal operating conditions there is little to change here.

Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 1.00 Changes: 0

Home Services Status System Network Statistics Logout

Web Compression and Filtering SMS GPS Tracking Remote Access WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor

Settings Filters Log Help

Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

Compression **General Settings** **Advanced**

Filtering

Enable/Disable content filtering.

Default filtering scheme

Light

Filtering makes changes to the webpages to either help with compression or filter content by removing it before loading on the users' page. Filtering schemes are as follows:
Light - Safe for all sites. Most content will remain on page with little modification to the original content.
Moderate - Safe for most sites. Moderate content filtering with removal of some elements.
Aggressive - Reasonable privacy protection with best bandwidth utilization but require some exceptions for trusted sites, most likely because of cookies or SSL.

Listen address

3128

Bind proxy to interface IP address and port number using [ipaddress:port] formatting. Omit IP address to bind to all interfaces.

Listen interfaces

LAN - 192.168.10.1

Bind proxy to the following interfaces

Enforce Blocks

Whether the user is allowed to ignore blocks and can "go there anyway".

Buffer Limit

4096

Maximum size of the buffer for content filtering.

Forwarded Connect Retries

2

How often the Proxy retries if a forwarded connection request fails.

Keep Alive Timeout

300

Number of seconds after which an open connection will no longer be reused.

Socket Timeout

300

Number of seconds after which a socket times out if no data is received.

Log Rotation

weekly

Log rotation schedule.

Debug Level

4096
8192

Key values that determine what information gets logged. 1 = Log the destination for each request the Proxy lets through. 4096 = Startup banner and warnings. 8192 = Non-fatal errors.

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Some items of interest include:

- **Default Filtering Scheme:** impacts the amount of content filtering that is applied to a webpage, by removing elements, before presenting it to the end user. It determines the amount of filtering to be done to the page. “Light” has the least impact and is not recommended for those on low data plans. “Aggressive” has the most impact and is suggested for the best bandwidth utilization. This blocks YouTube, flash, etc.
- **Debug Level:** determine what will show on the Web Compression and Filtering ‘Log’ page. Adding the debug level of “1”, all URLs will be logged and will appear on the Log page, one line per URL.



CAUTION: Utilization of debug level 1 is not recommended for normal operation.
The Log files are kept in RAM and with debug level 1 activated you run the risk of RAM filling up, the Swap Partition filling up and the router will crash.

BEST PRACTICE: Activate debug level 1 for testing that your setup is working as you intend, i.e. the proxy server working as expected, whitelists and blacklists are working. Deactivate debug level 1 when testing is complete.

6.1.2. Filters

By default, you have control over what sites are ALLOWED (whitelist) and what sites are BLOCKED (blacklist) and some control over content filtering without having to enable compression.

The screenshot shows the Optimizer web interface with the 'Filters' tab selected. The 'Filters' section contains three main sections: 'Fragile sites that should not be filtered', 'Sites which should be blocked', and 'Sites which are allowed'. Each section has a text input area and a 'Clear' button. At the bottom right of the filters section are 'Reset' and 'Submit' buttons.

There are three filter categories:

- **Fragile Sites:** list sites that you want the content kept intact without any modification.
- **Sites Blocked:** the blacklist; users are prevented from viewing these sites.

- Sites Allowed:** the whitelist; these sites are allowed for viewing. This list overrides the blocked list.

Filters respond to POSIX Regular Expressions (see section 5.1.4 for details). Example: If you place a slash (/) in Sites Blocked then the entire Internet is blocked (blacklist). Enter the whitelist in the Sites Allowed section. If any of the allowed sites should be accessed without any content filtering, enter that site in the Fragile sites section as well.

6.2. Web Compression

If using a compatible satellite device, it is possible to send and receive SMS messages directly from the Optimizer and to route incoming SMS messages to one or more smartphones connected to the local wireless network. Access to Services > SMS requires the ‘superadmin’ login.

6.2.1. Web Settings

Use Settings to enable and configure the SMS parameters.

Optimizer | wXa-203 v2.61 | Load: 1.00 1.02 0.70 Changes: 0

Home Services Status System Network Statistics Logout

Web Compression and Filtering SMS GPS Tracking Remote Access WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor

Settings Management

sms parameters

configure the parameters for SMS

Enabled	<input checked="" type="checkbox"/>
Interval in seconds between LOCAL send attempts	240
number of days that messages stay in queue when receiving messages	3
Satellite device	Iridium
Check for received messages (in seconds)	360
Configure extensions to receive SMS	Redirect

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

1. Click the checkbox to enable SMS.

Satellite device

✓ Iridium

iSavi

Sailor FBB

Check for received messages (in seconds)

Configure extensions to receive SMS

Redirect

2. Select the appropriate Satellite device from the drop down menu.
3. Click <Save & Apply>.

6.2.2. Configure SIP Extensions to Receive SMS Messages

With SMS enabled, click <Redirect> (see SMS Settings screen above) to go to the Voice PBX Settings page. Click the Extensions tab to configure which extensions are to receive incoming SMS messages.

The screenshot shows the Optimizer web interface with the following details:

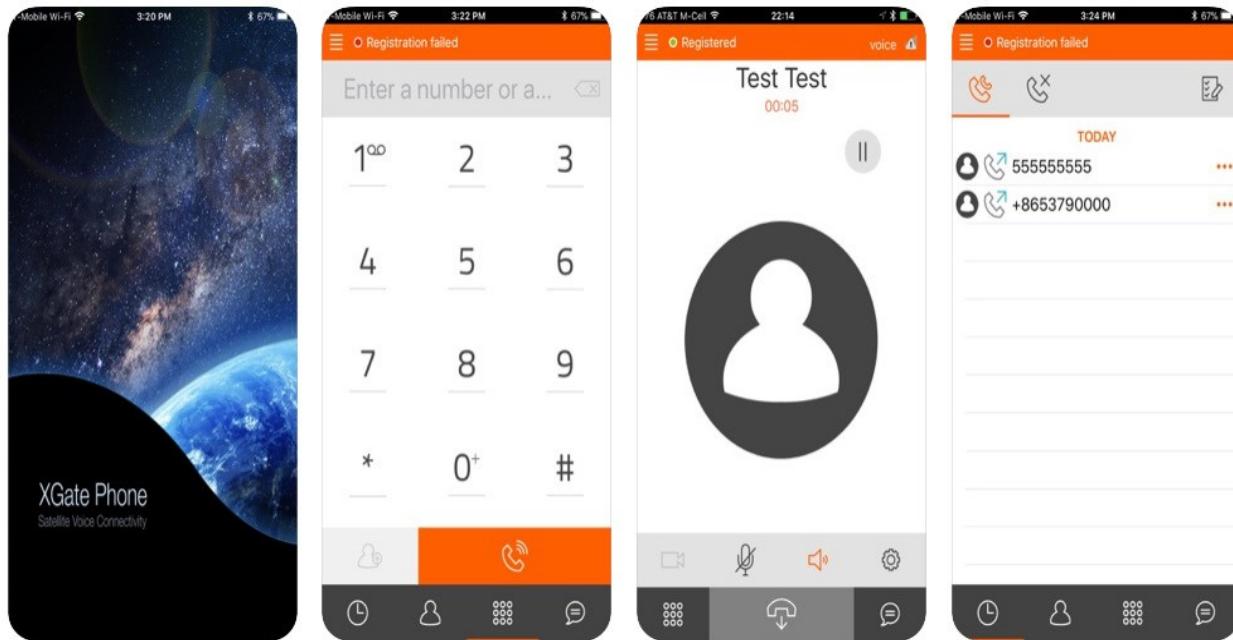
- Header: Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 0.81 | Changes: 0
- Top navigation bar: Home, Services, Status, System, Network, Statistics, Logout, Web Compression and Filtering, SMS, GPS Tracking, Remote Access, WiFi Extender, GPS/NMEA Repeater, **Voice PBX**, FBB Monitor.
- Sub-navigation bar: Settings, **Extensions**, Logs, Sat SIP Trunk, RedPort VoIP.
- Section title: Extensions.
- Table header: SIP Extensions, with columns: Ring, SMS, Extension, Password, Caller ID, Description.
- Table body:

Ring	SMS	Extension	Password	Caller ID	Description
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	201	1234	201	Captain line Value larger than 200 SIP extension password
<input type="checkbox"/>	<input type="checkbox"/>	202	1234	202	Crew line 1
<input type="checkbox"/>	<input type="checkbox"/>	203	1234	203	Crew line 2
<input type="checkbox"/>	<input type="checkbox"/>	204	1234	204	Crew line 3
- Buttons: Add, Reset, Delete (for each row), Save, Save & Apply.
- Footer: Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

To enable an extension to receive SMS messages, use the checkbox in the SMS column.

6.2.3. Settings

To use a smartphone or tablet to send/receive SMS messages requires XGate Phone App installed on the smartphone or tablet. The XGate Phone App can be found in Apple iTunes App Store for iOS devices and the Google Playstore for Android devices. Using the smartphone or tablet Settings, connect to the Optimizer wireless network ‘wXa-213-xxxx’. Open the XGate Phone App. Click <Chat> to send an SMS message or to view an SMS message received.



Only one SMS message can be sent at a time. Standard SMS message rates apply. (Multi-user Voice and SMS is possible with the optional RedPort VoIP service. Contact your service provider for details.)

6.2.4. SMS Management

With SMS enabled you can send SMS messages directly from the Optimizer user interface and you can manage SMS messages that have been sent and received.

Create Message

Destination phone number or email address	202
Enter your SIP extension	201
Message	(Large text area)
<input type="button" value="Send message"/> [Select] <input checked="" type="checkbox"/> Send the text message to the specified number	

Received Messages

Filename	From	Message	Date	Respond	delete	Select
This section contains no values yet						

Sent Messages

Filename	to	Message	Date	Delete	Select
This section contains no values yet					

Remove messages

Select all messages	<input checked="" type="checkbox"/> Select
Delete selected messages	<input type="checkbox"/> Delete Selected
Delete all sent messages	<input type="checkbox"/> Delete All Sent
Delete all received messages	<input type="checkbox"/> Delete All Received
Delete all messages in local queue	<input type="checkbox"/> Delete All Queued

Using the <Select> checkbox you can specify which messages to delete or you can delete all messages.

6.3. Voice PBX

Requires ‘superadmin’ login for configuration.

Users with smartphones can send/receive voice calls and SMS messages over the following satellite communication setups:

- Sailor FBB terminal - requires XGate Phone app*.
- IsatHub iSavi - requires IsatHub Control app and either IsatHub Voice app or XGate Phone app.
- Any satellite terminal with a RJ-11 port - requires XGate Phone app* AND an ATA accessory. Contact your satellite service provider for ATA information.

This configuration allows one voice call or one SMS message at a time and standard satellite voice airtime rates apply.

Multi-Voice capability is available with the optional RedPort VoIP service on virtually any satellite terminal. This VoIP service allows you to make calls for considerably less than standard satellite voice airtime costs and allows up to four users sending/receiving phone calls and/or SMS messages simultaneously. As of this writing, Multi-VoIP is compatible with the following:

- FBB
- BGAN
- VSAT
- RedPort Aurora
- Iridium Pilot
- Thuraya IP
- IsatHub iSavi

The Optimizer allows unlimited SIP extensions with free local calling and text messaging within your local area network using the XGate Phone app*.

*XGate Phone app is available for free in the Apple iTunes App Store and in the Google PlayStore.



Caution: Before enabling the PBX service, read section titled Router Security.

6.3.1. Voice PBX Settings

The Optimizer allows unlimited SIP extensions with free local calling and text messaging within your local area network using the XGate Phone app*.

*XGate Phone app is available for free in the Apple iTunes App Store and in the Google PlayStore.

NOTE: Prior to enabling PBX service, review section How to Secure Your Router. Click the checkbox to Enable the PBX.

When the PBX is enabled it is listening on all ports. This may leave you vulnerable to unwanted traffic. See section titled How to Secure Your Router.

