RedPort

GMN
Global Marine
NETWORKS

Optimizer Voice

Advanced User's Guide
for Installers/Network Administrators

RedPort Router:
wXa-153 (Optimizer Voice)

RedPort™

Table of Contents

Copyright © Global Marine Networks, LLC

Copyright © Global Marine Networks, LLC

Copyright © Global Marine Networks, LLC

Revision History

Date	Revision	Author
July 15, 2015	Initial Release	D. Brickhouse
June 15, 2016	version 2.0	D. Brickhouse
September 22, 2016	version 2.1	D. Brickhouse

1.0 About this Guide

This guide is intended for installers and network administrators of the RedPort Optimizer Voice wXa-153 routers. It features only those sections of the user interface that require configuration for a specific service or may need to be accessed to perform a specific function.

During normal daily operation, there is no need to access the full user interface that you see here. A separate document is designed for use by the onsite administrator that includes the login to the Home Page for access to the common tasks that will be used locally such as creating and managing crew email accounts. *See the Optimizer Voice Onsite Administrator User Guide for details.*

For information regarding the installation of the hardware, please see the *RedPort Optimizer Voice QuickStart Guide*.

wXa refers to the webXaccelerator by RedPort, a trademark of Global Marine Networks, LLC.

2.0 Introduction to Optimizer Voice

Global Marine Networks (GMN), the leaders in advancing satellite data speeds and services, helps Fixed and Mobile Satellite Services providers and their customers by offering the industry's fastest, most reliable and easy-to-use email, web, VoIP and other hardware and software services to maritime, oil and gas, first responder and business continuity users.

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

Optimizer Voice is a satellite WiFi 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 email and web compression, track your location via GPS, and provide routing, filtering and security.

2.1 Key Features

Designed specifically for use with satellite broadband terminals:

- Compatible with virtually any IP-based satellite broadband terminal.
- Replaces a standard router that is typically added to any satellite broadband installation.
- Powerful firewall accommodates virtually 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 RedPort Email Service
- 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 WiFi.
- Supports voice calling and SMS messages using smartphones connected to the local network.

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. *See Chapter 5.7.*

- **SMS Messaging** - allows smartphones to send sms messages to others on the local area network for free, or over the satellite link at stardard satellite airtime rates. Requires a supported satellite terminal. *See Chapter 5.3.*

- **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. *See Chapter 5.6.*

- **GSM Compatibility** - allows Internet connectivity via your GSM modem or cell phone with your own SIM card. *See Chapter 8.8.2.*

- **File Sharing** - Network Shares allows the sharing of files among Windows and Mac computers via WiFi, without the requirement of a wired local network of computers. *See Chapter 5.8.*

2.3 Premium Services Available

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

RedPort Email – is a multi-user satellite email service. Crew and/or passengers can access their RedPort Email account via smartphones, tablets or computers. See the *RedPort Email Administrator's Guide* for more information about this service. *See Chapter 5.2 and the Optimizer RedPort Email Guide.*

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. *See Chapter 5.1 and the RedPort Optimizer Voice QuickStart Guide for more information.*

GPS Tracking - Using a GPS-enabled device, submit position reports to a central database for viewing on the tracking website. *See Chapter 5.4.*

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. *See Chapter 5.7.7.*

3.0 Important Things to Know Before Getting Started

3.1 More Than Just a Router

The Optimizer Voice 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 being accessed by the users. You also have the option to communicate upstream to a compression proxy server.

- 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.

3.2 Designed Use of the Optimizer Voice

This router is suitable for two distinctly different audiences:

3.2.1 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.

3.2.2 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 Voice Onsite Administrator Guide.*

3.3 How It Works At First Launch (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 multii-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). See Section* 3.4, *How Data Flows Through the Router* to determine the customization required to best meet your needs.

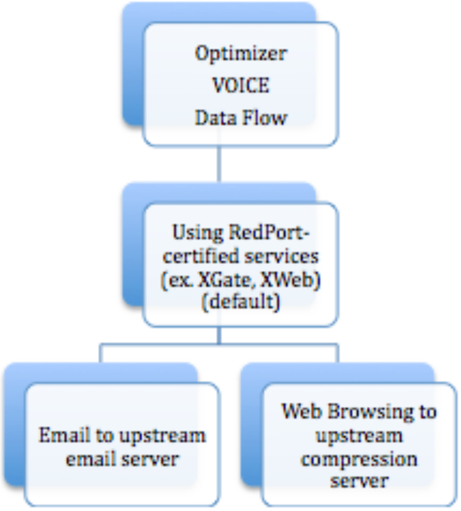
Best Practice is to have a knowledgeable technician (someone who knows about proxy servers and routers) go through and generate a custom configuration. In a fleet environment, this custom configuration can be recorded and used on other Optimizer Voice routers within the organization.

3.4 How Data Flows Through the Router

It is important to understand how data flows through the router so you can customize your configuration.

3.4.1 Default Configuration

The default configuration is:
Internal Transparent Proxy for http URL and content filtering - disabled
Web Compression - disabled
Firewall - closed, allows Internet access only via RedPort-certified email or web account
DNS - closed
RedPort Email - disabled
SMS, for compatible satellite devices - disabled
GPS Tracking - disabled
Voice Capability, for compatible satellite devices - disabled
RedPort VoIP - disabled
IMPORTANT NOTE: Prior to installation, review Chapter 4.3.1 How to Secure Your Router.


Optimizer VOICE Data Flow
Using RedPort-certified services (ex. XGate, XWeb) (default)
Email to upstream email server
Web Browsing to upstream compression server

In its default state, without any modifications, one primary account holder at-a-time can connect to send/receive email or web browse using a RedPort-certified email service like XGate or web browsing service like XWeb.

All email requests go directly to the upstream email server. The mail is downloaded to the end-users computer/device and then the mail is purged from the server. Limited mail filtering is possible thru the RedPort-certified email service program.

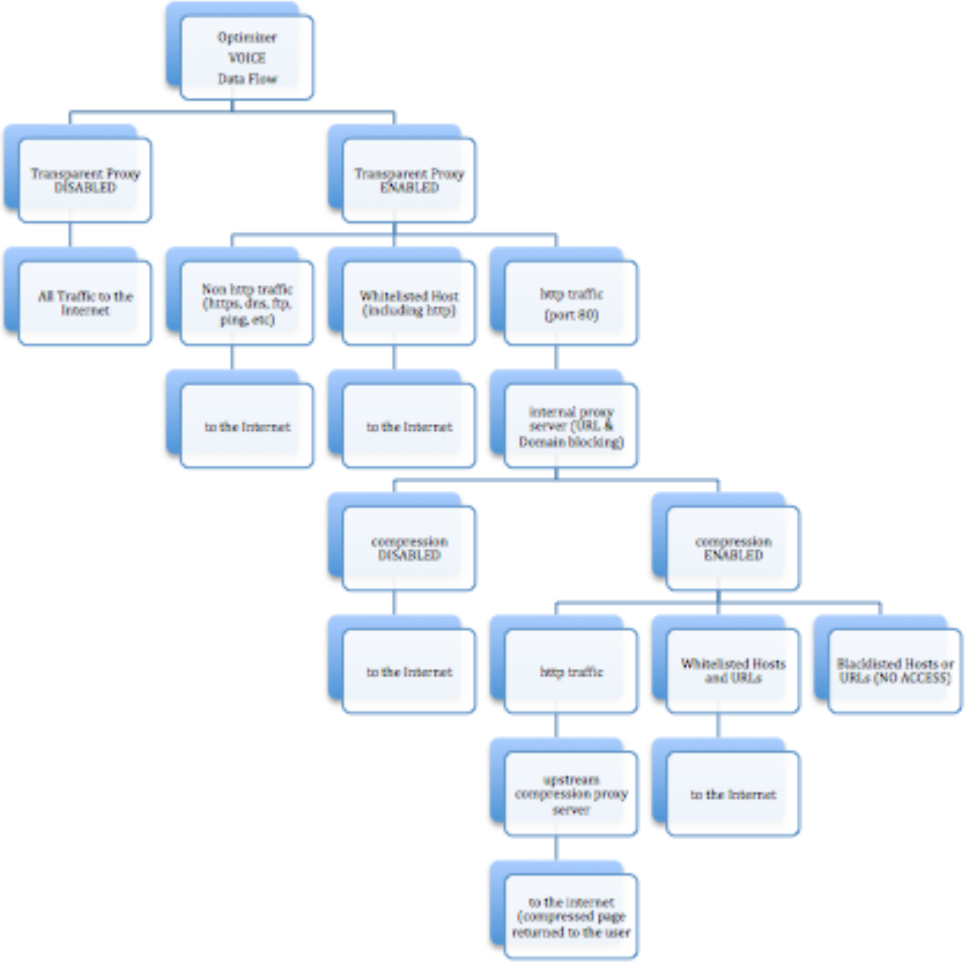
All web browsing requests go directly to the upstream compression server. Compressed webpages are returned to the end-user, whenever compression is possible. The end-user can set the compression level thru the RedPort-certified web service program. However, it is not possible to create any filters for content, to whitelist or blacklists hosts or URLs, or to designate sites to bypass content filters. Nor is it possible to set limits on usage.

The default state is designed for the single user that uses services like XGate and XWeb for email and web browsing and use the XGate Phone app on their smartphone for making voice calls.

Copyright © Global Marine Networks, LLC

3.4.2 Web Browsing without RedPort-Certified Service (XWeb)

In order to use the router for web browsing without XWeb service, you must first modify the firewall to allow traffic. *See Section 8.7.* ***IMPORTANT NOTE: Prior to installation, review Chapter 4.3.1 How to Secure Your Router.***


Optimizer
VOICE
Data Flow
Transparent Proxy DISABLED
Transparent Proxy ENABLED
All Traffic to the Internet
Non http traffic (https, dns, ftp, ping, etc)
Whitelisted Host (including http)
http traffic (port 80)
to the Internet
to the Internet
internal proxy server (URL & Domain blocking)
compression DISABLED
compression ENABLED
to the Internet
http traffic
Whitelisted Hosts and URLs
Blacklisted Hosts or URLs (NO ACCESS)
upstream compression proxy server
to the Internet
to the internet (compressed page returned to the user

With the firewall open and Transparent Proxy disabled by default, any user on the local network can browse the web without restrictions, limits, or, compression. All traffic goes straight to the Internet without any filtering.

If you ENABLE Transparent Proxy you can apply some filtering of content and whitelist or blacklist domains and URLs.

With Transparent Proxy ENABLED, data can then take one of three paths:

1. Non-http traffic bypasses the internal proxy server and goes straight to the Internet: https, dns lookups, ftp, ping, scp, etc. Since the firewall rules are totally open there is nothing blocking full access to the Internet.

2. Traffic to a Whitelisted Host *(See Section 5.1.2),* including http, goes straight to the Internet, bypassing the internal proxy server. If you whitelist a webserver, that traffic goes straight to the Internet, bypassing the internal proxy server, so there is no filtering. Typically you would not want to whitelist a webserver; however, you may want to whitelist a mail server, or a vpn

Copyright © Global Marine Networks, LLC

3. All http traffic (on port 80) that is not Whitelisted, and only http traffic (not https or secure traffic) is intercepted and redirected to the internal proxy server (Transparent Proxy). The internal proxy server does URL blocking and domain blocking. Also, the internal proxy server can speak to an upstream proxy server to provide compression (premium service--fees apply). Traffic through the internal proxy server can take one of several paths, dependent upon whether or not compression is enabled.

- If compression is DISABLED, http traffic goes straight to the Internet.

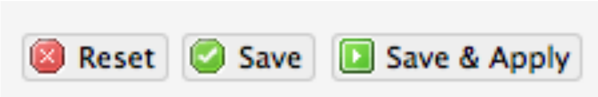
- If compression is ENABLED:
  - all http traffic goes to the upstream compression proxy server and returns a compressed page. Ads are stripped out, text is compressed, images are resampled and more. On average, you will experience 3-5x compression on http traffic, thereby increasing the speed of your connection and your effective per Mb cost of your connection.
  - Whitelisted Hosts or URLs bypass the upstream compression proxy server and go straight to the Internet, bypassing compression.
- Blacklisted Hosts or URLs have no Internet access, regardless of compression status.

3.5 Navigating the User Interface

Access to the user interface depends upon how you login to the router. There are two logins available: admin and superadmin. *See Chapter 4.1*.

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.

Copyright © Global Marine Networks, LLC

4.0 Getting Started - User Interface Access

In a typical situation, the Optimizer Voice 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)
- RedPort Email (additional fees may apply)
- GPS Tracking (additional fees may apply)
- RedPort VoIP for multi-user calls and SMS (additional fees may apply)

This guide is designed to help you understand how the router works so you can customize the configuration to meet your needs.

4.1 Access the Home page

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

1. Connect to the WiFi Hotspot created by the router using a PC. Connect to the WiFi Hotspot just like you would any other WiFi 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-153-XXXX' where 'XXXX' is the last four digits of the Optimizer Voice's Mac address.

Copyright © Global Marine Networks, LLC

For alternative Home Page access methods, see the *RedPort Optimizer Voice Installation Guide.*

2. Open any web browser on the computer and enter the URL:

http://192.168.10.1

The Optimizer Voice ships with two existing accounts:

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

4.1.1 Onsite Administrator Login (Admin)

Onsite Administrator: username=admin, password=webxaccess

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

- send/receive email (if email is enabled)
- manage crew email accounts (if email is enabled)
- monitor the system status
- reboot the router, if necessary
- change the router password for the admin account, if necessary

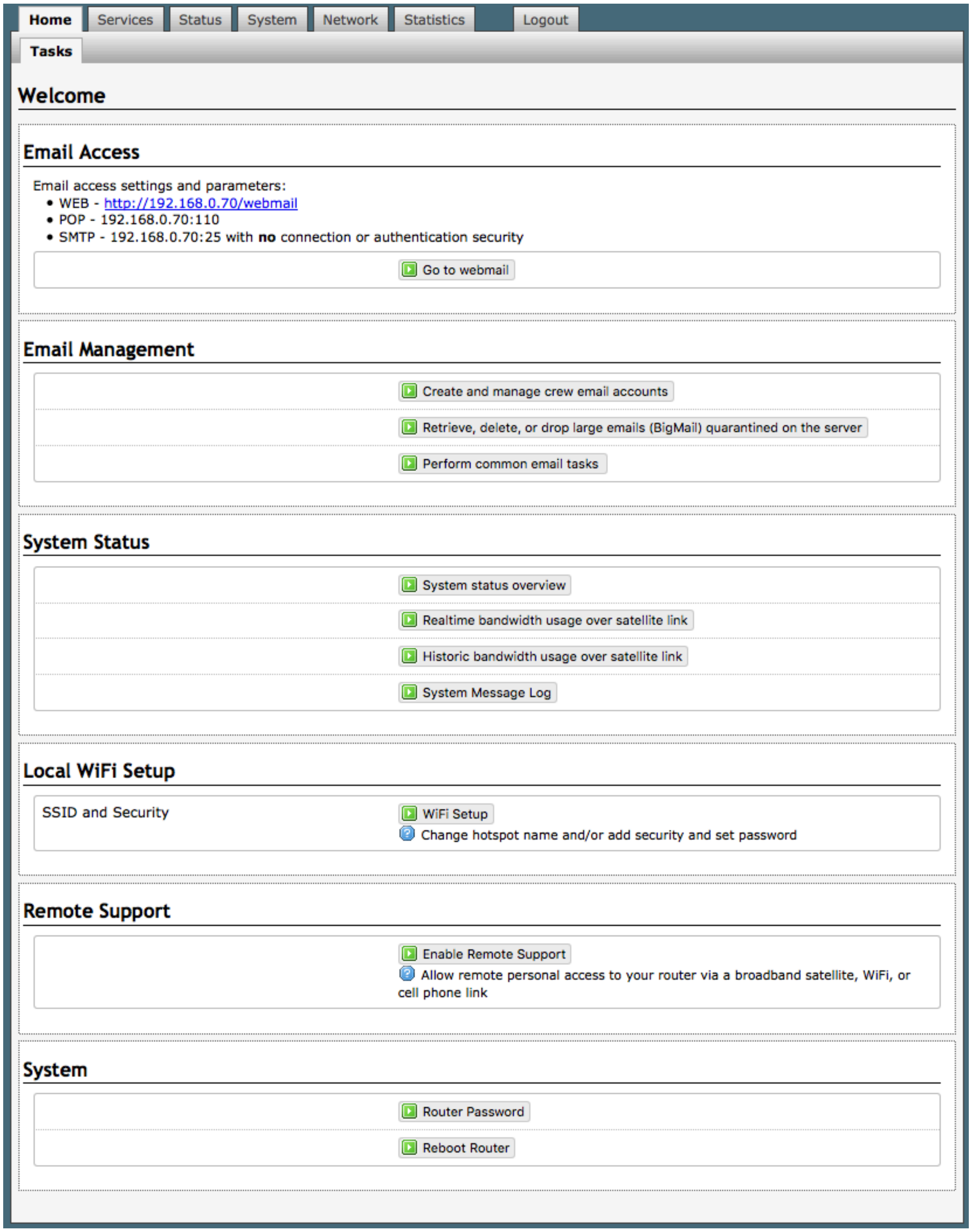
See the *Optimizer Voice Onsite Administrator Guide* for information in administering the most-used features of the Optimizer Voice.

4.1.2 Installer/Network Administrator Login (Superadmin)

Technician: 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:



Welcome

Email Access

Email access settings and parameters:

- WEB - http://192.168.0.70/webmail
- POP - 192.168.0.70:110
- SMTP - 192.168.0.70:25 with **no** connection or authentication security

Go to webmail

Email Management

Create and manage crew email accounts

Retrieve, delete, or drop large emails (BigMail) quarantined on the server

Perform common email tasks

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

Remote Support

Enable Remote Support

Allow remote personal access to your router via a broadband satellite, WiFi, or cell phone link

System

Router Password

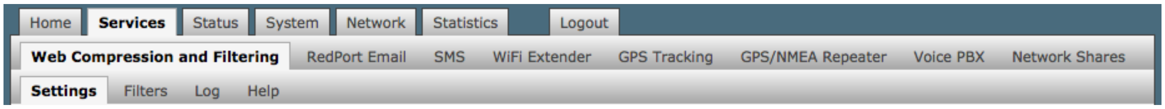
Reboot Router

This Home Page is the onsite administrator's gateway to the most used features. See the Optimizer Voice Onsite Administrator Guide for Home Page details and use.

Copyright © Global Marine Networks, LLC

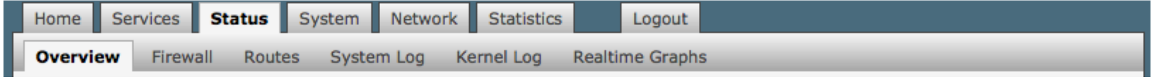
From the Home Page you have access to the remaining sections of the user interface.

Services: allows access to all the services available on the router.



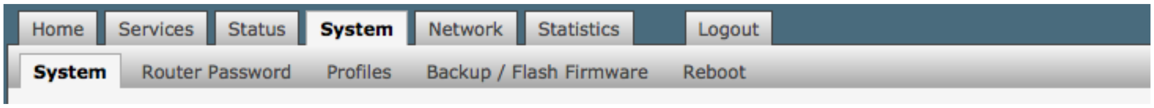
Each service is contained in its own tab under the Services section. This is where you will enable/disable the services and configure them for use.

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



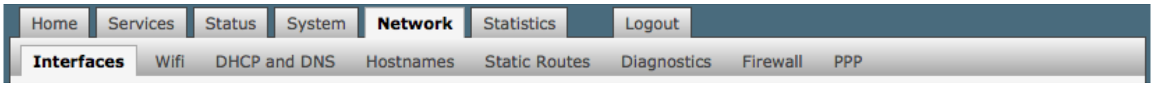
The System Log contains detailed information of the router's performance. It will report error messages and can be useful when troubleshooting connection issues. Realtime Graphs report how much data is being using by the different interfaces. All Status information is Read Only.

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



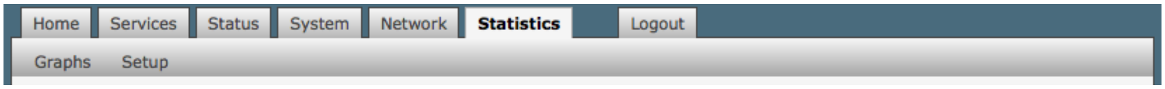
Use this section to set your time zone, change the 'admin' and/or 'superadmin' password, flash new firmware to the router, reboot the router if necessary. Profiles is a way to 'clone' the router configuration for use on another Optimizer Voice router.

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.



4.2 How to Use with Default Setup

We ship the router ready for use with a RedPort-certified compression email and/or web browsing account; Voice and SMS are 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 multii-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). See Section 3.4, How Data Flows Through the Router to determine the customization required to best meet your needs.

4.2.1 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-153-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.

4.2.2 Voice Calls

Voice is disabled by default but can be enabled for use with compatible satellite devices using standard satellite airtime. *See Section 5.7 for details on configuration and use of the Voice service.*

IMPORTANT NOTE: When you enable the Voice PBX it is listening on all ports. Without further configuration, this could leave you vulnerable to unwanted traffic. Please review Chapter 4.3.1 How to Secure Your Router.

4.2.3 SMS Messaging

SMS is disabled by default but can be enabled for use with compatible satellite devices using standard satellite airtime. *See Section 5.3* for details on configuration and use of the SMS Messaging service.

IMPORTANT NOTE: When you enable the SMS service it is listening on all ports. Without further configuration, this could leave you vulnerable to unwanted traffic. Please review Chapter 4.3.1 How to Secure Your Router.

4.3 Router Security***IMPORTANT***

If you modify the firewall from its default state you may have WAN ports open.

If you enable the Voice PBX, SMS messaging it is listenting on all ports.

If you enable RedPort Email, POP and SMTP are open to the WAN.

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.

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.

4.3.1 How to Secure Your Router***IMPORTANT***

First, confirm that the Disable anti-lock rule setting is "Unchecked" in System > System Settings. *(See Chapter 7.1)* 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 anti-lock 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. *See Chapter 7.2*.

If RedPort Email is enabled, the POP and SMTP servers are listening on ALL ports so they are open to the WAN, leaving them vulnerable. If you enable RedPort Email, you should configure the firewall to block all but desired email traffic. *See Chapter 8.7 - Network > Firewall*. Note that 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 (*see Chapter 5.7.1)* OR, you can leave it to listening on all interfaces and use a firewall rule to restrict traffic (*see Chapter 8.7Network > Firewall*). Note that 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. *See Chapter 7.1*.

Now you can Enable the BLOCK ALL from WAN firewall rule in Network > Firewall > Firewall Rules.