The screenshot shows the Optimizer web interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.35 1.15 1.05 | Changes: 0
- Top Navigation:** Home, Services (selected), Status, System, Network, Statistics, Logout
- Sub-navigation:** Web Compression and Filtering, SMS, GPS Tracking, Remote Access, WiFi Extender, GPS/NMEA Repeater, Voice PBX (selected), FBB Monitor
- Current Tab:** Voice PBX
- Sub-tab:** Settings
- Section:** PBX Services
- Fields:**
 - Enable PBX: Enable/Disable PBX VOIP service.
 - Listen port: Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.
 - Listen interfaces: Bind proxy to the following interfaces
- Buttons:** Reset, Save, Save & Apply
- Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

6.3.2. SIP Extensions

By default, there are 4 extensions enabled. Extension 201 is enabled for inbound and outbound calling. The remaining extensions are enabled but are configured for outbound calling only.

Incoming calls will ring only on those extensions with Ring enabled.

To enable Ring (or SMS) on an extension simply check the box for the service you want enabled.

Ring	SMS	Extension	Password	Caller ID	Description
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	201	1234	201	Captain line <small>Value larger than 200 SIP extension password</small>
<input type="checkbox"/>	<input type="checkbox"/>	202	1234	202	Crew line 1
<input type="checkbox"/>	<input type="checkbox"/>	203	1234	203	Crew line 2
<input type="checkbox"/>	<input type="checkbox"/>	204	1234	204	Crew line 3

Extensions

SIP Extensions

Value larger than 200 SIP extension password

Free text

You may enter a description here for your reference

Add Save Save & Apply

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

When Ring is checked, the smartphone configured with the corresponding Extension will Ring with every incoming call.

When SMS is checked, that smartphone will receive every incoming SMS message.

To use a smartphone to send/receive phone calls requires the XGate Phone app installed on the smartphone. The XGate Phone app can be found in Apple iTunes App Store for iOS devices and the Google Playstore for Android devices.

The smartphone user configures the XGate Phone app with their corresponding SIP Extension.

On this page, you can also:

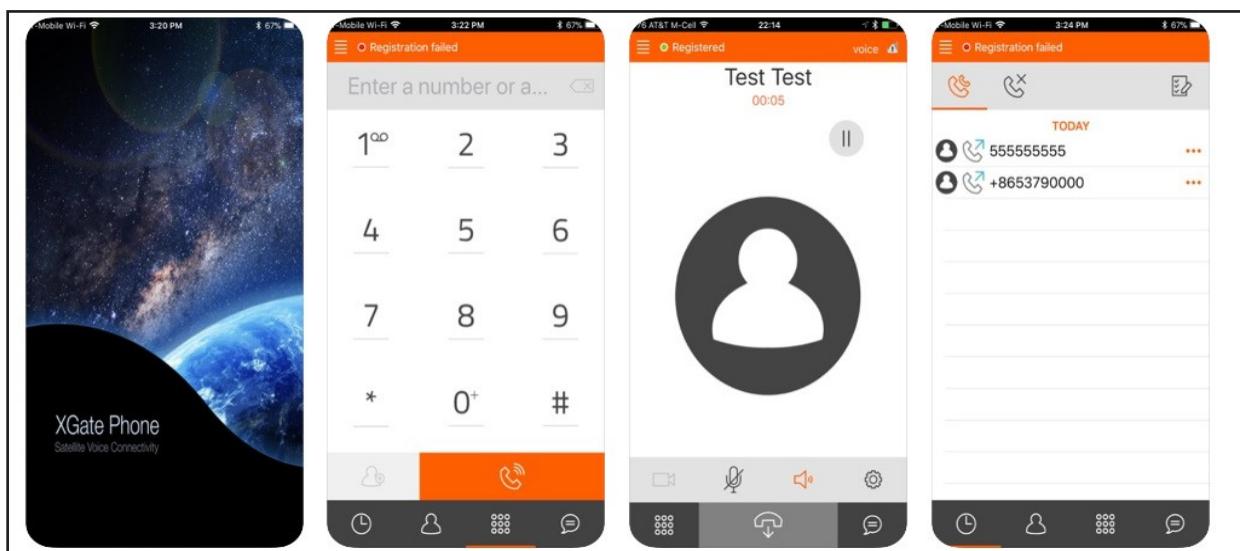
- Change the SIP extension password
- Change the outgoing CallerID display
- Enter a description for your reference

6.3.3. How to Make and Receive Voice Calls

Using your smartphone or tablet Wi-Fi network settings, connect to the Optimizer wireless network 'wXa-213-xxxx'.

Open the XGate Phone App to make and receive calls. Note: Standard voice calling rates apply.

Only one phone call can be active at a time. (Multi-user Voice and SMS is possible -- up to four consecutive sessions -- with the optional RedPort VoIP service. Contact your service provider for details.



6.3.4. FleetBroadband Monitor (FBB)

FleetBroadband Monitor requires that the Fleet Broadband be configured to accept AT commands.

The screenshot shows the Optimizer web interface for the wXa-203 v2.61 version. The top navigation bar includes Home, Services (selected), Status, System, Network, Statistics, Logout, and a 'Changes: 0' indicator. Below the navigation is a horizontal menu with tabs: Web Compression and Filtering, SMS, GPS Tracking, Remote Access, WiFi Extender, GPS/NMEA Repeater, Voice PBX, and FBB Monitor (selected). A sub-menu titled 'Fleet Broadband Monitor' is open. The main content area is titled 'Fleet Broadband monitoring' and contains a note: 'Fleet Broadband Monitoring requires that the Fleet Broadband be configured to accept AT commands.' Below this is a section titled 'Fleet Broadband Monitoring Settings' with the following configuration options:

Setting	Value	Description
Enable	<input checked="" type="checkbox"/>	
Configure Port and IP	<input type="checkbox"/> <small>Use this to configure the IP address and port if different than the default route</small>	
Debug	<input checked="" type="checkbox"/> <small>Enable debug output in the system log</small>	
Threshold	25.5	<small>Signal Levels greater than this produce a constant orange LED If the lower the LED is off</small>

At the bottom of the form are 'Reset', 'Save', and 'Save & Apply' buttons. The footer of the page states 'Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)'.

6.4. Halo Wi-Fi Extender

Requires a Halo Long Range Wi-Fi Extender for use.

The Halo long-range Wi-Fi extender system takes a weak Wi-Fi signal – at a marina, for example, or truck stop, basecamp, etc. – and amplifies that signal and routes it through the RedPort Optimizer Wi-Fi hotspot. It has a marine enclosure designed for outside installation. Install the Wi-Fi Extender almost anywhere outside.

Please consult the Halo Long Range Wi-Fi Extender Quick Start Guide for initial set up.



CAUTION: Attach the antenna to the Halo body BEFORE powering the unit. Powering the Halo without the antenna attached will damage the unit and may render it inoperable.

6.4.1. Configure Optimizer for use with the Halo Wi-Fi Extender

With the Halo powered ON and connected to the Optimizer, login to the Optimizer router. Configuration of the Halo Wi-Fi Extender can be accessed by default through either the admin or superadmin user type. Configuration of the Optimizer for use with your Halo Long Range Wi-Fi Extender is outlined as follows:

1. On the portal dashboard locate the Wi-Fi Extender Setup panel. In step 1 click the <Connect> button.

The screenshot shows the Optimizer portal interface. At the top, there's a header bar with tabs for Home, Services, Status, System, Network, Statistics, and Logout. The Home tab is selected. To the right of the header, it says "Changes: 0". Below the header, there's a "Tasks" section with a "Welcome" message. Under "Welcome", there's a "WiFi Extender Setup" section. This section contains three steps:

- Step 1**: Contains a "Connect" button with a green checkmark and a note: "Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port."
- Step 2**: Contains an "Enable WiFi Extender" button with a green checkmark and a note: "WiFi Extender Status: OFF". It also includes a note: "Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi Extender first (see Step 1)."
- Step 3 (Automatic)**: Contains a "Disable Firewall" button with a red circle and a note: "Firewall Status: ON". It also includes a note: "Disabling the firewall allows all traffic to/from the Internet through the router. This option should be used with caution and only when connected to land based WiFi."

2. Click <Scan> to see what wireless networks may be available.

Optimizer | wXa-WiFi v2.0 | Load: 0.41 0.29 0.20 | Auto Refresh: **on** Changes: 0

Home Status Admin

Wireless Overview

	Generic MAC80211 802.11bgn (radio0) WiFi Extender	Channel: 8 (2.4 GHz) Bitrate: ? Mbit/s	SSID: GMN WiFi Mode: Client	BSSID: 92:3B:AD:26:39:A3 Encryption: -	<input type="button" value="Scan"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>
--	--	--	---	--	--

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
<i>No information available</i>						

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

3. Click the wireless network you want to connect to and press <Join Network>.

Optimizer | wXa-WiFi v2.0 | Load: 0.09 0.22 0.15 Changes: 0

Home Status Admin

Join Network: Wireless Scan

	GMN WiFi 100% Channel: 8 Mode: Master BSSID: 92:3B:AD:26:39:A3 Encryption: WPA2 - PSK	<input type="button" value="Join Network"/>
	ATT8qfw8C4 100% Channel: 4 Mode: Master BSSID: 14:ED:BB:42:1F:51 Encryption: WPA2 - PSK	<input type="button" value="Join Network"/>
	GMN WiFi 100% Channel: 8 Mode: Master BSSID: 92:3B:AD:26:3A:D4 Encryption: WPA2 - PSK	<input type="button" value="Join Network"/>
	CGNM-0408 61% Channel: 6 Mode: Master BSSID: 1C:AB:C0:81:04:08 Encryption: mixed WPA/WPA2 - PSK	<input type="button" value="Join Network"/>
	NTGR_VMB_1480705304 100%	<input type="button" value="Join Network"/>

4. If the Wi-Fi source you are connecting to is password protected enter the password to access the external wireless network and click <Submit>.

Optimizer | wXa-WiFi v2.0 | Load: 0.38 0.25 0.17 Changes: 0

Home Status Admin

Join Network: Settings

WPA passphrase	<input type="text" value="....."/>
Specify the secret encryption key here.	
Name of the new network	<input type="text" value="wwan"/>

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Notice the signal strength is 0% as you are not yet connected to the wireless network. Click <Save & Apply> to tell the Halo to connect to that network.

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

- General Setup
- Status

Operating frequency

Mode	Channel	Width
(N)	(8 (2447 MHz))	(20 MHz)

Signal Strength: 0% (Blinking)

Mode: Client | **SSID:** GMN WiFi
BSSID: 92:3B:AD:26:39:A3 | **Encryption:** WPA2 PSK (CCMP)
Channel: 8 (2.447 GHz) | **Tx-Power:** 27 dBm
Signal: -15 dBm | **Noise:** -84 dBm
Bitrate: 72.2 Mbit/s | **Country:** US

[Back to Overview](#) [Reset](#) [Save](#) [Save & Apply](#)

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Notice that now the signal strength now registers greater than 0%.

NOTE: If the signal status is blinking from 0% to 100% this typically means that the Wi-Fi Network Password/Key was entered incorrectly. Check with the external Wi-Fi Network Administrator to confirm the correct password. Click the Wireless Security tab and enter the correct password in the Key field and <Save & Apply>.

5. Click the <Home> Tab to return to the Welcome screen.

Wireless Overview

WiFi Extender Status

- Authentication Status: Authenticated
- Interface Live Status:
 - HTTP is active web:direct
 - WIFI is active IPv4:192.168.51.71
 - DNS is active server:192.168.51.1

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

6.4.2. Route Network Traffic through the Halo Wi-Fi Extender

1. On the portal dashboard locate the Wi-Fi Extender Setup panel. In step 2 click the <Enable WiFi Extender> button.

The screenshot shows the Optimizer portal interface for a wXa-203 device. The top navigation bar includes links for Home, Services, Status, Statistics, and Logout, along with a 'Changes: 0' indicator. The main content area is titled 'Welcome' and contains a 'WiFi Extender Setup' section. This section is divided into three steps:

- Step 1:** Contains a 'Connect' button with a green checkmark icon and the text: 'Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.'
- Step 2:** Contains a 'Disable WiFi Extender' button with a red crossed-out circle icon and the text: 'WiFi Extender Status: ON'. Below it, the instruction 'Disable WiFi Extender to route traffic through Satellite Link.' is displayed.
- Step 3 (Automatic):** Contains an 'Enable Firewall' button with a green checkmark icon and the text: 'Firewall Status: OFF'. Below it, the instruction 'Enabling the firewall disables all traffic to the Internet except for optimized Email and web browsing.' is displayed.

All traffic is now routed through the Wi-Fi Extender. You can run XGate and XWeb.