Copyright © Global Marine Networks, LLC

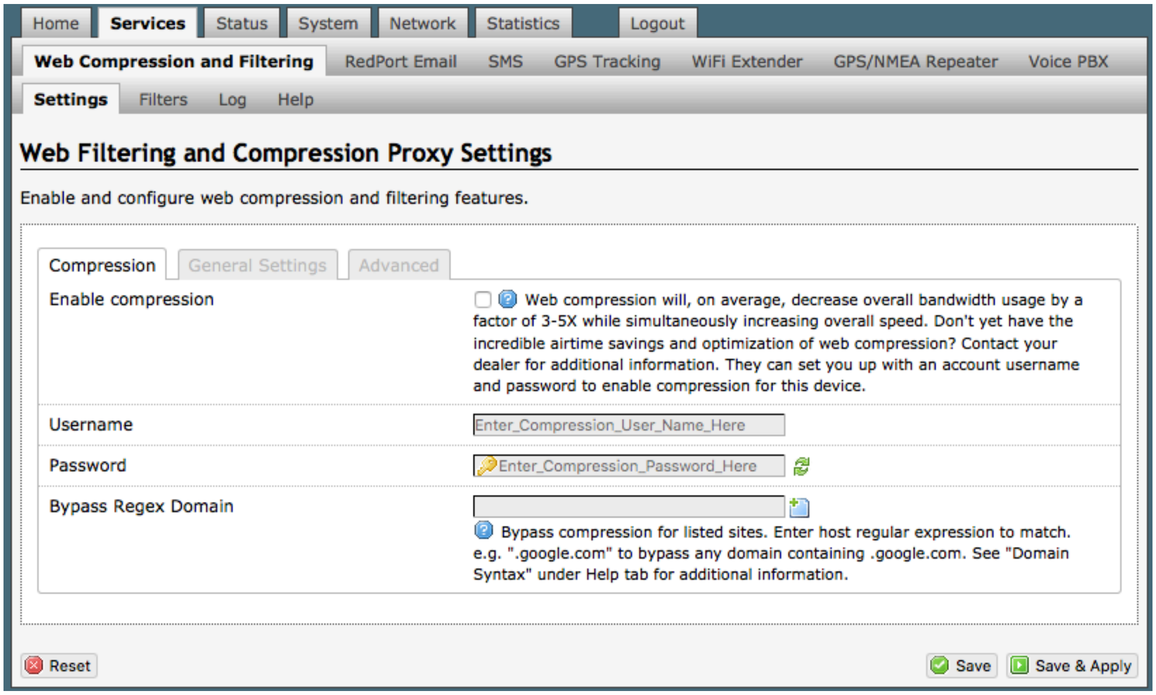
5.0 Services

5.1 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

5.1.1 Settings



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

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.

Username: Enter_Compression_User_Name_Here

Password: Enter_Compression_Password_Here

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.

5.1.1.1 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.

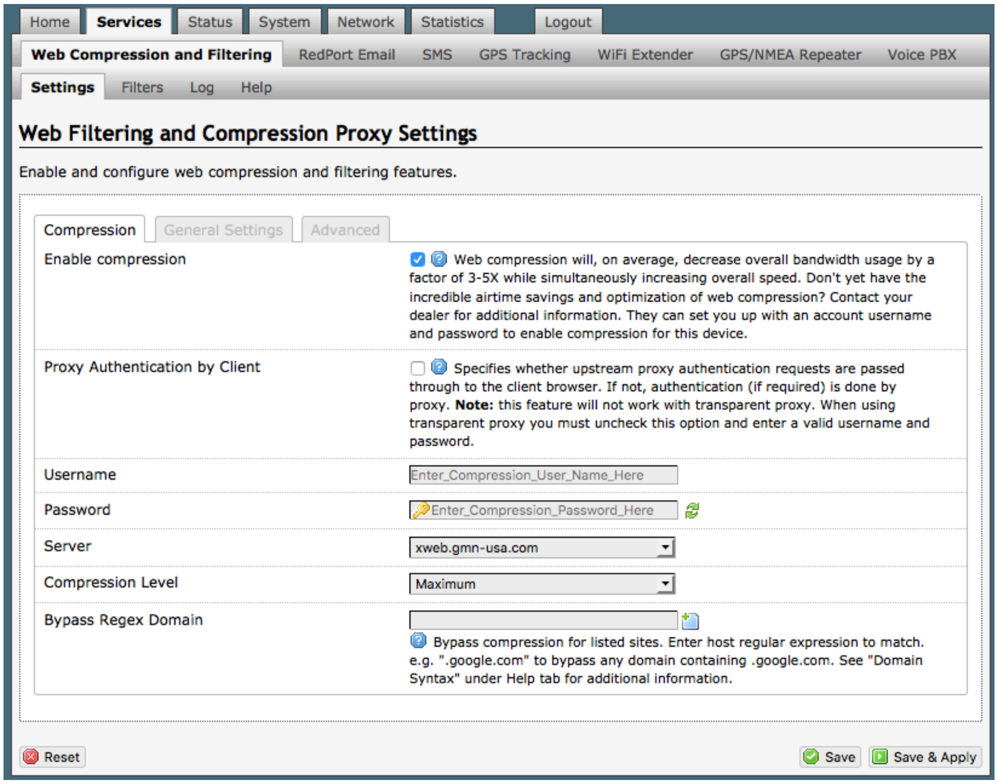
Enable Compression: If you have purchased Web Compression service, select the checkbox to Enable compression. The page will expand; see With Compression Enabled below.

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, select the Add icon . Proper syntax must be used to successfully bypass compression. See the Help tab for guidance and examples of using regular expressions.

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



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

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	Enter_Compression_User_Name_Here
Password	Enter_Compression_Password_Here
Server	xweb.gmn-usa.com
Compression Level	Maximum
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.

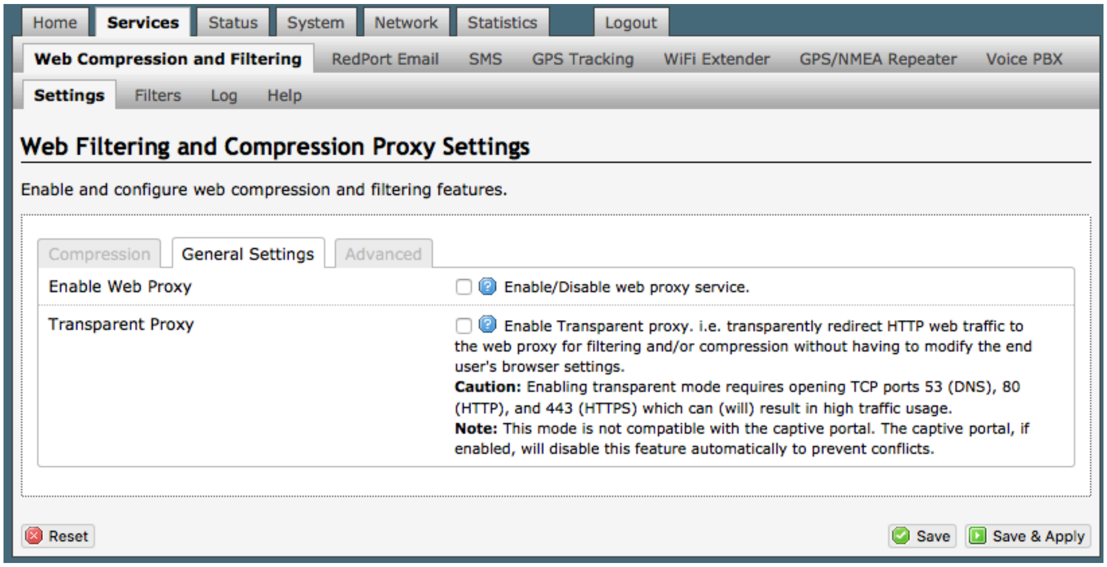
Proxy Authentication by Client: By default this is unchecked as it does not work with the Captive Portal enabled. In this state, unchecked, the upstream proxy server will login on your behalf. If this is checked, then the authentication happens at the user end, which means that when a user goes to any 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 selet "Maximum". Those on high data plans may prefer "Standard" or "Minimum".

5.1.1.2 General Settings

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.



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

Enable Web Proxy □ Enable/Disable web proxy service.

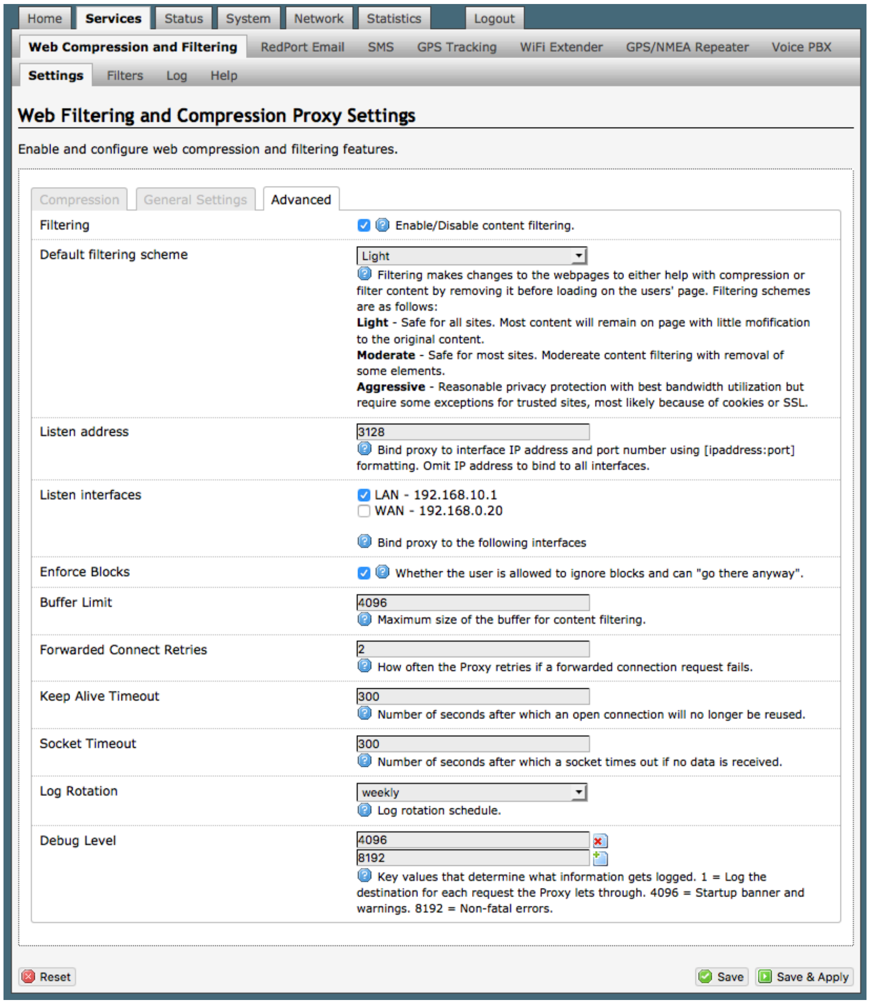
Transparent Proxy □ Enable Transparent proxy. i.e. transparently redirect HTTP web traffic to the web proxy for filtering and/or compression without having to modify the end user's browser settings.
Caution: Enabling transparent mode requires opening TCP ports 53 (DNS), 80 (HTTP), and 443 (HTTPS) which 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.

Before enabling Transparent Proxy, refer to *Chapter 4.3 Router Security.*

Copyright © Global Marine Networks, LLC

5.1.1.3 Advanced Settings

Under normal operating conditions there is little to change here.



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

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 mofification to the original content. **Moderate** - Safe for most sites. Modereate 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 ☐ WAN - 192.168.0.20 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.

Some items of interest include:

Default Filtering Scheme: impactsd 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.

5.1.2 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.

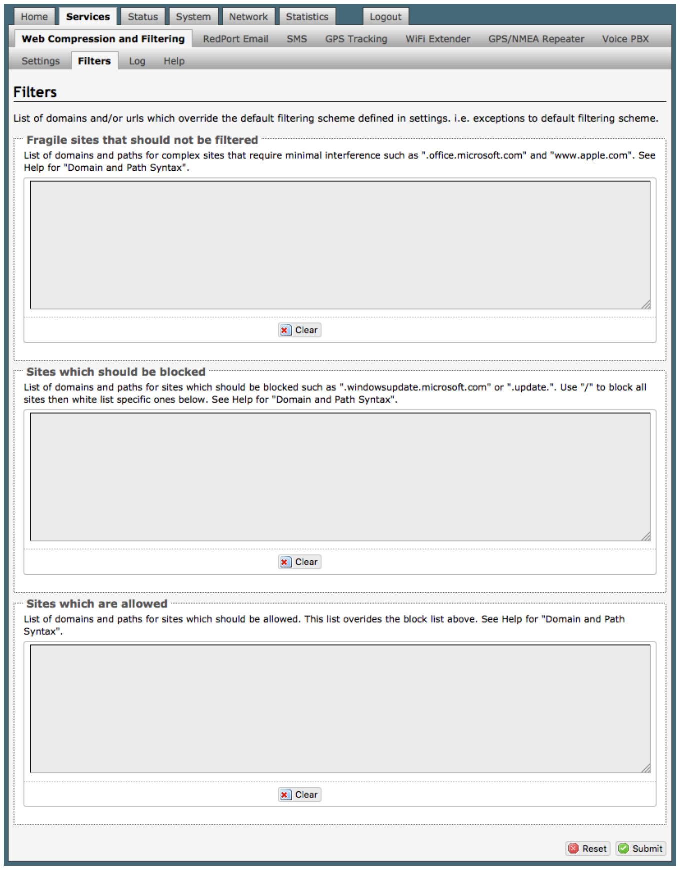
Filters respond to POSIX Regular Expressions

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.



Filters

List of domains and/or urls which override the default filtering scheme defined in settings. i.e. exceptions to default filtering scheme.

Fragile sites that should not be filtered

List of domains and paths for complex sites that require minimal interference such as ".office.microsoft.com" and "www.apple.com". See Help for "Domain and Path Syntax".

Sites which should be blocked

List of domains and paths for sites which should be blocked such as ".windowsupdate.microsoft.com" or ".update.". Use "/" to block all sites then white list specific ones below. See Help for "Domain and Path Syntax".

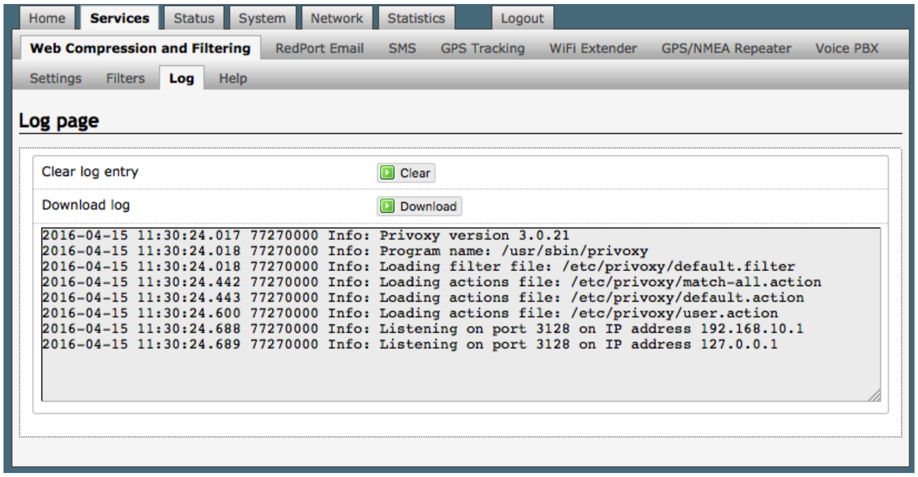
Sites which are allowed

List of domains and paths for sites which should be allowed. This list overides the block list above. See Help for "Domain and Path Syntax".

Copyright © Global Marine Networks, LLC

5.1.3 Log

The Log shows activity on the router. How much activity is logged is determined by the entry in Web Compression and Filtering > Settings > Advanced > Debug Level. Descriptions of debug levels can be found in the Help tab *(see Section 5.1.4 below).*



```
2016-04-15 11:30:24.017 77270000 Info: Privoxy version 3.0.21
2016-04-15 11:30:24.018 77270000 Info: Program name: /usr/sbin/privoxy
2016-04-15 11:30:24.018 77270000 Info: Loading filter file: /etc/privoxy/default.filter
2016-04-15 11:30:24.442 77270000 Info: Loading actions file: /etc/privoxy/match-all.action
2016-04-15 11:30:24.443 77270000 Info: Loading actions file: /etc/privoxy/default.action
2016-04-15 11:30:24.600 77270000 Info: Loading actions file: /etc/privoxy/user.action
2016-04-15 11:30:24.688 77270000 Info: Listening on port 3128 on IP address 192.168.10.1
2016-04-15 11:30:24.689 77270000 Info: Listening on port 3128 on IP address 127.0.0.1
```

Log files are kept in RAM and are rotated weekly, by default. You can change the Log Rotation schedule in Web Compression and Filtering > Settings > Advanced > Log Rotation.

Log files can be downloaded to a .csv file if history must be maintained.

5.1.4 Help

For your convenience the Help page includes:

- A list of Debug Levels and their description.
- A brief explanation and some examples of the POSIX Regular Expressions that must be used for the Domain and/or Path Syntax when creating Filters.

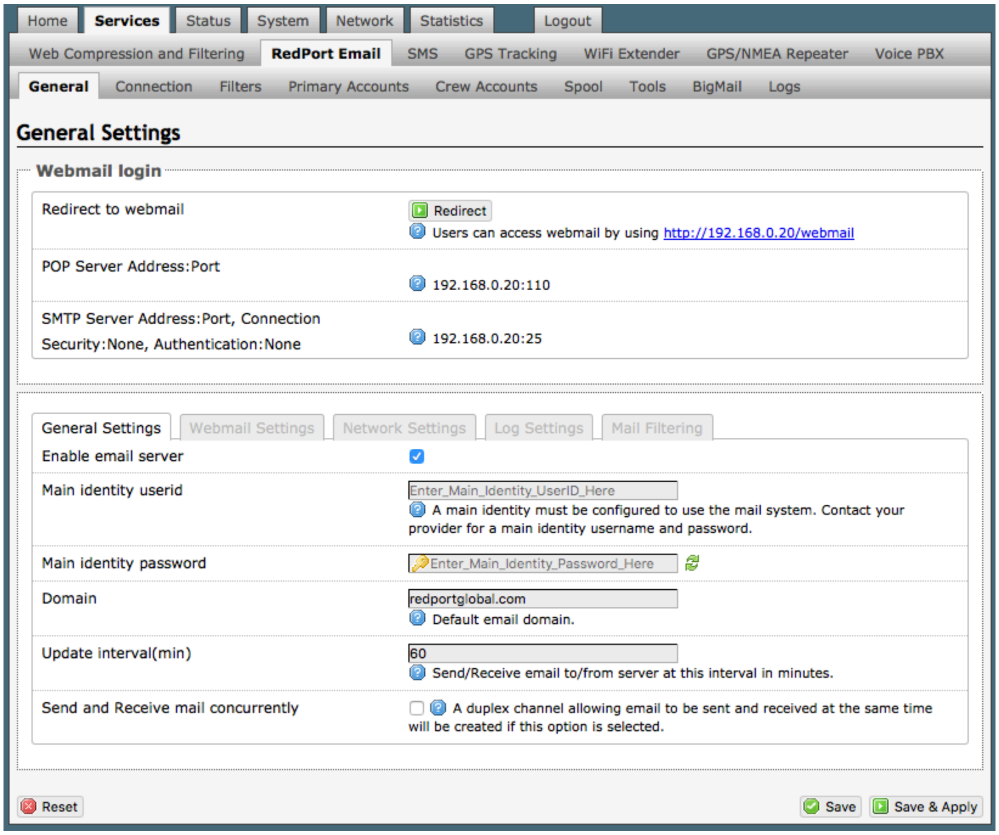
If you are unfamilliar with POSIX regular expressons, a web search should reveal more detailed explanations and tutorials.

Copyright © Global Marine Networks, LLC

5.2 RedPort Email

This is a full-featured Crew solution that runs on the router. RedPort email is designed specifically for use over satellite connections. It uses block compression, mid-file restart, bigmail quarantine and more to maximize data transfers.

Access to Services > RedPort Email requires the 'superadmin' login.



General Settings

Webmail login

Redirect to webmail: Redirect
Users can access webmail by using http://192.168.0.20/webmail

POP Server Address:Port: 192.168.0.20:110

SMTP Server Address:Port, Connection Security:None, Authentication:None: 192.168.0.20:25

Enable email server: ☑

Main identity userid: Enter_Main_Identity_UserID_Here
A main identity must be configured to use the mail system. Contact your provider for a main identity username and password.

Main identity password: Enter_Main_Identity_Password_Here

Domain: redportglobal.com
Default email domain.

Update interval(min): 60
Send/Receive email to/from server at this interval in minutes.

Send and Receive mail concurrently: □ A duplex channel allowing email to be sent and received at the same time will be created if this option is selected.

Once enabled, the onsite administrator can manage email for the entire crew. The users can login to a webmail program to view their email so they do not need special software on their computer or device. The Optimizer Voice is a POP and SMTP server as well so users can access email using their preferred email client instead of webmail access, if desired.

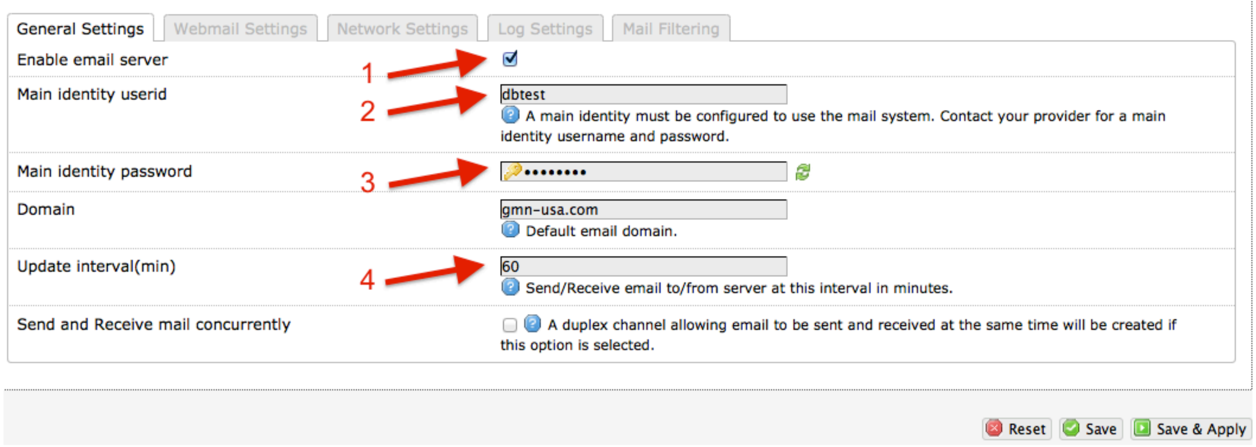
Contact your service provider for details and pricing.

The onsite administrator using the 'admin' login to the user interface does not have access to the RedPort Email Settings.

Copyright © Global Marine Networks, LLC

5.2.1 Enable and Configure RedPort Email

In the RedPort Email General Settings:



Enable email server ☑

Main identity userid: dbtest

A main identity must be configured to use the mail system. Contact your provider for a main identity username and password.

Main identity password: ••••••••

Domain: gmn-usa.com

Default email domain.

Update interval(min): 60

Send/Receive email to/from server at this interval in minutes.

Send and Receive mail concurrently ☐

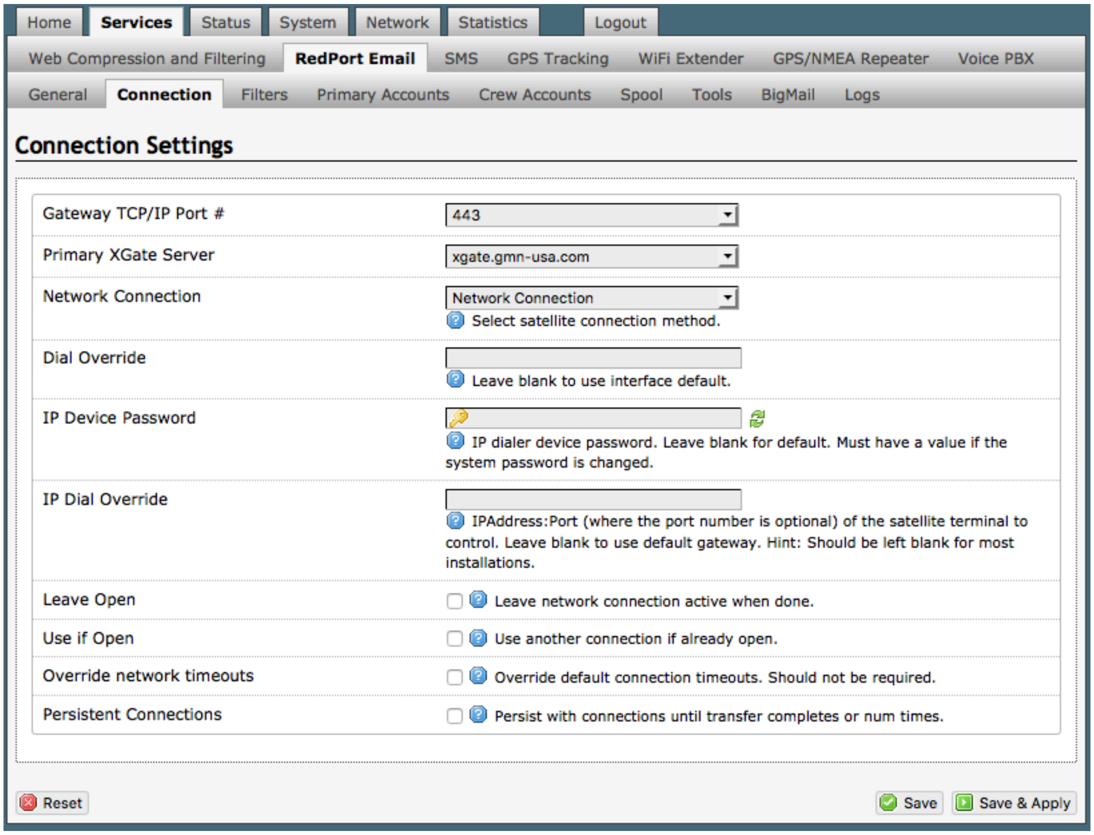
A duplex channel allowing email to be sent and received at the same time will be created if this option is selected.