To return to routing traffic through your satellite device, simply Click <Disable Wi-Fi Extender>.

6.4.3. Manage Halo Firewall

NOTE: This step is optional.

With the Halo powered ON and connected to the Optimizer, login to the Optimizer router. Configuration of the Halo Wi

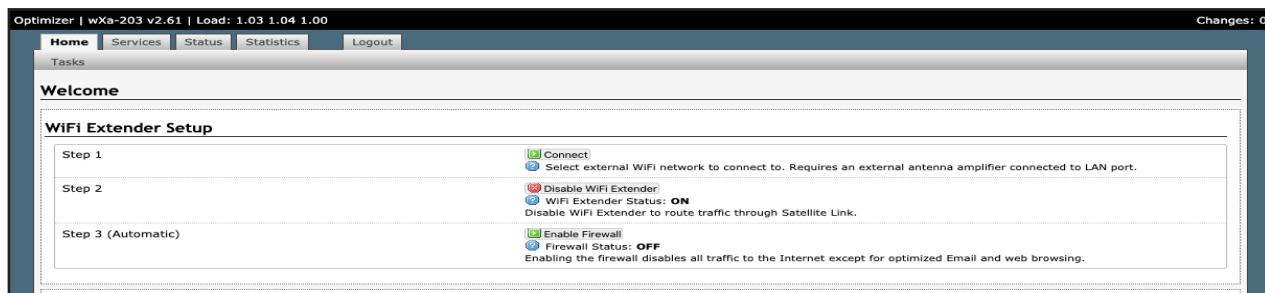
If the firewall is ENABLED, ALL traffic from your computer is blocked from the Internet with the exception of XGate and XWeb traffic. This setting is recommended when using the Halo in areas where there may be many users competing for the wireless network bandwidth thereby causing slow and painful Internet connections.

If the firewall is DISABLED, ALL traffic is permitted, allowing unfettered access to the Internet as well as XGate and XWeb traffic.

If you want to sync some applications or perform some other function that is currently being blocked, i.e. streaming video, you must Disable the Firewall.

To Disable the Firewall, click <Disable Firewall>.

To Enable the Firewall, click <Enable Firewall>.



NOTE: When the <Disable Firewall> button is presented and the “Status” of the Firewall is: ON, then the Firewall is currently on, and Clicking the button will Disable the Firewall. Otherwise, when the <Enable Firewall> button is presented and the “Status” of the Firewall is: OFF, then the Firewall is currently off.

6.4.4. Disconnect from the Halo Wi-Fi

To disconnect from the Halo, click <Disable Wi-Fi Extender>.

The screenshot shows the Optimizer web interface with the following details:

- Header: Optimizer | wXa-203 v2.61 | Load: 1.15 1.04 1.01 | Changes: 0
- Navigation: Home, Services, Status, Statistics, Logout
- Section: Welcome
- Sub-section: WiFi Extender Setup
- Content:
 - Step 1:
 - Connect
 - Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
 - Step 2:
 - Enable WiFi Extender
 - WiFi Extender Status: **OFF**
 - Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi Extender first (see Step 1).
 - Step 3 (Automatic):
 - Disable Firewall
 - Firewall Status: **ON**
 - Disabling the firewall allows all traffic to/from the Internet through the router. This option should be used with **caution** and only when connected to land based WiFi.

Notice that the Firewall is turned back on automatically to protect you from runaway airtime charges.

NOTE: An alternate method of disconnecting from the Halo is to cycle power to Optimizer or Reboot the Optimizer. This will also restore the Firewall Status to ON.



CAUTION: It is important to <Disable Wi-Fi Extender> when the external Wi-Fi network is no longer available, and you want to use your satellite device. Failure to Disable will prevent a successful satellite connection as the Optimizer continues to look for the external Wi-Fi network.

6.5. GPS Tracking

GPS Tracking is a premium service with a monthly charge and is not included with the purchase of a RedPort Optimizer. If you wish to have tracking service using your satellite device, the Optimizer works with RedPort Tracking. Contact your RedPort dealer or RedPort directly (support@redportglobal.com) to enable RedPort Tracking before you set it up on your Optimizer.

6.5.1. Tracking powered by RedPort

Using a GPS-enabled satellite device (e.g. Aurora, Glow), the Optimizer can be configured to submit position reports to a central database for viewing on the tracking website.

To enable this service, Click Services > GPS Tracking > Tracking.

The screenshot shows the Optimizer web interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.05 1.03 1.00 | Changes: 0
- Top Navigation:** Home, Services, Status, System, Network, Statistics, Logout, Web Compression and Filtering, SMS, GPS Tracking (selected), Remote Access, WiFi Extender, GPS/NMEA Repeater, Voice PBX, FBB Monitor
- Section:** Tracking
- Tracking Parameters:**
 - Enable Tracking:
 - Provider: Select Provider (dropdown menu) - Help: Tracking provider. Please contact provider to setup tracking account.
 - Tracking Interval: 60 (minutes) - Help: Specify the tracking interval in minutes.
- Tracking powered by RedPort:**
 - Please visit www.RedPortGlobal.com for registration information
 - INMARSAT FleetBroadband:
 - Fleet Broadband IP: - Help: IP address of Fleetbroadband. Leave blank for default gateway.
 - Thales Certus VesselLink:
 - Iridium OpenPort/Pilot:
 - INMARSAT Isatphone:
 - VSAT or broadband satellite: Help: A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
 - Globalstar phone: Help: A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
 - Iridium terminal/Aurora/MCG-101: Help: A valid NMEA/GPS feed is required.
- Tracking via SMS:**
 - Send GPS information to an email address using satellite provider's SMS service
 - INMARSAT Isatphone:
 - Iridium terminal/Aurora/MCG-101: Help: A valid NMEA/GPS feed is required.
 - Recipient Email Address: GSatTrack (dropdown menu) - Help: Select SMS tracking service or enter a valid email address. Also used for SOS messages. Enter blank to reset defaults.
 - Vessel name: - Help: Enter optional vessel name and/or other free text.
- Buttons:** Reset, Save, Save & Apply
- Page Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

1. Enter the Tracking Interval in minutes; the default is set to hourly reporting (60 minutes). This means that every 60 minutes a position report will be transmitted over your satellite link. Keep in mind that standard airtime charges will apply to each position report. Adjust the Tracking Interval to meet your needs.
2. Select the satellite terminal you are using.

NOTE: A valid NMEA/GPS feed is required when using some satellite devices.

3. Click <Save & Apply>.

6.5.2. SMS Tracking

If using certain satellite devices, GPS information can be sent to an email address using your satellite provider's SMS service. Standard SMS charges may apply; check with your satellite airtime provider for details.

The screenshot shows the Optimizer software interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.05 1.03 1.00 | Changes: 0
- Top Navigation:** Home, Services, Status, System, Network, Statistics, Logout. The "Services" tab is selected.
- Sub-Header:** Web Compression and Filtering, SMS, GPS Tracking (highlighted), Remote Access, WiFi Extender, GPS/NMEA Repeater, Voice PBX, FBB Monitor.
- Section:** Tracking
- Tracking Parameters:**
 - Enable/disable tracking and set parameters. Standard airtime charges apply.
 - General Tracking Parameters:**
 - Enable Tracking:
 - Provider: Select Provider. Please contact provider to setup tracking account.
 - Tracking Interval: Specify the tracking interval in minutes.
 - Tracking powered by RedPort:**
 - Please visit www.RedPortGlobal.com for registration information.
 - INMARSAT FleetBroadband:
 - Fleet Broadband IP: IP address of Fleetbroadband. Leave blank for default gateway.
 - Thales Certus VesselLink:
 - Iridium OpenPort/Pilot:
 - INMARSAT Isatphone:
 - VSAT or broadband satellite: A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
 - Globalstar phone: A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
 - Iridium terminal/Aurora/MCG-101: A valid NMEA/GPS feed is required.
 - Tracking via SMS:**
 - Send GPS information to an email address using satellite provider's SMS service.
 - INMARSAT Isatphone:
 - Iridium terminal/Aurora/MCG-101: A valid NMEA/GPS feed is required.
 - Recipient Email Address: Select SMS tracking service or enter a valid email address. Also used for SOS messages. Enter blank to reset defaults.
 - Vessel name: Enter optional vessel name and/or other free text.
- Buttons:** Reset, Save, Save & Apply.
- Page Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

1. Enter the Tracking Interval in minutes; the default is set to hourly reporting (60 minutes). This means that every 60 minutes a position report will be transmitted via the SMS service provided by your satellite provider network. Keep in mind that standard SMS charges may apply to each position report. Adjust the Tracking Interval to meet your needs.
2. Select which satellite device you are using. At this time, tracking via SMS is available with the Inmarsat IsatPhone, Iridium handheld 9575 Extreme, Iridium GO! or an Iridium terminal such as the Pilot.

NOTE: A valid NMEA/GPS feed is required when using an Iridium terminal.

3. Enter the recipient's email address. The SMS message with the GPS information will be sent to this email address at the interval entered in Step 1.
4. Click <Save & Apply>.

6.6. GPS/NMEA Repeater

The Optimizer supports USB and RS-232 NMEA devices allowing multiple applications to share the GPS/NMEA data. If you have a NMEA RS-422 device, adding a RS-422 to RS-232 converter to your setup may allow the sharing of data.

The Optimizer does not transmit data but can be configured to receive and repeat GPS/NMEA data from:

- A broadband satellite terminal with integrated GPS when connected to the Optimizer via a standard Ethernet connection. (As of this writing, supported terminals include: Iridium Pilot, Inmarsat FBB and Inmarsat BGAN.)
- A handheld satellite phone with integrated GPS when connected to the Optimizer with the satphone's USB- Mini/Micro USB cable. (As of this writing, supported handheld satphones include: Iridium 9575 Extreme and Inmarsat IsatPhonePro.)



CAUTION: IsatPhone users! The phone only transmits GPS coordinates about every 10 minutes. It is NOT recommended for navigation or any application that requires real time data.

- A USB connected GPS or NMEA device.
- A serial port connected GPS or NMEA device.

NOTE: If you are using a satellite phone with a serial port (RS-232) that transmits GPS data (i.e. some fixed phones and fleet phones), it is NOT compatible with the Optimizer. In order to repeat GPS data, a separate GPS device must be connected.

6.6.1. GPS/NMEA Repeater Equipment Setup

A physical connection is required from the source (satellite terminal or satellite phone that transmits GPS coordinates, or other GPS/NMEA device) to the Optimizer.

6.6.1.1. Broadband Satellite Terminal with Integrated GPS

When using a supported broadband satellite terminal with integrated GPS, connect the terminal to the Optimizer SAT port using a standard Ethernet cable. (OPTIONAL: Use a second Ethernet cable to connect the computer with the destination software, like a navigation program, to the Optimizer LAN port.) The Optimizer will broadcast the GPS signal both over Ethernet and Wi-Fi, so you can connect your computer either way in order to establish a successful connection with your destination software.

6.6.1.2. USB NMEA Device

When using a NMEA device that supports a USB connection, connect the GPS/NMEA device to the Optimizer with an appropriate USB to NMEA device cable as indicated by the NMEA device manufacturer.

(OPTIONAL: Use an Ethernet cable to connect the computer with the destination software, like a navigation program, to the Optimizer LAN port.)

The Optimizer will broadcast the GPS signal both over Ethernet and Wi-Fi, so you can connect your computer either way in order to establish a successful connection with your destination software.

NOTE: If your satellite device requires a USB connection to the Optimizer (for example, an Iridium 9555) you can use a 2-port USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accommodate two USB devices.

6.6.1.3. RS-232 NMEA Device

When using a NMEA device with Serial Port connection, a USB to Serial Adapter (PL-2303HX) is required to connect the device to the Optimizer.



CAUTION: The PL-2303 is the only USB to Serial Adapter that is compatible with the Optimizer.

The Optimizer will broadcast the GPS signal both over Ethernet and Wi-Fi, so you can connect your computer either way in order to establish a successful connection with your destination software.

NOTE: If your satellite device requires a USB connection to the Optimizer (for example, an Iridium 9555) you can use a 2-port USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accommodate two USB devices.