Before enabling RedPort Email Service, refer to *Chapter 4.3 Router Security.*

1. **Enable Email Server**: click the checkbox to enable email.
2. **Main Identity Userid**: Enter the username assigned to the Main Identity Primary Account for email, as given to you by your service provider.
3. **Main Identity Password**: Enter the password assigned to the Main Identity Primary Account, as given to you by your service provider.
4. **Update Interval**: This is how often (expressed in minutes) the mail program will automatically login to the satellite device to send any pending email and to receive any email pending. The default is set to 60 minutes, but can be modified to fit business needs. (See RedPort Email Guide for information on email block compression and its impact on Update intervals.)
5. Click <Save>.

   Note: Typicially the Main Identity is the onsite email administrator. The Main Identity must be a Primary Account. There must be at least one primary account present on the system before sub/crew accounts can be created. See section 5.2.2 for more information regarding primary accounts.

6. Go to the **Connection** tab:



Connection Settings

Gateway TCP/IP Port #	443
Primary XGate Server	xgate.gmn-usa.com
Network Connection	Network Connection Select satellite connection method.
Dial Override	Leave blank to use interface default.
IP Device Password	IP dialer device password. Leave blank for default. Must have a value if the system password is changed.
IP Dial Override	IPAddress:Port (where the port number is optional) of the satellite terminal to control. Leave blank to use default gateway. Hint: Should be left blank for most installations.
Leave Open	□ Leave network connection active when done.
Use if Open	□ Use another connection if already open.
Override network timeouts	□ Override default connection timeouts. Should not be required.
Persistent Connections	□ Persist with connections until transfer completes or num times.

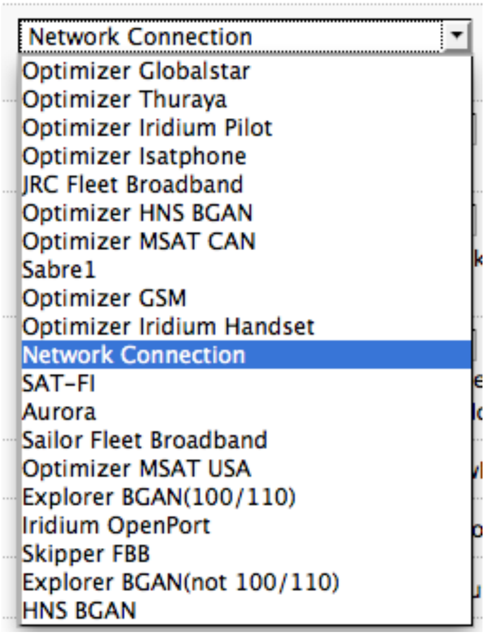
7. Click on <Network Connection> to open up the drop-down menu.

8. Select the appropriate setting for your satellite connection method. This tells the router which satellite device you are using and instructs the router to bring up the connection prior to attempting to send email. Otherwise, it will attempt to send email before the connection is up and because it cannot open the socket to the server it will fail due to a timeout error.

The router supports both Managed and Unmanaged connections for broadband terminals.

9. Select <Save & Apply> to apply the change.

For more information about RedPort Email setup and use, please see the separate document, *Optimizer RedPort Email Guide*.



Copyright © Global Marine Networks, LLC

5.2.2 Primary Accounts

The Main Identity must be a Primary Account. There must be at least one primary account present on the system. The username and password are assigned to you by your service provider.

Typically there is only one Primary Account, however RedPort Email allows access to multiple primary accounts if needed. For example, a fleet manager that travels from vessel to vessel would have a primary account and would need access to that account from each vessel in the fleet.

Primary accounts have access to email whether on or off the vessel as the account exists on the GMN mail servers.

Primary accounts also have access to Filters to customize settings to meet the account needs. These filters include:

- Mail Management including BigMail (See Chapters 6.0 and 8.0 of the RedPort Email Guide for details)
- Inbound Mail Filter (See Chapter 7.0 of the RedPort Email Guide for details)
- Outbound Mail Filter (See Chapter 7.0 of the RedPort Email Guide for details)

The Primary Account receives all Email system messages.

The email address of the primary account will be: username@redportglobal.com. See Appendix A of the RedPort Email Guide for information on using a custom domain name for the email address.

BEST PRACTICE: The Main Identity Primary Account is reserved for the Email Administrator. The Email Administrator does NOT have a sub account. With this arrangement the Email Administrator will receive the system messages that cannot be viewed via a sub account.

Once the Primary Account is setup, the onsite administrator can setup and manage the sub/crew accounts.

Please see the *Optimizer RedPort Email Guide* for comprehensive information on the use of RedPort Email service.

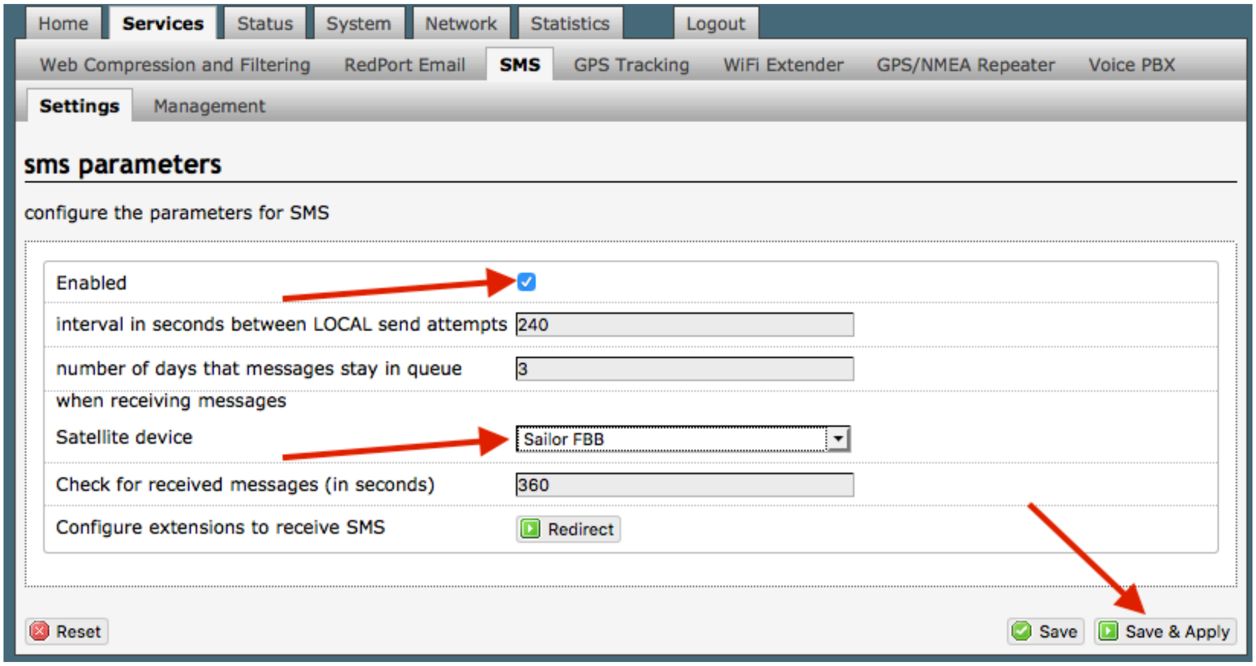
5.3 SMS Messaging

If using a compatible satellite device, it is possible to send and receive SMS messages directly from the Optimizer Voice router 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.

5.3.1 SMS Settings

Use Settings to enable and configure the SMS parameters.



sms parameters

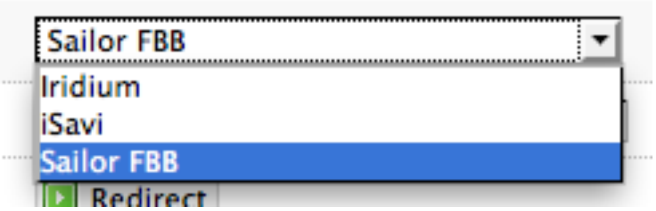
configure the parameters for SMS

Enabled	☑
interval in seconds between LOCAL send attempts	240
number of days that messages stay in queue when receiving messages	3
Satellite device	Sailor FBB
Check for received messages (in seconds)	360
Configure extensions to receive SMS	Redirect

1. Select the checkbox to enable SMS.

2. Select the appropriate Satellite device from the drop down menu.

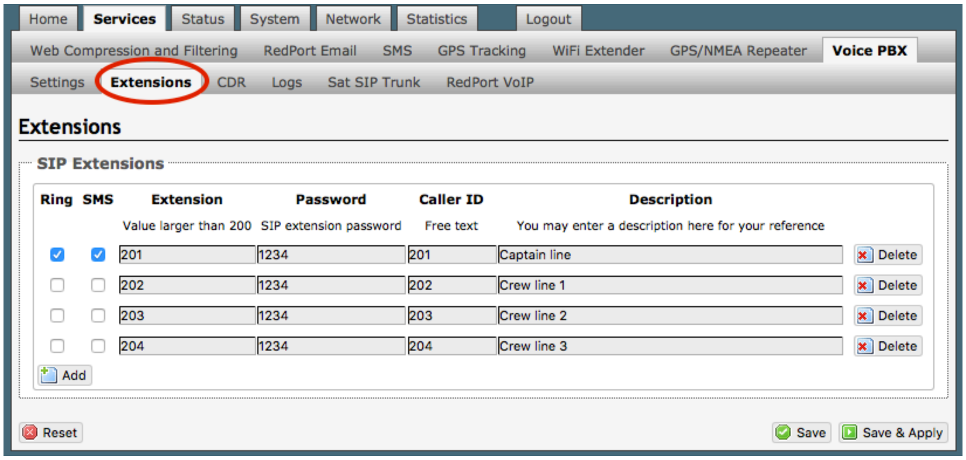
3. Select <Save & Apply>.



Copyright © Global Marine Networks, LLC

5.3.2 Configure SIP Extensions to Receive SMS Messages

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



Extensions

SIP Extensions

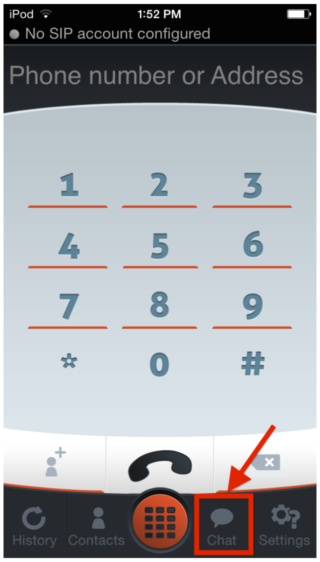
Ring	SMS	Extension	Password	Caller ID	Description	
		Value larger than 200	SIP extension password	Free text	You may enter a description here for your reference	
☑	☑	201	1234	201	Captain line	Delete
□	□	202	1234	202	Crew line 1	Delete
□	□	203	1234	203	Crew line 2	Delete
□	□	204	1234	204	Crew line 3	Delete

To enable an extension to receive SMS messages, use the checkbox in the SMS column. For more information on configuring SIP Extensions *see Chapter 5.7.2.*

5.3.3 How to Send/Receive SMS Messages

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 Voice wireless network 'wxa-153-xxxx'.



No SIP account configured

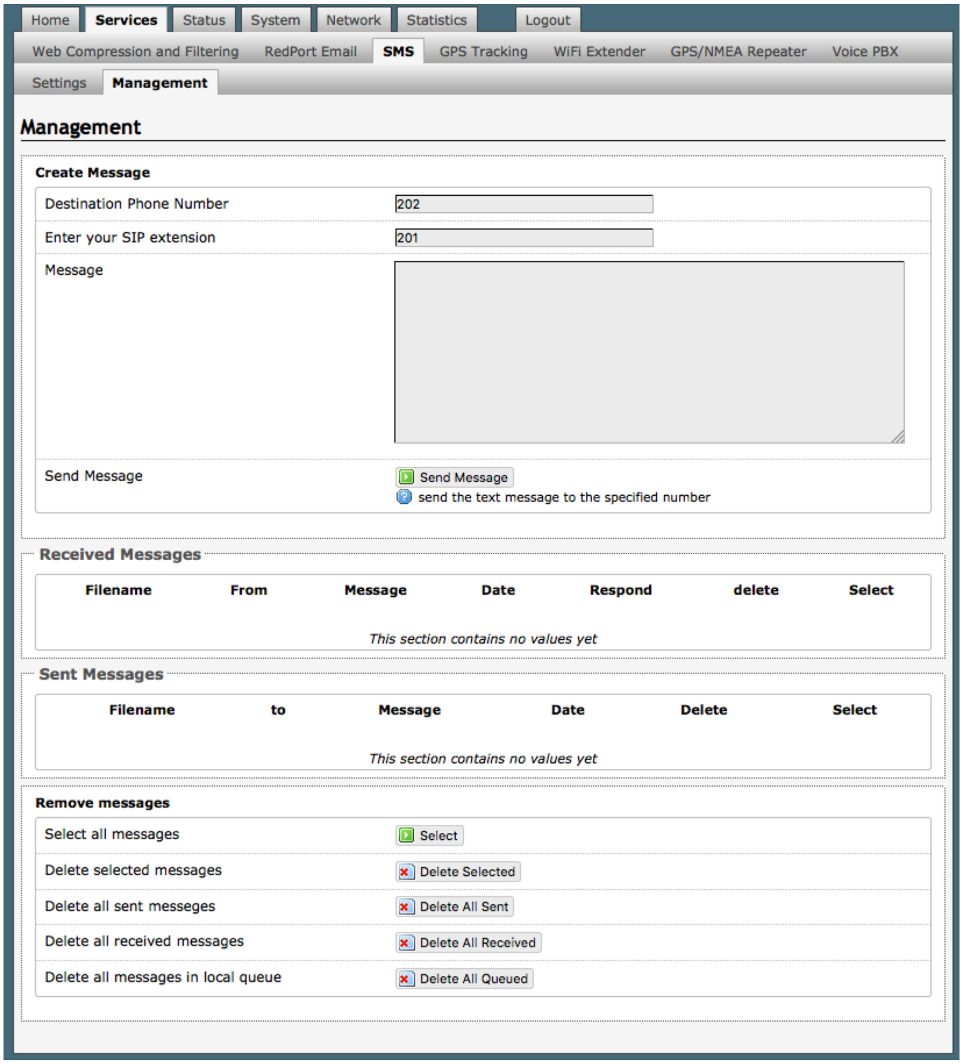
Open the XGate Phone App. Select <Chat> to send a SMS message or to view a SMS message received.

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.)

Copyright © Global Marine Networks, LLC

5.3.4 SMS Management

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



Management

Create Message

Destination Phone Number	202
Enter your SIP extension	201
Message	
Send Message	Send Message 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	Select
Delete selected messages	Delete Selected
Delete all sent messeges	Delete All Sent
Delete all received messages	Delete All Received
Delete all messages in local queue	Delete All Queued

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

5.4 GPS Tracking

If you wish to have tracking service using your satellite device, the Optimizer offers GPS Tracking service powered by GSatTrack or Tracking service via SMS message.

Access to Services > GPS Tracking requires the 'superadmin' login.

5.4.1 Tracking powered by RedPort with GSatTrack

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

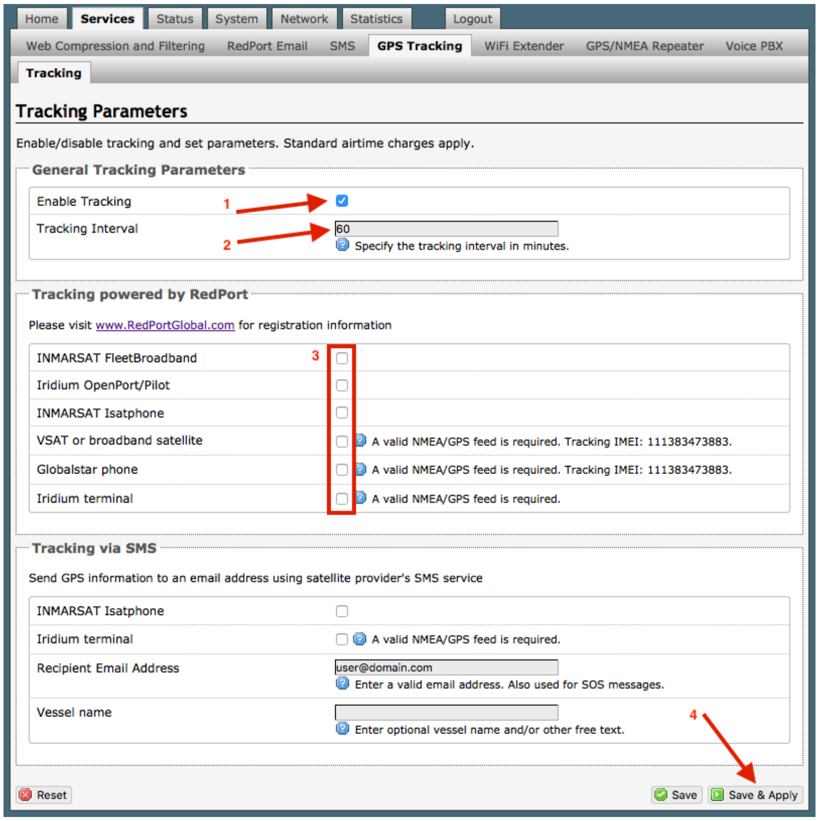
This tracking service must be purchased separately. See your satellite service provider for details.

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

1. Select the checkbox to **Enable Tracking**.

2. 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 the satellite link. Keep in mind that standard airtime charges will apply to each postition report. Adjust the Tracking Interval to meet your needs.

3. Select the satellite terminal you are using. Note: a valid NMEA/GPS feed is required when using some satellite devices.



Tracking Parameters

Enable/disable tracking and set parameters. Standard airtime charges apply.

General Tracking Parameters

Enable Tracking	☑
Tracking Interval	60 Specify the tracking interval in minutes.

Tracking powered by RedPort

Please visit www.RedPortGlobal.com for registration information

INMARSAT FleetBroadband	☐
Iridium OpenPort/Pilot	☐
INMARSAT Isatphone	☐
VSAT or broadband satellite	☐ A valid NMEA/GPS feed is required. Tracking IMEI: 111383473883.
Globalstar phone	☐ A valid NMEA/GPS feed is required. Tracking IMEI: 111383473883.
Iridium terminal	☐ A valid NMEA/GPS feed is required.

Tracking via SMS

Send GPS information to an email address using satellite provider's SMS service

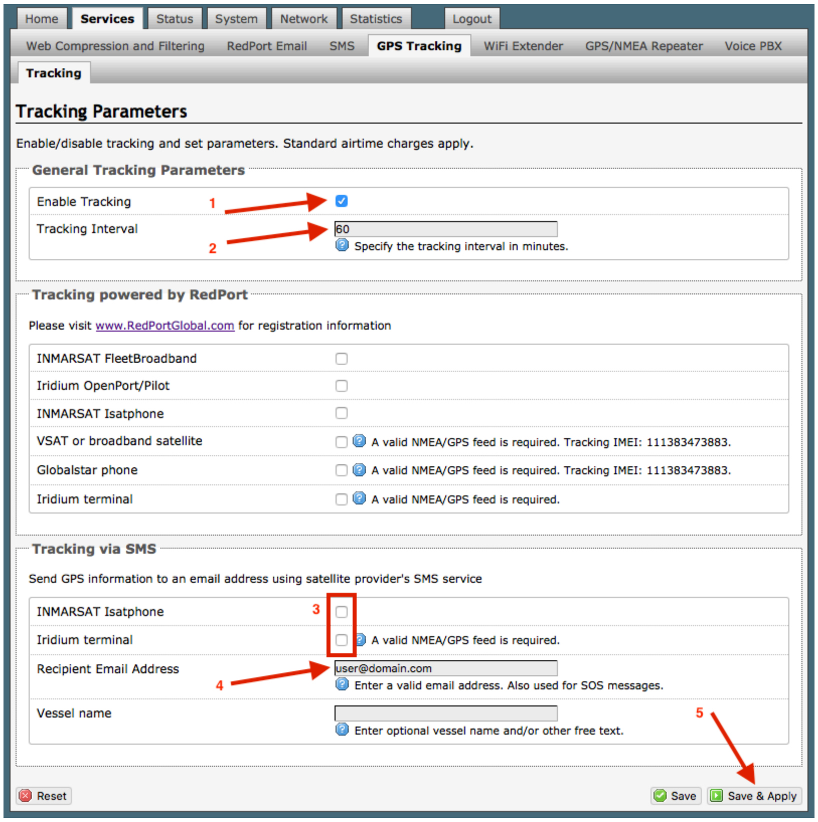
INMARSAT Isatphone	☐
Iridium terminal	☐ A valid NMEA/GPS feed is required.
Recipient Email Address	user@domain.com Enter a valid email address. Also used for SOS messages.
Vessel name	 Enter optional vessel name and/or other free text.

Step 4. Select <Save & Apply>.

Copyright © Global Marine Networks, LLC

5.4.2 Tracking via SMS

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.



Tracking Parameters

Enable/disable tracking and set parameters. Standard airtime charges apply.

General Tracking Parameters

Enable Tracking ☑

Tracking Interval 60
Specify the tracking interval in minutes.

Tracking powered by RedPort

Please visit www.RedPortGlobal.com for registration information

INMARSAT FleetBroadband □
Iridium OpenPort/Pilot □
INMARSAT Isatphone □
VSAT or broadband satellite □ A valid NMEA/GPS feed is required. Tracking IMEI: 111383473883.
Globalstar phone □ A valid NMEA/GPS feed is required. Tracking IMEI: 111383473883.
Iridium terminal □ 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 □ A valid NMEA/GPS feed is required.
Recipient Email Address user@domain.com
Enter a valid email address. Also used for SOS messages.
Vessel name
Enter optional vessel name and/or other free text.

1. Select the checkbox to **Enable Tracking**.

2. 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 postition report. Adjust the Tracking Interval to meet your needs.

3. 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.

4. 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 2.

Step 5. Select <Save & Apply>.