For those users without a Serial Port Connector

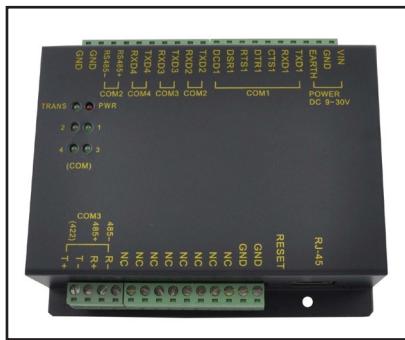
Some NMEA devices do not have a serial port; instead they have a group of wires extending from the back or bottom of the unit. These devices require proper wiring to a serial port.

As the Optimizer does not transmit, it only repeats the data, you will only need two of the wires. The Receive (RD) wire goes to pin 2 and the Ground (SG) wire goes to pin 5.

A simple solution is to use a terminal block as shown here. Simply connect the RD wire to pin2 and the SG wire to pin 5. Then connect the terminal block to the PL-2302 USB to serial adapter.

6.6.1.4. Connecting Multiple NMEA Devices

It is possible to connect up to four NMEA devices if you have the proper hardware. It will require a USB to RS-232 4-port Hub or a RS-232 4-port terminal block that you would simply plug into the Optimizer's USB port.



NOTE: The Optimizer supports RS232. If you have a NMEA RS-422 device, adding a properly wired RS-422 to RS-232 converter to your setup may allow the sharing of data.

6.6.2. GPS/NMEA Repeater Parameters Configuration

In order for the destination software to properly route the GPS data you must configure the GPS/NMEA Repeater Parameters in the Optimizer User Interface.

From the Optimizer Home page Click Services > GPS/NMEA Repeater tab.

1. Select the source of the GPS/NMEA information (choose only one):
 - GPS from broadband satellite: Click this if you are using a broadband satellite terminal with integrated GPS.
 - GPS/NMEA feed from USB: Click this when connecting a GPS or NMEA device via USB cable. NMEA Baud Rate - Using the drop down menu, Click the baud rate required for the destination software. By default, most NMEA 183 devices (GPS) and applications use 4800 baud for this setting.
2. UDP Listener Port - Enter the UDP port number that the GPS is connected to. The default is set to the standard UDP Listener Port for NMEA 183 devices of 10101.
3. UDP Port - Enter the UDP port number to broadcast the GPS data to. The default is set to the standard UDP Port for NMEA 183 devices of 11101.

NOTE: Configure the destination software to match this port number; or, change this entry to match the requirements of the destination software.

4. TCP Port - Enter the TCP port number to broadcast the GPS data to. The default is set to the standard TCP Port for NMEA 183 devices of 11102.

NOTE: Configure the destination software to match this port number; or, change this entry to match the requirements of the destination software.

NOTE: The data will be broadcast to both the UDP Port and the TCP Port. It is important to make sure that these two ports are NOT set to the same port number.

To use the GPS Repeater feature, your computer must be connected to the Optimizer's Wi-Fi network or directly connected to the LAN port of the Optimizer.

6.7. Remote Support



CAUTION: Remote Support requires a upstream connection source. If using a satellite device with activate satellite airtime will require the use of your satellite airtime data.

NOTE: Do not set your remote Access Port to the presented port in this document's screen shots. The router will present a port to you. Do not attempt to log in with the example remote login, it is just presented for your knowledge.

Remote Support Access can be granted from two locations, each with some differences.

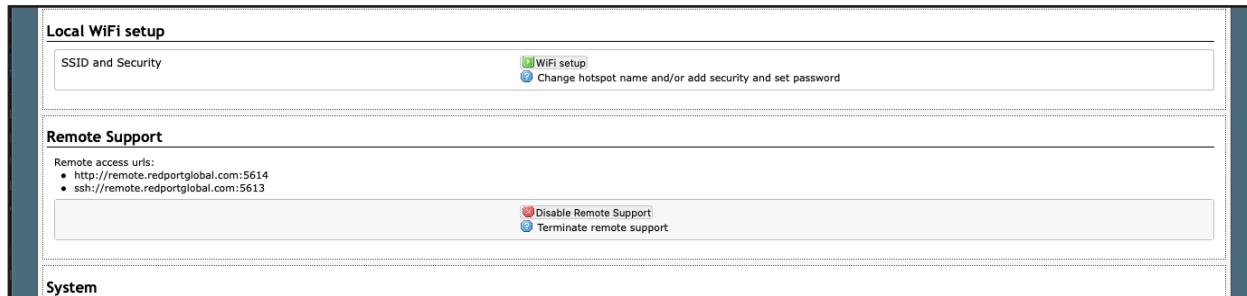
- Temporary Remote Support Access - The first remote support login access is located from the homepage and permits a one-time temporary access. Once the router is rebooted, this access will no longer be available.

The screenshot shows the Optimizer web interface for wXa-203 v2.61. The top navigation bar includes Home, Services, Status, Statistics, and Logout. The main content area has a 'Welcome' header. Under 'WiFi Extender Setup', there are three steps: Step 1 (Connect: Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port), Step 2 (Disable WiFi Extender: WiFi Extender Status: ON), and Step 3 (Automatic: Enable Firewall, Firewall Status: OFF). Below this are sections for System Status, Local WiFi setup, Remote Support, and System, each with their respective configuration options. At the bottom, it says 'Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)'.

To enable Temporary Remote Support Access, click <Home> tab, scroll down to the “Remote Access” section.

Click <Enable remote support> under “Remote Support” section of the <Home> tab.

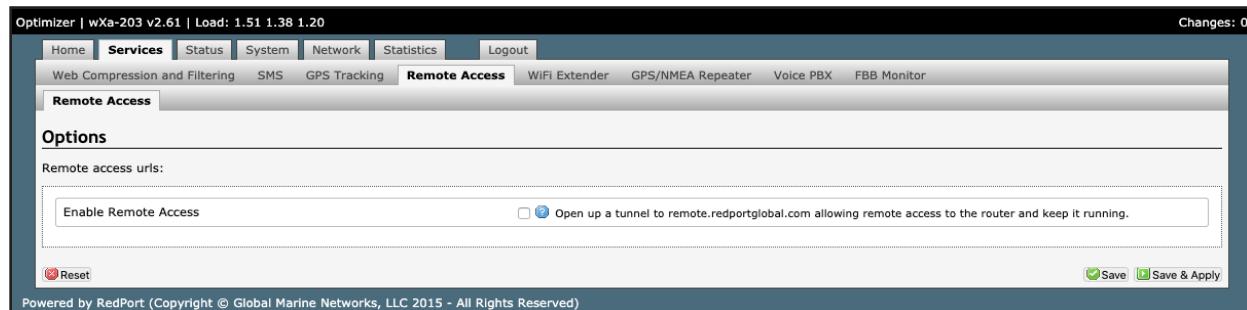
When remote support is enabled Remote Access URLs are displayed.



Disabling this Remote Support will not disable the persistent Remote Support. To disable this remote support access, either:

- Reboot the router.
- Click <Disable Remote Support>.
- Persistent Remote Support Access - The second remote support login access is located from the Services tab and permits persistent access. Even if the router is rebooted, this access will remain.

To enable Persistent Remote Support Access - Navigate to <Services> tab, then to <Remote Access>.



Click the “Enable Remote Support” button and then click <Save & Apply>.

When remote support is enabled Remote Access URLs are displayed.

The screenshot shows the Optimizer web interface with the title "Optimizer | wXa-203 v2.61 | Load: 1.66 1.42 1.22". The top navigation bar includes Home, Services, Status, System, Network, Statistics, Logout, and a "Changes: 0" indicator. Below the navigation is a horizontal menu with Web Compression and Filtering, SMS, GPS Tracking, Remote Access (which is selected), WiFi Extender, GPS/NMEA Repeater, Voice PBX, and FBB Monitor. The main content area is titled "Remote Access" and contains a section for "Options". It lists "Remote access urls:" with two entries: http://remote.redportglobal.com:5041 and ssh://remote.redportglobal.com:5040. There is a checkbox labeled "Enable Remote Access" with a tooltip "Open up a tunnel to remote.redportglobal.com allowing remote access to the router and keep it running." followed by an "Access Port" input field containing "5040". At the bottom are "Reset", "Save", and "Save & Apply" buttons.

Disabling this Remote Support will not disable the one-time Remote Support. To disable remote support access:

- Click <Services> tab, then click “Enable Remote Access”.

7. Status

Available to both ‘admin’ and ‘superadmin’ login.

Use the Status tab to display current information of the router’s performance.

The screenshot shows the Optimizer web interface with the title "Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 1.00 | Auto Refresh: on". The top navigation bar includes Home, Services, Status (selected), System, Network, Statistics, and Logout, with a "Changes: 0" indicator. Below the navigation is a horizontal menu with Overview (selected), Firewall, Routes, System Log, Kernel Log, and Realtime Graphs. The main content area displays a summary of system status and performance metrics.

Some of the information provided here includes:

- How much memory the router is currently using
- Who is currently connected via wifi
- Error messages reported in the System Log and can be useful when troubleshooting connection issues.
- Realtime Graphs report how much data is being used by the different interfaces.

All Status information is READ ONLY

7.1. Access System Log

If you are experiencing connection issues your service provider may request that you send them a copy of the Optimizer System Log.

Step 1. Attempt an email connection.

Step 2. Login to the Optimizer Home page.

Step 3. Go to Status > System Log.

Step 4. Copy/paste the entire log into an email and send to your service provider.

```

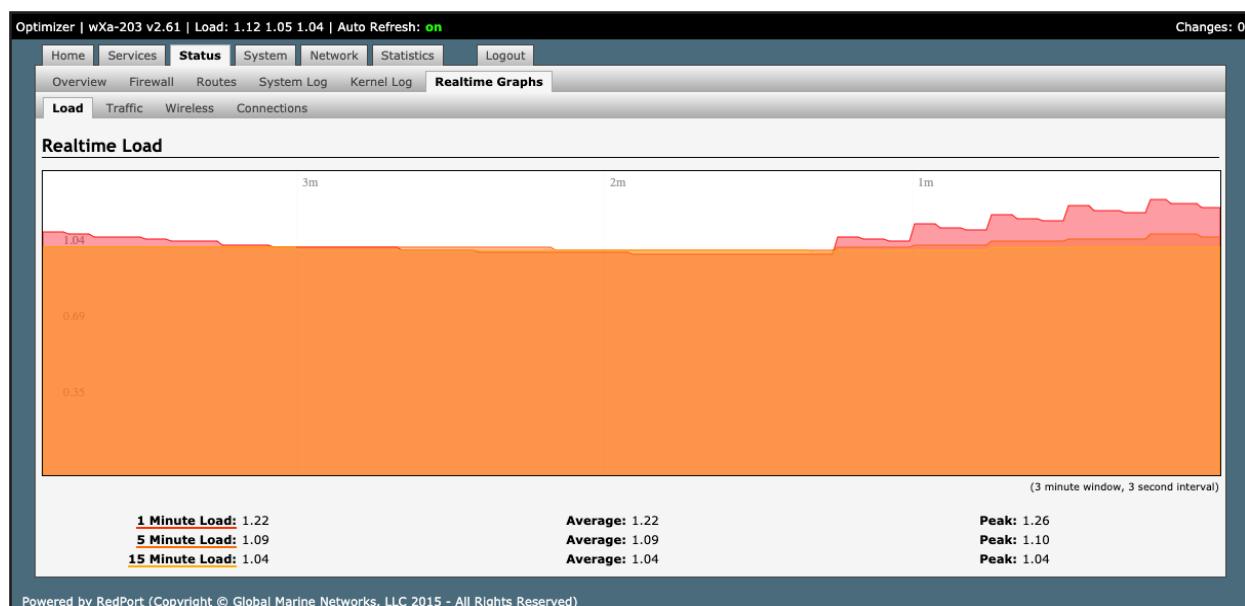
Optimizer | wXa-203 v2.61 | Load: 1.02 1.03 1.04
Changes: 0
Home Services Status System Network Statistics Logout
Overview Firewall Routes System Log Kernel Log Realtime Graphs
System Log
System Log
Wed Mar 25 12:29:51 2020 daemon.info dnsmasq[738]: read /tmp/hosts/dhcp - 2 addresses
Wed Mar 25 12:29:51 2020 daemon.info dnsmasq-dhcp[738]: read /etc/ethers - 0 addresses
Wed Mar 25 12:30:07 2020 daemon.info dnsmasq[738]: exiting on receipt of SIGTERM
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq[866]: started, version 2.80 cachesize 150
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq[866]: compile time options: IPv6 GNU-getopt no-DBus no-i18n no-IDN DHCP DHCPv6 no-Lua TFTP no-contrack ipset auth DNSSEC no-I
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq-dhcp[866]: DHCP, IP range 192.168.10.100 -- 192.168.10.249, lease time 12h
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq-tftp[866]: TFTP root is /tftpboot
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq[866]: read /etc/hosts - 1 addresses
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq[866]: read /tmp/hosts/dhcp - 2 addresses
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq-dhcp[866]: read /etc/ethers - 0 addresses
Wed Mar 25 12:30:11 2020 daemon.err uhttpd[1398]: Warning: Section #zone[1] (cap) cannot resolve device of network 'cap'

```

NOTE: The System Log date will show May 31 unless you have synced the Optimizer Local Time with a browser in System Tab > Local Time > Sync with browser. This is NOT recommended when using a satellite connection and it is not necessary to ever sync the time. If you do sync the time, as soon as power is removed from the Optimizer the date will revert to May 31.