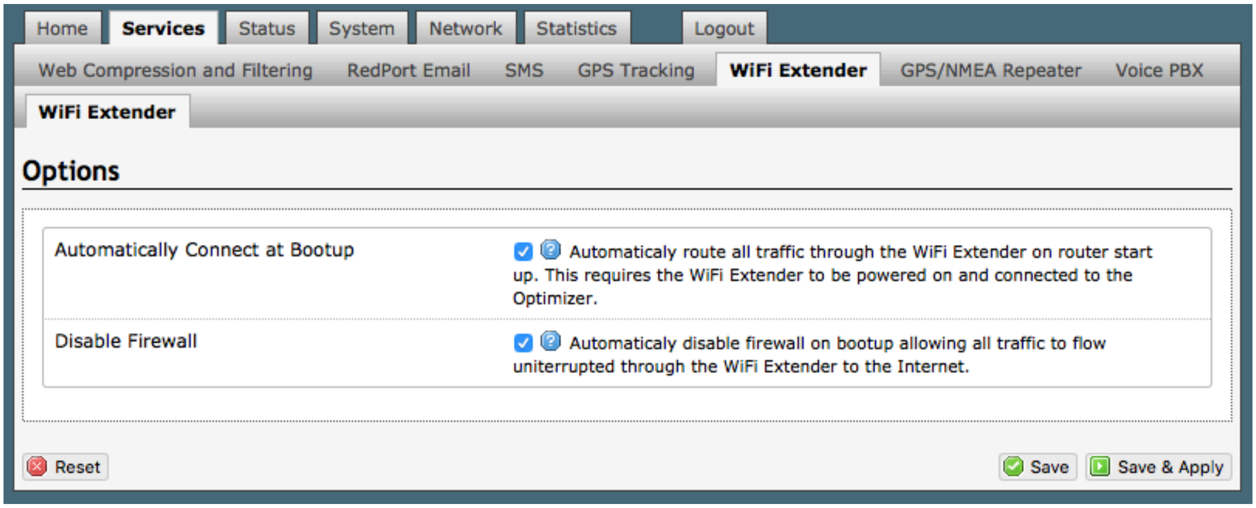
Copyright © Global Marine Networks, LLC

5.5 WiFi Extender

If you using the RedPort WiFi Extender, you can configure the Optimizer to automatically route all traffic through it.

IMPORTANT: The RedPort WiFi Extender must be powered ON and connected to the Optimizer before turning the Optimizer ON.

Access to Services > WiFi Extender requires the 'superadmin' login.



Options

Automatically Connect at Bootup ☑ Automaticaly route all traffic through the WiFi Extender on router start up. This requires the WiFi Extender to be powered on and connected to the Optimizer.

Disable Firewall ☑ Automaticaly disable firewall on bootup allowing all traffic to flow uniterrupted through the WiFi Extender to the Internet.

When using the RedPort WiFi Extender it is assumed that you are not using a satellite device for the Internet connection, therefore, disabling the firewall allows Internet traffic to flow freely.

For RedPort Wifi Extender configuration and use details, see the Optimizer Voice Onsite Administrator Guide.

Copyright © Global Marine Networks, LLC

5.6 GPS/NMEA Repeater

Requires 'superadmin' login.

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:

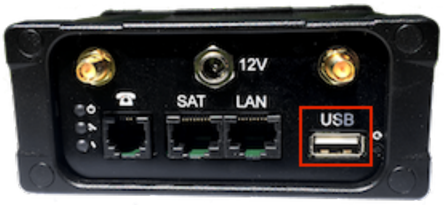
- A USB connected GPS or NMEA device.
- A serial port connected GPS or NMEA device with appropriate USB to Serial Adapter.

5.6.1 Equipment Setup

A physical connection is required from the source (GPS/NMEA device) to the Optimizer.

5.6.1.1 USB NMEA Device

When using a NMEA device that supports a USB connection, connect the NMEA device to the USB port on the rear of the Optimzier with an appropriate USB to NMEA device cable as indicated by the NMEA device manufacturer.



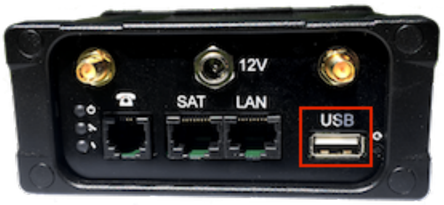
The Optimizer will broadcast the GPS signal over WiFi, so you can connect your computer to the WiFi network in order to establish a successful connection with your destination software.

5.6.1.2 RS-232 NMEA Device

With Serial Port Connector

When using a NMEA device with Serial Port connection, a USB to Serial Adapter (PL-2303HX or FTDi Chip) is required.

CAUTION: While all standard USB to serial adapters may work, the PL-2303HX and the FTDi Chip are the only USB to Serial Adapters that we recommend as compatible with the Optimizer.



Connect the NMEA device to the USB port on the rear of the Optimizer with an appropriate USB to Serial Adapter.

The Optimizer will broadcast the GPS signal over WiFi, so you can connect your computer to the WiFi network in order to establish a successful connection with your destination software.

Without 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 USB to serial adapter as noted above.

5.6.1.3 Connecting Multiple NMEA Devices

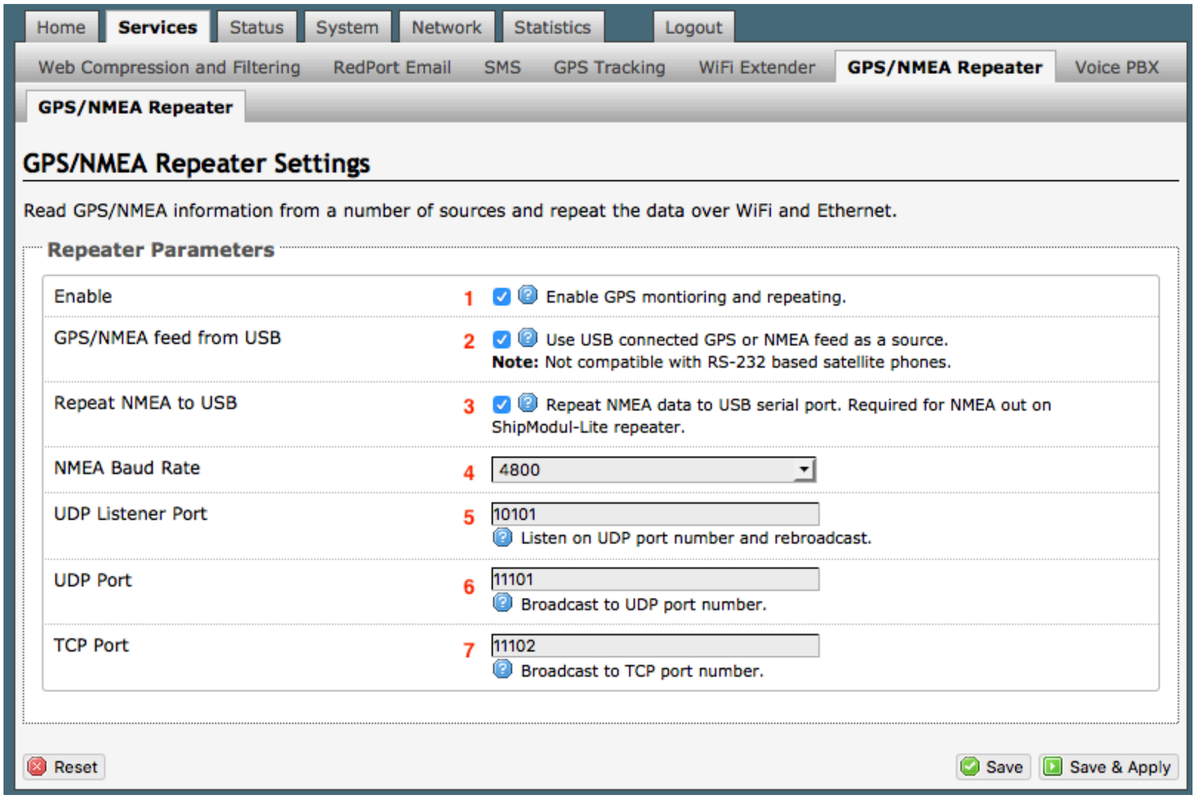
It is possible to connect up to four NMEA devices if you have the proper hardware. It will require a USB to RS-232 4-port Hub or a RS-232 4-port terminal block that you would simply plug into the Optimizer's USB port.

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.

5.6.2 GPS/NMEA Repeater Parameters Configuration

Requires 'superadmin' login.

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.



GPS/NMEA Repeater Settings

Read GPS/NMEA information from a number of sources and repeat the data over WiFi and Ethernet.

Repeater Parameters

Enable	1	☑ Enable GPS montioring and repeating.
GPS/NMEA feed from USB	2	☑ Use USB connected GPS or NMEA feed as a source. **Note:** Not compatible with RS-232 based satellite phones.
Repeat NMEA to USB	3	☑ Repeat NMEA data to USB serial port. Required for NMEA out on ShipModul-Lite repeater.
NMEA Baud Rate	4	4800
UDP Listener Port	5	10101 Listen on UDP port number and rebroadcast.
UDP Port	6	11101 Broadcast to UDP port number.
TCP Port	7	11102 Broadcast to TCP port number.

1. Select this checkbox to **Enable** GPS monitoring and repeating.

2. Select this checkbox when connecting a GPS or NMEA device via USB cable

3. Select this checkbox to repeat NMEA data to a USB serial port for use by other devices.

4. Using the drop down menu, select the baud rate required for the destination software. By default, most NMEA 183 devices (GPS) and applications use 4800 baud for this setting.

5. Enter the UDP port number to which the GPS is connected. The default is set to the standard UDP Listener Port for NMEA 183 devices of 10101.

6. Enter the UDP port number to which the GPS data will be broadcast. The default is set to the standard UDP Port for NMEA 183 devices of 11101. (Note: configure the destination

Copyright © Global Marine Networks, LLC

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

7. Enter the TCP port number to which the GPS data will be broadcast. 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.)

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.***

5.7 VOICE PBX

Requires 'superadmin' login.

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

- Sailor FBB terminal - requires XGate Phone app*. *(See Chapter 5.7.6)*
- IsatHub iSavi - requires IsatHub Control app and either IsatHub Voice app or XGate Phone app*. *(See Appendix A)*
- 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. *See Chapter 5.7.7.*

As of this writing, Multi-VoIP is compatible with the following:

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

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

Caution: Before enabling the PBX service read chapter 4.3 Router Security.

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

Copyright © Global Marine Networks, LLC

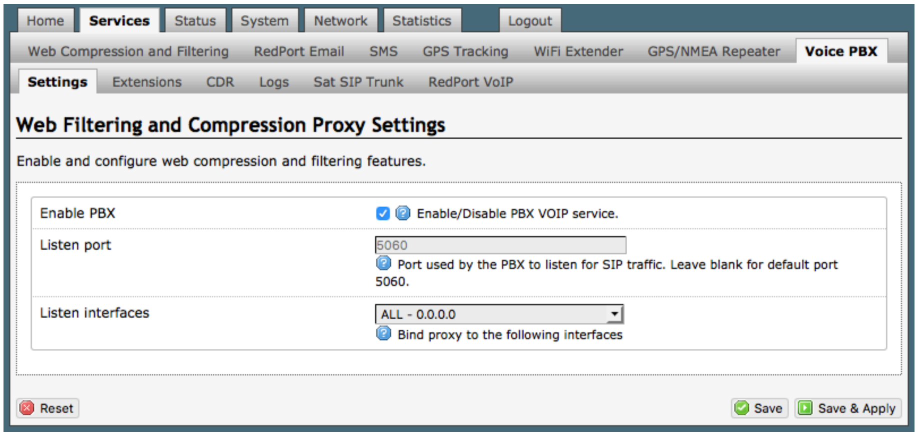
5.7.1 Voice PBX Settings

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

IMPORTANT NOTE: Prior to enabling PBX service, review Chapter 4.3.1 How to Secure Your Router.

Select 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 Chapter x.x.x for How To Secure Your Router.