7.2. System Status for Monitoring Usage

For those that are interested, you can view the connection status in Status > Realtime Graphs.



8. System

8.1. Change Default User Password

The default password for both the superadmin login and the admin login is set to: webxaccess.

The easiest way to change the login admin password is to modify the XGate Settings. See the XGate Help File > User Interface > Settings > Optimizer, wXa, & Sat-Fi for details. The only way to change the superadmin password is via the Optimizer User Interface.

To change the password(s), login to the Optimizer:

The screenshot shows the Optimizer User Interface with the following sections visible:

- WiFi Extender Setup** (selected tab):
 - Step 1: Connect (Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.)
 - Step 2: Enable WiFi Extender (WiFi Extender Status: OFF) (Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi Extender first (see Step 1).)
 - Step 3 (Automatic): Disable Firewall (Firewall Status: ON) (Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution and only when connected to land based WiFi.)
- System Status** (disabled):
 - System status overview
 - Realtime bandwidth usage over satellite link
 - Historic bandwidth usage over satellite link
 - System message log
- Local WiFi setup** (disabled):
 - SSID and Security: WiFi setup (Change hotspot name and/or add security and set password)
- System** (disabled):
 - Router password
 - Reboot router

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Click <Router password>.

When logged in as the superadmin, you will see this screen. If logged in as the admin user, you can only change the password for the admin login.

The screenshot shows the Optimizer web interface with the title "Optimizer | wXa-203 v2.61 | Load: 1.02 1.05 1.06". The top navigation bar includes links for Home, Services, Status, System, Network, Statistics, Logout, System, Router Password, Profiles, Backup / Flash Firmware, and Reboot. A "Changes: 0" indicator is in the top right. The main content area is titled "Router Password" and contains two sections: "Change Password" for the "superadmin" user and another "Change Password" section for the "admin" user. Both sections include "Password" and "Confirmation" fields with small icons next to them. At the bottom left is a "Reset" button, and at the bottom right are "Save" and "Save & Apply" buttons.

1. Enter the new password in the password text box.
2. Enter the same password again in the Confirmation text box.
3. Click <Save & Apply>.

This procedure changes the password for the Superadmin or the Admin login only. When connecting your computer, iOS or Android device to the wireless network, you will not use this Admin login password. This password is used only to access the Optimizer user interface.

8.2. Profiles

Profiles is designed for users of multiple satellite devices and integrators of custom installations. You can configure the Optimizer for a specific satellite device and save the profile. This is good for failover situations when using multiple devices. An extreme example would be that you might have the firewall wide open on a VSAT device but in an emergency must use an Iridium handheld device where you want the full protection of the Optimizer firewall. Have a profile for each configuration and select the appropriate one for the satellite device being used.

To access Profile Manager, go to System > Profiles.

Profile	Description	Actions
ATA	Analog Telephone Adapter and WiFi-Ethernet Network Bridge	<input type="button" value="Install"/> <input type="button" value="Delete"/>
SatFi	SatFi ATA Profile	<input type="button" value="Install"/> <input type="button" value="Delete"/>
Factory	Factory default settings	<input type="button" value="Install"/> <input type="button" value="Delete"/>
<input type="button" value="Add"/>		

There are three default profiles:

ATA: This profile is used to make the Optimizer into an Analog Telephone Adapter when linking an Analog Telephone through Wi-Fi Ethernet Networking Bridge and repeats the satellite terminal's SSID. This profile would be installed automatically as needed when the Optimizer is plugged into a satellite terminal.

Factory: This profile will reset the Optimizer to factory defaults and all custom configuration will be lost.

To create and use a new Profile:

1. Click <Add>.
2. Enter a Name of the new profile and a description.
3. Click <Install> to add the new profile.
4. Click <Save & Apply>.



To change from using one profile to another, simply Click <Install> for the desire profile, then <Save & Apply>.

8.3. Update Optimizer Firmware

Get the latest Optimizer firmware version from here:

redportglobal.com/support/technical-downloads/ Save the .bin file to your computer (pc or mac).

NOTE: If you have created any Profiles you may want to Export them before flashing new firmware and Import them when done.

Login to the Optimizer and go to: System > Backup/Flash Firmware.

1. Keep Settings: remove the check in the box to uncheck Keep Settings.
2. <Browse> to where you saved the .bin file and Click that file.
3. Click <Flash Image>.
4. Wait for the gray button on top of the Optimizer to begin flashing. When the button stops flashing, the firmware is done updating. This typically takes several minutes.

To confirm the firmware upgrade, login to the Optimizer Home Page again. The firmware version displays in the top banner of the User Interface.

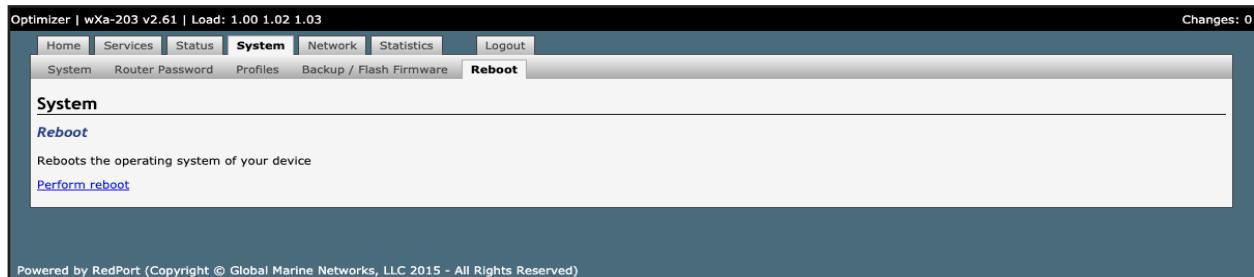
8.4. Reboot the Optimizer Router

The easiest way to reboot the Optimizer is to use the reset button on the bottom of the router. Using a pointed instrument, press and hold the red reset button for 20-30 seconds and release. Wait for the Optimizer reboot, this will take several minutes. After this reset, the Optimizer will be configured with its factory defaults. You will need to reenter any modifications you made to the user interface. You can also reboot the router from within the Optimizer user interface:

1. Login to the Optimizer Home page.

The screenshot shows the Optimizer v2.1.0 user interface. At the top, there is a navigation bar with tabs: Home, Services, Status, System, Network, Statistics, and Logout. The Home tab is selected. On the left, there is a sidebar titled "Tasks" with sections for "Welcome", "WiFi Extender Setup", "System Status", "Local WiFi setup", and "System". The "WiFi Extender Setup" section is expanded, showing three steps: Step 1 (Connect), Step 2 (Enable WiFi Extender), and Step 3 (Automatic). Step 3 includes options to Disable Firewall (which is ON) and Firewall Status (which is ON). Below this, the "System Status" section is expanded, showing system status overview, realtime bandwidth usage, historic bandwidth usage, and a system message log. The "Local WiFi setup" and "System" sections are partially visible. At the bottom, there is a footer with the text "Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)".

Click <Reboot Router>.



3. Click <Perform reboot>.

The gray button on top of the Optimizer will flash during the reboot process. When the light stops flashing the reboot is complete. This will take several minutes.

During the reboot process you will lose access to the Optimizer User Interface. You must login again if you want access.

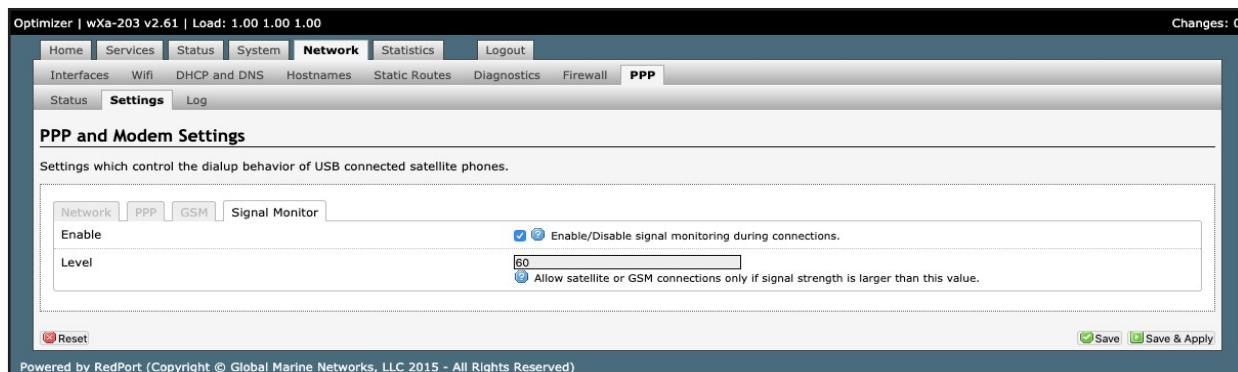
9. Network

9.1. Signal Monitor

Signal monitor queries your satellite device to determine if the signal strength is sufficient to make a successful data connection. Typically, a minimum of 60% signal is required; however, 100% is ideal for the fastest possible data transfer rate.

NOTE: Some of the older satellite phones (for example, the Iridium 9505a) do not support the signal monitor feature. For these older satellite phones, the signal monitor **MUST** be DISABLED for a successful data connection.

To modify the Signal Monitor, go to: Network > PPP > Settings.



From this screen you can enable/disable signal monitor using the “Enable” checkbox.

You can change the level of the Signal Monitor. Keep in mind that 60% is typically the minimum required for a successful data connection. If you must change the Signal Monitor, we recommend lowering the Level vs. disabling it. Many IsatPhonePro users have had success by lowering the level to 40 or 30.



CAUTION: Reducing the signal strength to less than 60% or disabling it altogether may cause lengthy data connections due to poor signal.

When you are done making changes, click <Save & Apply>.

Signal monitor can also be changed from within the XGate Settings. See the XGate Help File > User Interface > Settings > Optimizer, wXa, & Sat-Fi for details.

9.2. GSM

The GSM feature is offered for your convenience, but we are not able to support it. The information provided here is general in nature but may not be sufficient to establish a GSM connection. If you run into any difficulties, you must contact your GSM network provider for support.

If you have a GSM-based cellular phone, it may be possible to use the GSM network, when available, for XGate and XWeb data over the Optimizer. You will get the benefits of compression and a faster data transfer rate than over a satellite phone which typically equates to cost savings.

Only GSM-based service is supported. LTE-based and CDMA-based service is NOT supported. If you are unsure of which service you have, contact your cellular provider before attempting to configure for GSM connection.

9.2.1. GSM Configuration in Optimizer

With the Halo powered Before you can configure the Optimizer for GSM, you must:

- Obtain a USB data dongle from your cellular provider. Your provider may also require you to purchase a data plan.
- Activate the USB data dongle with your cellular carrier and test it to make sure it works. Typically, testing requires only that you plug the USB Data Dongle into your computer and see if you can get on the Internet. If testing fails, contact your cellular carrier for support.
- Contact your cellular provider to obtain the information required to connect to their GSM network. The information may include:
 - Access Point Name (APN).
 - Username required for access to the APN.
 - Password required for access to the APN.

To configure the Optimizer for GSM service.

Login to the Optimizer and go to: Network > PPP > Settings > GSM.

The screenshot shows the Optimizer web interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.04 1.01 1.00 | Changes: 0
- Top Navigation:** Home, Services, Status, System, Network, Statistics, Logout
- Sub-Header:** Interfaces, Wifi, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, PPP
- Current Tab:** PPP
- Section:** Status, Settings (selected), Log
- Page Title:** PPP and Modem Settings
- Page Description:** Settings which control the dialup behavior of USB connected satellite phones.
- Form Fields:**
 - APN:** Access Point Name (input field)
 - APN Delay:** Value set under PPP settings and displayed here for convenience (input field, value 7)
 - Username:** Blank Entry
 - Password:** Blank Entry
 - Pincode:** SIM card pin. Leave blank if none required (input field)
- Buttons:** APN Wizard, Select APN by Country, Provider, and Plan, Save, Save & Apply
- Page Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

1. Enter the Access Point Name (APN) as provided to you by your cellular carrier.
2. If you have protected your cellular SIM card with a pincode, enter the pincode here.
3. Click <Save & Apply>.

NOTE: As of this writing, some customers have found the APN Wizard helpful in lieu of entering the information

manually; however, it is still under development and may or may not help with your configuration.

Now go to: Network > PPP > Settings > PPP.

Optimizer | wXa-203 v2.61 | Load: 1.04 1.01 1.00 Changes: 0

Home Services Status System Network Statistics Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP

Status Settings Log

PPP and Modem Settings

Settings which control the dialup behavior of USB connected satellite phones.

Network PPP GSM Signal Monitor

Modem Interface	<input type="button" value="System Default"/> <input checked="" type="radio"/> Select COM port assigned to modem.
Modem Speed	<input type="button" value="System Default"/> <input checked="" type="radio"/> Baud rate for modem serial interface.
Username	<input type="text"/> <input checked="" type="radio"/> Leave blank if none required.
Password	<input type="text"/> <input checked="" type="radio"/> Leave blank if none required.
Phone Number	<input type="text"/> <input checked="" type="radio"/> Phone number to dial. Leave blank for system default.
Idle Timeout	<input type="text" value="60"/> <input checked="" type="radio"/> Drop connection after X seconds if no network traffic is detected. Note It is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.
Persist	<input type="checkbox"/> <input checked="" type="radio"/> Enable persistent connections. Persistent connections forces the modem to reconnect if connection drops.
Extra Init	<input type="text"/> <input checked="" type="radio"/> Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before dialing.
MTU	<input type="text"/> <input checked="" type="radio"/> Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.
debug	<input type="checkbox"/> <input checked="" type="radio"/> Write PPP connection debugging information to the system log.

Reset Save Save & Apply

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

1. Enter the username required for access to the APN, if any.
2. Enter the password required for access to the APN, if any.
3. Click <Save & Apply>

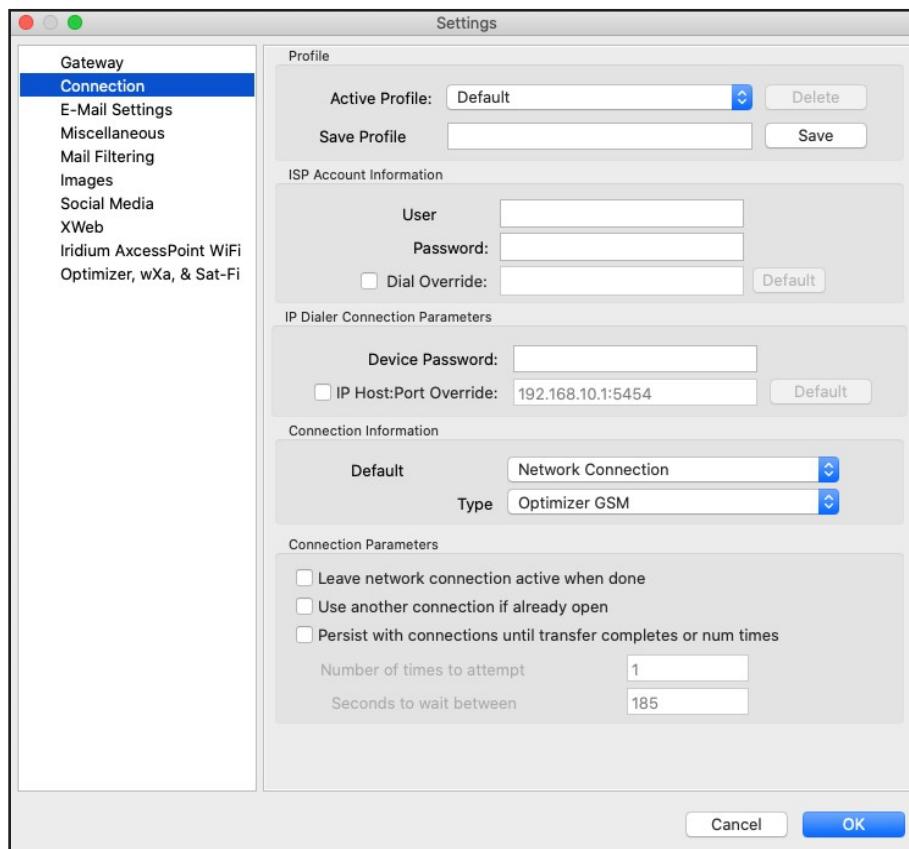
9.2.2. Using GSM

When you want to use GSM service instead of satellite service:

Plug the USB data dongle you obtained from your cellular provider into the Optimizer's USB port.

NOTE: If your satellite terminal is connected to the Optimizer's SAT port, unplug the cable from the SAT port before attempting a GSM connection.

Configure XGate Settings for GSM connection. Open XGate to Settings > Connection



Click the Connection Type <Optimizer GSM>. Click <OK> to apply the change.

9.2.3. Changing from GSM Service to Satellite Service

When you travel beyond GSM range you must:

- Remove the GSM data dongle from the Optimizer's USB port.
- Connect your satellite phone/terminal to the Optimizer (either via USB port or SAT port).
- Change the XGate > Settings > Connection Type back to the appropriate Optimizer setting.

NOTE: We are not able to support GSM connected devices or carriers. If you experience any connection difficulties when using this feature, you must contact your GSM network provider for support.

9.3. Restrict Wireless Network Access (Add or Change Network Password)

When in public locations, for example, a crowded marina or anchorage, you may want to restrict access to your Wi-Fi hotspot created by your satellite device and the Optimizer. You can password protect your Wi-Fi hotspot so others cannot use it.

Add/change a password to the Wi-Fi Hotspot (wXa-203-xxxx).

1. Login to the Optimizer:

The screenshot shows the Optimizer web interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.08 1.02 1.01 | Changes: 0
- Navigation Bar:** Home, Services, Status, System, Network, Statistics, Logout
- Tasks:** WiFi Extender Setup, System Status, Local WiFi setup, System
- WiFi Extender Setup (Step 1):**
 - Connect: Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
- WiFi Extender Setup (Step 2):**
 - Enable WiFi Extender: WiFi Extender Status: OFF
 - Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi Extender first (see Step 1).
- WiFi Extender Setup (Step 3 (Automatic)):**
 - Disable Firewall: Firewall Status: ON
 - Disabling the firewall allows all traffic to/from the Internet through the router. This option should be used with caution and only when connected to land based WiFi.
- System Status:**
 - System status overview
 - Realtime bandwidth usage over satellite link
 - Historic bandwidth usage over satellite link
 - System message log
- Local WiFi setup:**
 - SSID and Security: WiFi setup, Change hotspot name and/or add security and set password
- System:**
 - Router password
 - Reboot router

2. Click <Wi-Fi Setup> and go to: Interface Configuration > Wireless Security.

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

General Setup [Advanced Settings]

Status

radio0: Master "wXa-203-80f8" (wlan0)

Mode: Master | **SSID:** wXa-203-80f8
BSSID: 00:0A:52:05:80:FA | **Encryption:** None
Channel: 11 (2.462 GHz) | **Tx-Power:** 20 dBm
Signal: -74 dBm | **Noise:** 0 dBm
Bitrate: 65.0 Mbit/s | **Country:** 00

Wireless network is enabled

Operating frequency Mode Channel Width
N 11 (2462 MHz) 20 MHz

Transmit Power

Interface Configuration

General Setup [Wireless Security] [MAC-Filter]

Encryption

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

3. Click the Encryption mode from the drop down menu. We suggest WPAPSK/WPA2-PSK Mixed Mode.

4. Enter your desired password in the Key field.

5. Click <Save & Apply>

This procedure adds/changes the password for the Wi-Fi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the password you will use. This password does not change the router superadmin or admin password when logging in to access the Optimizer user interface.

9.4. Rename the Wireless Network (Change SSID Name)

NOTE: Renaming the Wireless Network (SSID Name) will not transfer into a Profile Save as each router needs to have a unique Wireless Network (SSID Name) to avoid network conflict.

It is possible to change the name of your wireless network. This is the name of the wireless network that you connect to using your computer or iOS or Android device. The default name is wXa-203-xxxx where the xxxx represents a unique number specific to your device. There is no default password to connect to the network.

The screenshot shows the Optimizer web interface for the wXa-203 router. The top navigation bar includes links for Home, Services, Status, System, Network, Statistics, and Logout, along with a 'Changes: 0' indicator. The main content area is titled 'Welcome' and contains several sections:

- WiFi Extender Setup**:
 - Step 1: A 'Connect' button with a note about connecting to an external WiFi network via a LAN port.
 - Step 2: An 'Enable WiFi Extender' button and a note that the WiFi Extender status is currently **OFF**. It also notes that the extender routes all network traffic through WiFi Extender.
 - Step 3 (Automatic): A 'Disable Firewall' button and a note that the firewall status is **ON**, with a warning about using caution when disabled.
- System Status**: Buttons for system status overview, real-time bandwidth usage, historic bandwidth usage, and system message log.
- Local WiFi setup**: Buttons for WiFi setup and changing hotspot name and security.
- System**: Buttons for router password and rebooting the router.

At the bottom of the page, a footer note reads: "Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)".

Click <Wi-Fi Setup> and go to: Interface Configuration > General Setup.

The screenshot shows the Optimizer web interface for a wXa-203 router. The top navigation bar includes Home, Services, Status, System, Network (selected), Statistics, and Logout. Below the navigation is a sub-menu with Interfaces, WiFi (selected), DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, and PPP. The main content area is titled "radio0: Master 'wXa-203-80f8'" and "Wireless Network: Master 'wXa-203-80f8' (wlan0)". A note states: "The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration." The "Device Configuration" section contains tabs for General Setup (selected) and Advanced Settings. Under General Setup, the ESSID is set to "wXa-203-80f8", Mode is "Access Point", and the Network dropdown shows "lan:" selected. Other fields include Operating frequency (N, Channel 11, 20 MHz) and Transmit Power (20 dBm). The "Interface Configuration" section has tabs for General Setup (selected), Wireless Security, and MAC-Filter. Under General Setup, the ESSID is set to "wXa-203-80f8", Mode is "Access Point", and the Network dropdown shows "lan:" selected. Other fields include Hide ESSID and WMM Mode. At the bottom are Back to Overview, Reset, Save, and Save & Apply buttons. The footer notes: "Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)".

1. Enter the new wireless network name in ESSID field.

2. Click <Save & Apply>.

This procedure changes the name for the Wi-Fi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the network name that will appear in the wireless network list. This name does not change the router superadmin or admin name when logging in to access the Optimizer user interface.

9.5. Firewall

Requires “superadmin” login.



CAUTION: Turning off the firewall and modify the default state will leave you vulnerable to unwanted traffic and potential for excessive airtime overages. Ports open to the Internet on satellite systems that have public IP addresses are vulnerable to attackers that run dictionaries trying to guess usernames and passwords on the router. These dictionary attacks, at best, can result in large amounts of accounted traffic; and, at worst, they are a security breach that could endanger communications. Systems open to the public internet must take special precautions to secure the router from intrusion and overages. By modifying the default state of the Optimizer Firewall and proceeding forward you acknowledge these risks.

The Firewall allows you to control network traffic flow, allow port forwarding for remote access, has a table of pre-defined traffic rules, and allows you to edit existing rules and create new rules. Most installations do not require any firewall.

9.5.1. Firewall General Settings

Use this screen to create and edit Firewall zones. Each Firewall Zone can have its own firewall rules. Each Interface must be assigned a Firewall Zone.

The screenshot shows the Optimizer software interface for managing Firewall zones. At the top, there are tabs for Home, Services, Status, System, Network, Statistics, and Logout. Under the Network tab, there are sub-tabs for Interfaces, WiFi, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall (which is selected), and PPP. Below these tabs, there are links for General Settings, Port Forwards, Firewall Rules, IPset, and IP Proxy. The main content area is titled "Firewall - Zone Settings". It contains two sections: "General Settings" and "Zones".

General Settings:

- Enable SYN-flood protection: checked (indicated by a blue checkmark).
- Drop invalid packets: unchecked (indicated by a grey square).
- Input: dropdown menu set to "reject".
- Output: dropdown menu set to "accept".
- Forward: dropdown menu set to "reject".

Zones:

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	Action
ppp: ppp: → REJECT	reject	accept	reject	checked	unchecked	Edit Delete
cap: (empty) → ACCEPT	accept	accept	accept	unchecked	unchecked	Edit Delete
lan: lan: → ppp wan	reject	accept	reject	unchecked	unchecked	Edit Delete
wan: wan: → REJECT	accept	accept	reject	checked	unchecked	Edit Delete

At the bottom of the interface, there are buttons for "Reset", "Save", and "Save & Apply".

It is important to understand the following before considering modifications:

Input: access to the router itself.

Output: access to the “lan”. DO NOT MODIFY.

Forward: pass traffic thru the router via an interface and out of the router. If Forward is allowed you must configure the Inter-Zone Forwarding.

Accept: allows traffic unless there is a Rule to block it.

Reject: block traffic unless there is a Rule to allow it. An error is displayed to the end user.

Drop: this setting drops the traffic with no indication to the end user.

The router is shipped to you with several Firewall Zones configured and interfaces assigned to them:



The “ppp” firewall zone has only the ppp interface assigned to it. This is the zone for dialup connections. In this default configuration, only Output traffic is allowed. Input and Forwarded traffic are rejected.



The “cap” firewall zone is reserved for Optimizer routers that have Captive Portal available. Captive Portal is not available on the Optimizer or Optimizer Voice. If Captive Portal to restrict Crew Internet Access is required, please see your service provider about the Optimizer Premier.



The “lan” firewall zone has the lan interface assigned to it. This is the zone for the internal local network. In this default configuration, only Output traffic is allowed.



The “wan” firewall zone has the wan interface assigned to it. This is the zone for satellite connections and Wi-Fi extenders. In this default configuration, only Output traffic is allowed.

9.5.2. Add a Firewall Zone

To create a new Firewall Zone, select the <Add> icon on the General Settings page.

General Settings

- Enable SYN-flood protection:
- Drop invalid packets:
- Input:
- Output:
- Forward:

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	Actions
ppp: ppp: → [REJECT]	reject ↗	accept ↗	reject ↗	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
cap: (empty) → [ACCEPT]	accept ↗	accept ↗	accept ↗	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
lan: lan: → ppp wan	reject ↗	accept ↗	reject ↗	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
wan: wan: → [REJECT]	accept ↗	accept ↗	reject ↗	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	Actions
lan: lan: → ppp wan	reject ↗	accept ↗	reject ↗	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
wan: wan: → [REJECT]	accept ↗	accept ↗	reject ↗	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Optimizer | wXa-203 v2.61 | Load: 1.05 1.03 0.83

Home Services Status System Network Statistics Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP

General Settings Port Forwards Firewall Rules IPset IP Proxy

Firewall - Zone Settings - Zone "newzone"

Zone "newzone"

This section defines common properties of "newzone". The **input** and **output** options set the default policies for traffic entering and leaving this zone while the **forward** option describes the policy for forwarded traffic between different networks within the zone. **Covered networks** specifies which available networks are members of this zone.

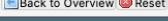
General Settings Advanced Settings

Name	newzone
Input	reject
Output	accept
Forward	reject
Masquerading	<input type="checkbox"/>
MSS clamping	<input type="checkbox"/>
Covered networks	<input type="checkbox"/> lan:   <input type="checkbox"/> ppp:   <input type="checkbox"/> wan:   <input type="checkbox"/> wan6:   <input type="checkbox"/> create: <input type="text"/>

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. **Destination zones** cover forwarded traffic originating from "newzone". **Source zones** match forwarded traffic from other zones targeted at "newzone". The forwarding rule is **unidirectional**, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Allow forward to <i>destination zones</i> :	<input type="checkbox"/> cap: (empty) <input type="checkbox"/> lan: lan:   <input type="checkbox"/> ppp: ppp:   <input type="checkbox"/> wan: wan:  
Allow forward from <i>source zones</i> :	<input type="checkbox"/> cap: (empty) <input type="checkbox"/> lan: lan:   <input type="checkbox"/> ppp: ppp:   <input type="checkbox"/> wan: wan:  

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Enter the desired General and Advanced Settings. Click <Save & Apply>.

9.5.3. Port Forwards

To allow remote access to a specific computer or service within the private LAN requires Port forwarding.

The screenshot shows the Optimizer web interface with the following details:

- Header:** Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 0.93 | Changes: 0
- Navigation:** Home, Services, Status, System, Network, Statistics, Logout | Firewall, PPP
- Sub-navigation:** Interfaces, Wifi, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, PPP | General Settings, Port Forwards, Firewall Rules, IPset, IP Proxy
- Section:** Firewall - Port Forwards
- Description:** Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.
- Table:** Port Forwards

Name	Match	Forward to	Enable Sort
This section contains no values yet			

- Form:** New port forward:
Name: New port forward | Protocol: TCP+UDP | External zone: cap | External port: cap | Internal zone: cap | Internal IP address: cap | Internal port: Add
- Buttons:** Save, Save & Apply, Reset
- Footer:** Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

This page shows a list of the enabled port forwards configured. To add a new port forward, enter the desired parameters and click <Add>. To save the configuration, click <Save & Apply>. The new port forward will appear in the list.

9.5.4. Firewall Rules

This page is the firewall traffic rules table. The table includes all the firewall rules on the router. If you are using the Optimizer with XGate (or other RedPort certified email service) for email and web compression, there is no need to modify this page.

If you have a specific need, you can Add, Edit and Delete firewall rules.

Traffic Rules

Name	Match	Action	Enable	Sort
BLOCK WAN DO_NOT MODIFY	Any traffic From any host in wan To any router IP on this device	Discard input	<input type="checkbox"/>	
ALL DO_NOT MODIFY	Any traffic From any host in any zone To any host in any zone	Accept forward	<input type="checkbox"/>	
PASS DNS DO_NOT MODIFY	Any UDP From any host in any zone To any host, port 53 in any zone	Accept forward	<input type="checkbox"/>	
DNS DO_NOT MODIFY	Any UDP From any host in any zone To any router IP at port 53 on this device	Accept input	<input type="checkbox"/>	
HTTP DO_NOT MODIFY	Any TCP From any host in any zone To any host, port 80 in any zone	Accept forward	<input type="checkbox"/>	
HTTPS DO_NOT MODIFY	Any TCP From any host in any zone To any host, port 443 in any zone	Accept forward	<input type="checkbox"/>	
FTP DO_NOT MODIFY	Any TCP From any host in any zone To any host, ports 20-21 in any zone	Accept forward	<input type="checkbox"/>	

Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	<input type="text"/>

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
New SNAT rule	lan	wan	-- Please choose	<input type="text"/>

By default, the router is shipped to you with seven rules that all say DO NOT MODIFY. They are: BLOCK WAN, ALL, PASS DNS, DNS, HTTP, HTTPS and FTP.

The BLOCK WAN rule is designed to prevent you from locking yourself out of the router as you perform your initial configuration.

The remaining rules, when Enabled, allow that particular traffic to pass through the firewall. All the firewall rules can easily be enabled (checked) or disabled (unchecked).

The rule name “ALL”, when enabled, means the firewall is totally open and all traffic goes straight through the firewall. To disable the rule, uncheck it, scroll to the bottom of the page and click <Save & Apply>. With the ALL rule disabled, the remaining rules spring into action, if enabled.

Rules are evaluated from top to bottom. As soon as traffic hits a rule that matches, it will stop. For example, if you want to allow all traffic except http traffic:

- Disable (uncheck) the first rule “ALL-DO NOT MODIFY”. This forces the remaining “enabled” rules to take precedent.
- Disable (uncheck) the rule “HTTP-DO NOT MODIFY”. This blocks http traffic from passing through the firewall.

With the ALL rule disabled (unchecked) you can enable/disable the others very quickly. The next one is DNS. Do you want DNS? Yes (checked), No (unchecked). Do you want http? Yes (checked), No (unchecked), etc. You can also create a custom rule.

9.5.4.1. Create a Custom Firewall Rule

Optimizer | wXa-203 v2.61 | Load: 1.00 1.00 0.97 Changes: 0

Home Services Status System Network Statistics Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP

General Settings Port Forwards Firewall Rules IPset IP Proxy

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Name	Match	Action	Enable	Sort
BLOCK WAN DO_NOT MODIFY	Any traffic From any host in wan To any router IP on this device	Discard input	<input type="checkbox"/>	
ALL DO_NOT MODIFY	Any traffic From any host in any zone To any host in any zone	Accept forward	<input type="checkbox"/>	
PASS DNS DO_NOT MODIFY	Any UDP From any host in any zone To any host, port 53 in any zone	Accept forward	<input type="checkbox"/>	
DNS DO_NOT MODIFY	Any UDP From any host in any zone To any router IP at port 53 on this device	Accept input	<input type="checkbox"/>	
HTTP DO_NOT MODIFY	Any TCP From any host in any zone To any host, port 80 in any zone	Accept forward	<input type="checkbox"/>	
HTTPS DO_NOT MODIFY	Any TCP From any host in any zone To any host, port 443 in any zone	Accept forward	<input type="checkbox"/>	
FTP DO_NOT MODIFY	Any TCP From any host in any zone To any host, ports 20-21 in any zone	Accept forward	<input type="checkbox"/>	

Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	<input type="text"/>

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Source NAT:

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
New SNAT rule	lan	wan	-- Please choose!	

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Scroll down to the bottom of the page to the section “New forward rule”. Click <Add and edit>.

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Source NAT

Optimizer | wXa-203 v2.61 | Load: 1.01 1.02 1.00 Unsaved Changes: 5

[Home](#) [Services](#) [Status](#) [System](#) **Network** [Statistics](#) [Logout](#)

[Interfaces](#) [Wifi](#) [DHCP and DNS](#) [Hostnames](#) [Static Routes](#) [Diagnostics](#) **Firewall** [PPP](#)

[General Settings](#) [Port Forwards](#) **Firewall Rules** [IPSet](#) [IP Proxy](#)

Firewall - Traffic Rules - (Unnamed Rule)

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	<input checked="" type="checkbox"/> Disable
Name	<input type="text"/>
Restrict to address family	<input type="button" value="IPv4 and IPv6"/>
Protocol	<input type="button" value="TCP+UDP"/>
Match ICMP type	<input type="button" value="any"/>
Source zone	<input type="radio"/> Any zone <input type="radio"/> cap: (empty) <input checked="" type="radio"/> lan: lan: <input type="radio"/> newzone: (empty) <input type="radio"/> ppp: ppp: <input type="radio"/> wan: wan:
Source MAC address	<input type="button" value="any"/>
Source address	<input type="button" value="any"/>
Source port	<input type="button" value="any"/>
Destination zone	<input type="radio"/> Device (input) <input type="radio"/> Any zone (forward) <input type="radio"/> cap: (empty) <input type="radio"/> lan: lan: <input type="radio"/> newzone: (empty) <input type="radio"/> ppp: ppp: <input checked="" type="radio"/> wan: wan:
Destination address	<input type="button" value="any"/>
Destination port	<input type="button" value="any"/>
Action	<input type="button" value="accept"/>
Extra arguments	<input type="text"/> <small>(*) Passes additional arguments to iptables. Use with care!</small>

[Back to Overview](#) [Reset](#) [Save](#) [Save & Apply](#)

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Here you can give the new rule a name, specify the protocol, restrict the rule to a certain zone, identify the source IP address, the destination IP address, port numbers. etc.

This is standard firewall convention. Once the rule is created, click <Save & Apply>. Place the rule where you want it on the traffic rule list using the Sort column arrows for up and down.

This is a full-featured firewall that you can customize to meet your needs.

See IP Sets section of this document for creating block and allow rules by domain name instead of IP address.

9.5.5. IP Sets

Use IP sets for cloud-based services where standard firewall rules will not work. This allows block and allow rules by domain name instead of by IP address. IP sets rules take priority over anything in the firewall.

The screenshot shows the Optimizer web interface for managing IP sets. The top navigation bar includes Home, Services, Status, System, Network, Statistics, Logout, and Firewall tabs. Under Firewall, the sub-tabs are Interfaces, Wifi, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall Rules, IPset (which is selected), and IP Proxy. The main content area is titled "IP Sets" and contains the following text: "Block, Allow, or Define groups of domains to be used by the firewall and/or the load balancer. High priority rules apply before user defined firewall rules while low priority rules apply after." Below this is a table with columns: IPset Name, Action, Priority, and Domains. A note states "This section contains no values yet". At the bottom of the table is an "Add" button. At the very bottom of the page is a footer with "Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)" and "Changes: 0".

Click <Add> to create a new IP set rule.

Action Definitions:

- Block: rejects the domain
- Pass: allows the domain

You can group multiple domain names into one IP set rule.

9.5.6. Allow WhatsApp Configuration

Navigate to the <Network> tab, under <Firewall> tab, and then the <IPset> tab.

The screenshot shows the Optimizer IP Sets configuration page. At the top, there is a header bar with tabs for Home, Services, Status, System, Network, Statistics, Logout, Firewall, and IPset. The IPset tab is selected. Below the header, there is a section titled "IP Sets" with a sub-section "IP Set Name". A note says: "Block, Allow, or Define groups of domains to be used by the firewall and/or the load balancer. High priority rules apply before user defined firewall rules while low priority rules apply after." A table is present with columns: IPSet Name, Action, Priority, and Domains. The table has one row with "Unique Name" and "Filtering Action". The "Priority" column has a dropdown menu with "Filter Priority". The "Domains" column has a text input field with "Domain(s) to Filter" and a note "This section contains no values yet". There are "Add" and "Delete" buttons. At the bottom, there are "Save" and "Save & Apply" buttons.

1. Click <Add> to create a new IP set rule.

The screenshot shows the Optimizer IP Sets configuration page with two new IP set rules added. The table now has four rows. The first row is a header with "Unique Name", "Action", "Priority", and "Domains". The second row is for "WhatsApp1" with "Pass" action, "High" priority, and domains "whatsapp.com" and "whatsapp.net". The third row is for "WhatsApp2" with "Pass" action, "High" priority, and domains "whatsapp.com" and "whatsapp.net". Both rows have "Delete" buttons. The "Add" button is still available. At the bottom, there are "Save" and "Save & Apply" buttons.

2. For WhatsApp you will be adding two new IP set rules. Give each a unique name such as WhatsApp1 and WhatsApp2.
3. For each new IP set rule give each two Domains of whatsapp.com and whatsapp.net.
4. Click <Save & Apply>.
5. Click on the <Firewall Rules> tab.

Optimizer | wXa-203 v2.61 | Load: 1.08 1.03 1.01 Changes: 0

Home Services Status System Network Statistics Logout

Interfaces WiFi DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP

General Settings Port Forwards Firewall Rules IPset IP Proxy

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Name	Match	Action	Enable	Sort
BLOCK WAN DO_NOT MODIFY	Any traffic From any host in wan To any router IP on this device	Discard input	<input type="checkbox"/>	
ALL DO_NOT MODIFY	Any traffic From any host in any zone To any host in any zone	Accept forward	<input type="checkbox"/>	
PASS DNS DO_NOT MODIFY	Any UDP From any host in any zone To any host, port 53 in any zone	Accept forward	<input type="checkbox"/>	
DNS DO_NOT MODIFY	Any UDP From any host in any zone To any router IP at port 53 on this device	Accept input	<input checked="" type="checkbox"/>	
HTTP DO_NOT MODIFY	Any TCP From any host in any zone To any host, port 80 in any zone	Accept forward	<input type="checkbox"/>	
HTTPS DO_NOT MODIFY	Any TCP From any host in any zone To any host, port 443 in any zone	Accept forward	<input type="checkbox"/>	
FTP DO_NOT MODIFY	Any TCP From any host in any zone To any host, ports 20-21 in any zone	Accept forward	<input type="checkbox"/>	
-	Any traffic From any host in lan To any host in wan	Accept forward	<input checked="" type="checkbox"/>	

Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	<input type="text"/>

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
New SNAT rule	lan	wan	-- Please choose	<input type="text"/> Do not rewrite

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

6. Click the checkbox for the DNS traffic Rule (not the Pass DNS traffic Rule).

PASS DNS DO_NOT MODIFY	Any UDP From any host in any zone To any host, port 53 in any zone	Accept forward	<input type="checkbox"/>	
DNS DO_NOT MODIFY	Any UDP From any host in any zone To any router IP at port 53 on this device	Accept input	<input checked="" type="checkbox"/>	
HTTP DO_NOT MODIFY	Any TCP From any host in any zone To any host, port 80 in any zone	Accept forward	<input type="checkbox"/>	

7. Click <Save & Apply>.

8. Click on the <Network> tab and then click on the <DHCP and DNS> tab.

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#) for [NAT](#) firewalls

Server Settings

General Settings		Resolv and Hosts Files	TFTP Settings	Advanced Settings
<input checked="" type="checkbox"/> Don't forward DNS -Requests without DNS-Name				
<input checked="" type="checkbox"/> This is the only DHCP in the local network				
<input type="checkbox"/> Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only				
<input type="checkbox"/> Local domain suffix appended to DHCP names and hosts file entries				
<input type="checkbox"/> Write received DNS requests to syslog				
<input type="text" value="example.org/10.1.2.3"/> <input type="checkbox"/> List of DNS servers to forward requests to				
<input type="checkbox"/> Discard upstream RFC1918 responses				

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Aarons-MBP	192.168.10.124	68:fe:f7:16:95:f6	10h 29m 47s

Active DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining
There are no active leases.			

Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the [Add](#) Button to add a new lease entry. The [MAC-Address](#) indentifies the host, the [IPv4-Address](#) specifies to the fixed address to use and the [Hostname](#) is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
This section contains no values yet			

[Add](#) [Save](#) [Save & Apply](#)

Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

9. Under the “Server Settings” section on the <General Settings> tab, add four new “DNS forwardings”:

- /whatsapp.com/8.8.8.8
- /whatsapp.com/8.8.4.4
- /whatsapp.net/8.8.8.8
- /whatsapp.net/8.8.4.4

10. Click <Save & Apply>.

11. Click on the <Resolve and Host Files> tab under the “Server Settings” section, and click the checkbox associated with “Ignore resolve file”.

12. Click <Save & Apply>.

10. Statistics

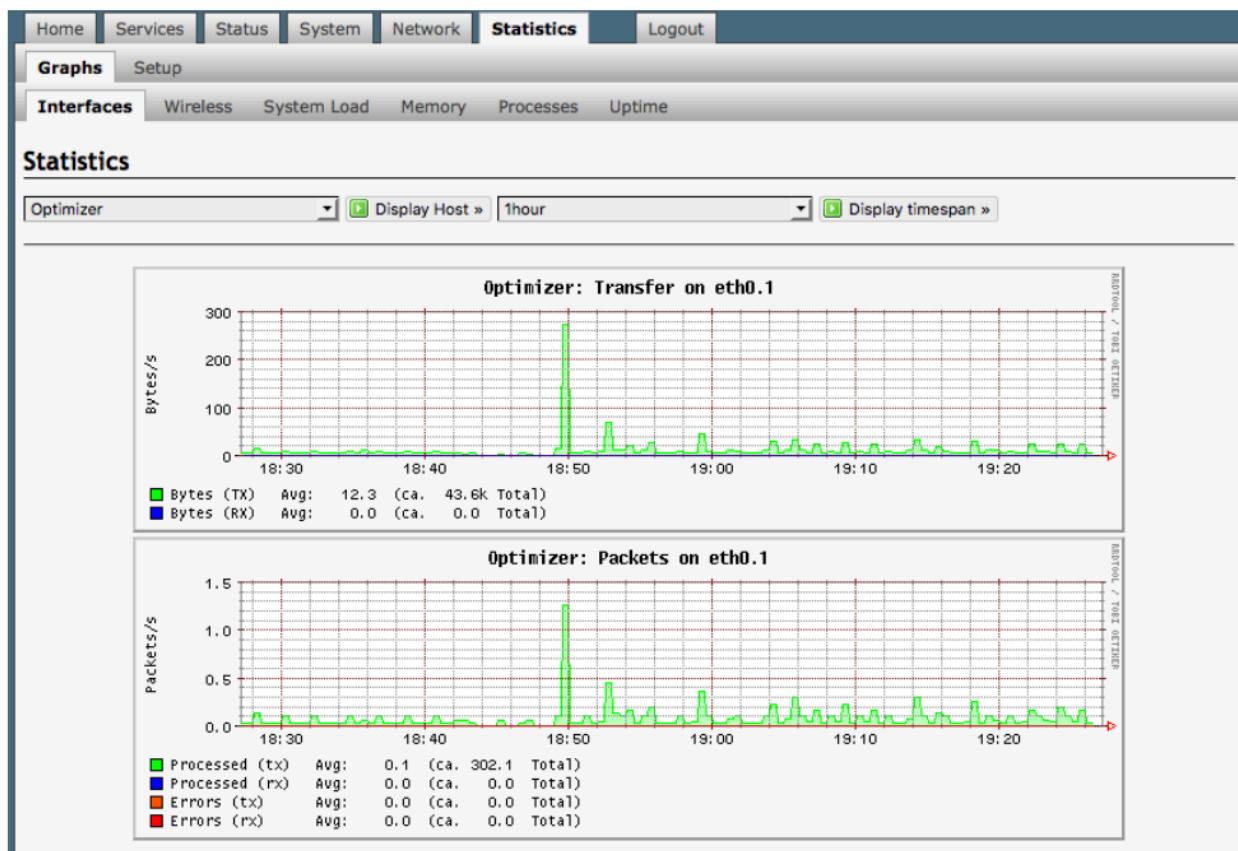
Requires "superadmin" login

The statistics package uses [Collectd](#) to gather data and [RRDtool](#) to render diagram images. You can [install](#) additional collectd-mod-* plugins to enable more statistics.

10.1. Graphs

Similar to the Realtime Graphs in the Status tab, Statistics Graphs shows usage over a specific timespan.

To modify the timespan, use the down arrow next to <Display timespan>, then select <Display timespan> to view the graph.



11. Using Optimizer with Satellite Handsets

12. Product Warranty and Support Information

12.1. Product Warranty Information

RedPort hardware carries a Limited 1-year manufacturer warranty against defects from the date of sale.

What is covered by this limited hardware warranty?

This limited hardware warranty covers defects in materials and workmanship in your RedPort-branded hardware products.

What is not covered by this limited hardware warranty?

This limited hardware warranty does not cover:

- Software, including without limitation, the operating system and software added to the RedPort -branded hardware products through our factory-integration system, third-party software or the reloading of software
- Non-RedPort-branded products and accessories
- Problems that result, directly or indirectly, from:
 - External causes such as accident, abuse, misuse, water ingress, or problems with electrical power.
 - Servicing not authorized by RedPort.
 - Usage that is not in accordance with product instructions.
 - Failure to follow the product instructions or failure to perform preventive maintenance.
 - Using accessories, parts or components not supplied by RedPort.
 - Products with missing or altered service tags or serial numbers
 - Products for which RedPort has not received payment
 - Normal wear and tear

12.2. Product Support Information

RedPort agrees to provide initial customer assistance, up to thirty (30) minutes at no charge. It is recommended that a customer has reasonable knowledge of basic computer and software setup procedures for the initial installation.

Feature	Description	Details For Warranty
Remote Email Support	Customer may contact their RedPort dealer or support@redportglobal.com to report an issue.	1 year included in RedPort hardware purchase
Remote Live Technical Support	Customer may contact their RedPort dealer or support@redportglobal.com to report an issue.	Up to 30 minutes of free phone support included during warranty period. Additional time available for purchase.

RedPort Company Information

For product orders, support or returns, please contact:

Phone: +1-865-379-8723

Email: info@redportglobal.com

Sales: sales@redportglobal.com

Web: redportglobal.com

RedPort Address

RedPort
3224 Wrights Ferry Road
Louisville, TN 37777
United States of America