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

Enable PBX	☑ Enable/Disable PBX VOIP service.
Listen port	5060 Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.
Listen interfaces	ALL - 0.0.0.0 Bind proxy to the following interfaces

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

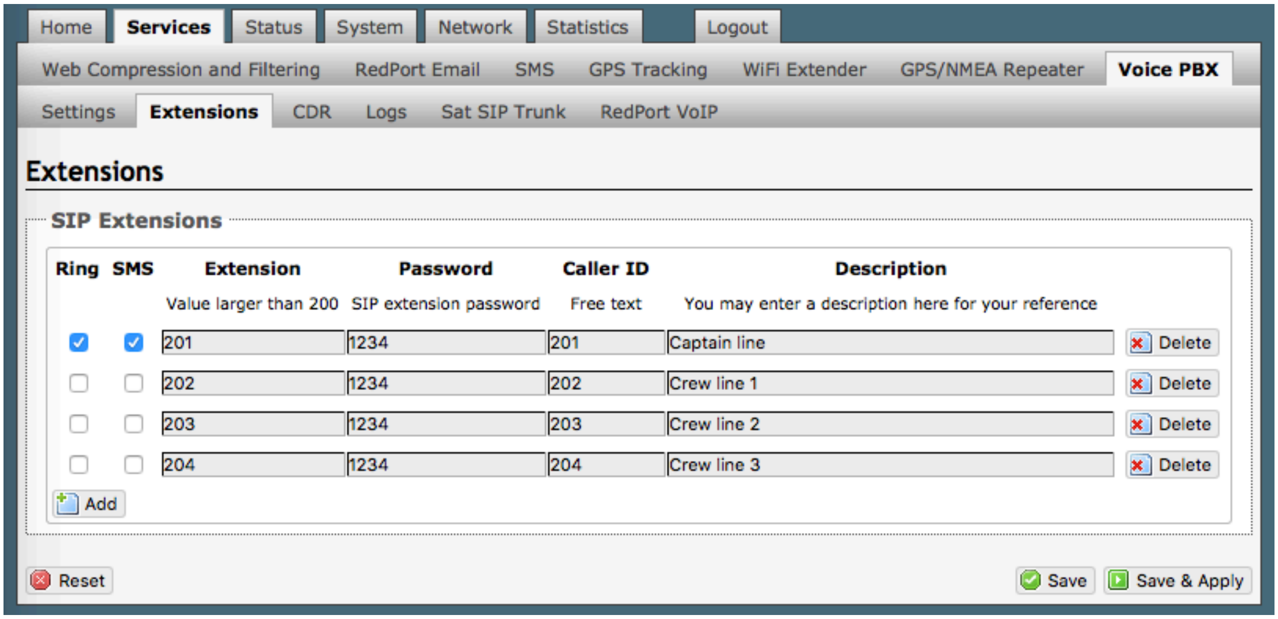
Copyright © Global Marine Networks, LLC

5.7.2 Setup 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.



Extensions

SIP Extensions

Ring	SMS	Extension	Password	Caller ID	Description	
		Value larger than 200	SIP extension password	Free text	You may enter a description here for your reference	
☑	☑	201	1234	201	Captain line	☒ Delete
□	□	202	1234	202	Crew line 1	☒ Delete
□	□	203	1234	203	Crew line 2	☒ Delete
□	□	204	1234	204	Crew line 3	☒ Delete

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

5.7.3 How to Make/Receive Voice Calls

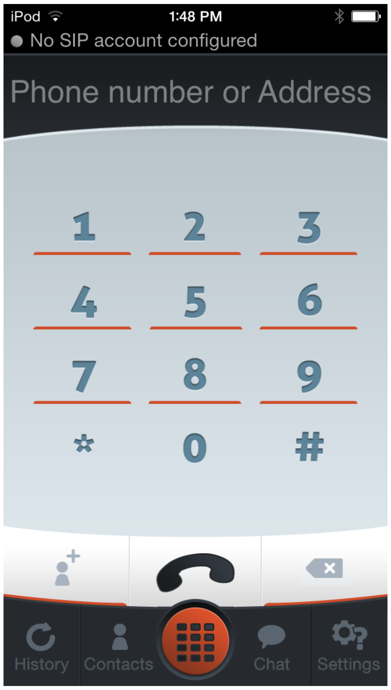
Using the smartphone or tablet Settings, connect to the Optimizer Voice wireless network 'wxa-153-xxxx'.

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 consective sessions -- with the optional RedPort VoIP service. Contact your service provider for details. *See Chapter 5.7.7.*

IMPORTANT: Inmarsat IsatHub (iSavi) users. *Please see Appendix A for instructions for setup and use of the Optimizer Voice with the iSavi terminal for voice calls, email and sms messaging.*

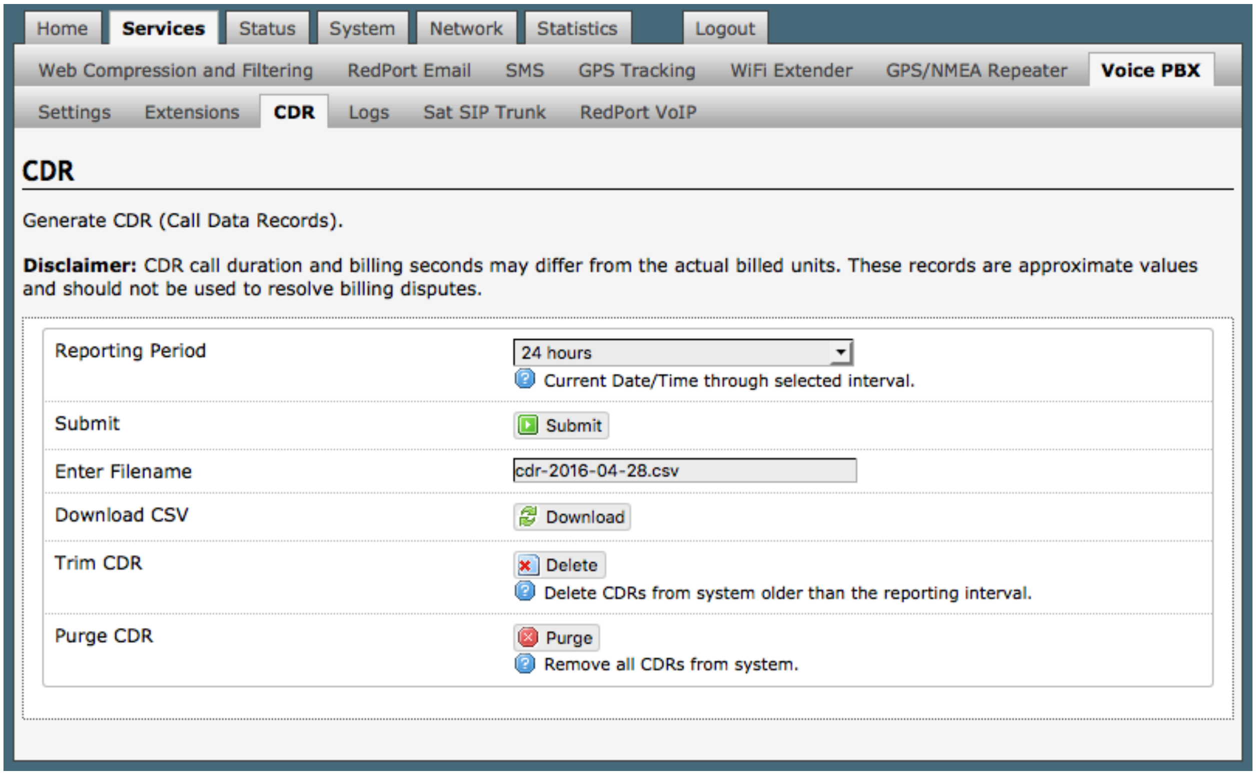


● No SIP account configured

5.7.4 CDR (Call Data Records)

Requires 'superadmin' login.

It is possible to view and download the Call Data Records. The Call Data Records stored on the Optimizer are approximate values and should not be used to resolve billing disputes. They are presented here for your convenience.



CDR

Generate CDR (Call Data Records).

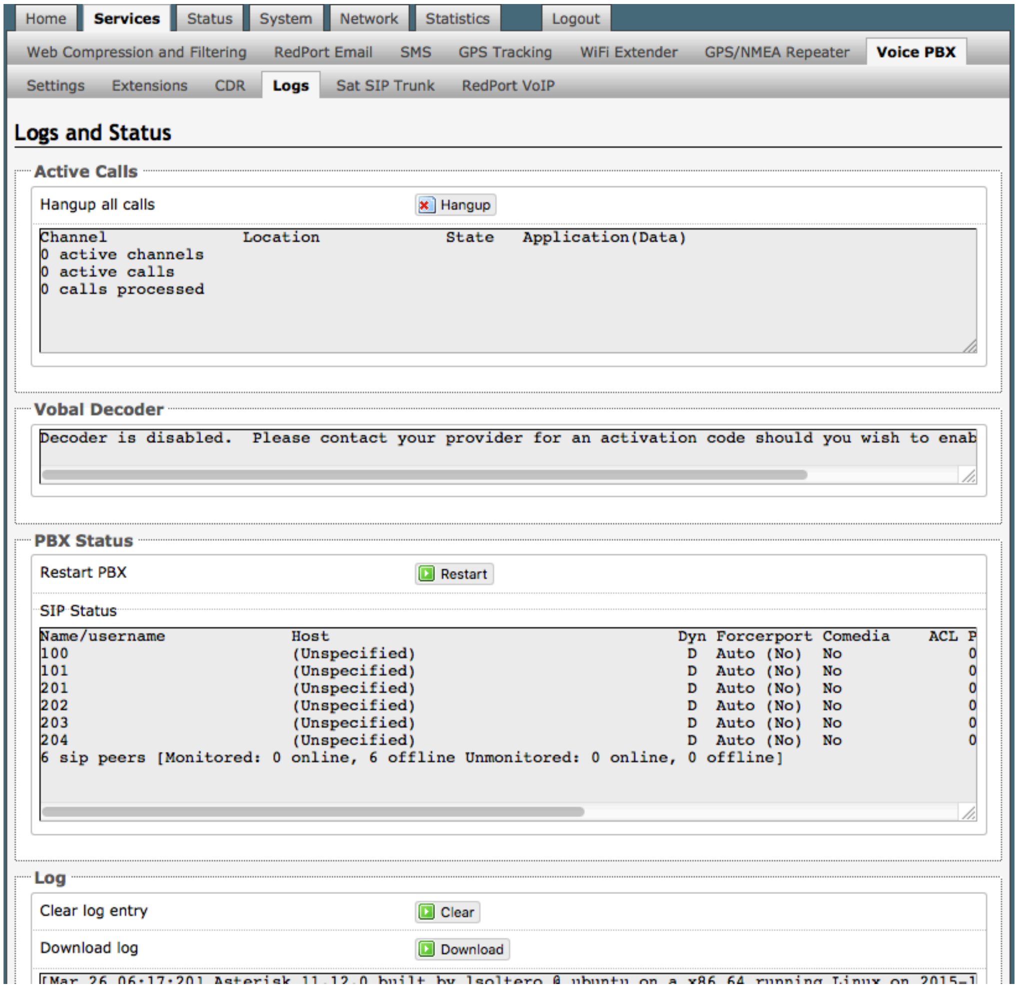
Disclaimer: CDR call duration and billing seconds may differ from the actual billed units. These records are approximate values and should not be used to resolve billing disputes.

Reporting Period	24 hours Current Date/Time through selected interval.
Submit	Submit
Enter Filename	cdr-2016-04-28.csv
Download CSV	Download
Trim CDR	Delete Delete CDRs from system older than the reporting interval.
Purge CDR	Purge Remove all CDRs from system.

On active systems, the call data records can quickly use some memory. It is recommend that you periodically trim or purge the records from the system.

5.7.5 Logs

Call status can be monitored from the Logs screen.



```
Channel              Location             State   Application(Data)
0 active channels
0 active calls
0 calls processed
```

```
Decoder is disabled.  Please contact your provider for an activation code should you wish to enab
```

```
Name/username             Host                                    Dyn Forcerport Comedia    ACL P
100                       (Unspecified)                            D  Auto (No)  No           0
101                       (Unspecified)                            D  Auto (No)  No           0
201                       (Unspecified)                            D  Auto (No)  No           0
202                       (Unspecified)                            D  Auto (No)  No           0
203                       (Unspecified)                            D  Auto (No)  No           0
204                       (Unspecified)                            D  Auto (No)  No           0
6 sip peers [Monitored: 0 online, 6 offline Unmonitored: 0 online, 0 offline]
```

```
[Mar 26 06:17:20] Asterisk 11.12.0 built by lsoltero @ ubuntu on a x86_64 running Linux on 2015-1
```

Active Calls: displays all active channels in use. Select <Hangup> to immediately hangup all active calls.

Vobal Decoder: Displays the VoIP Activation Key when RedPort VoIP service is enabled. *See Chapter 5.7.7.*

PBX Status: Displays the current status of all SIP extensions. Select <Restart> to reboot the PBX service.

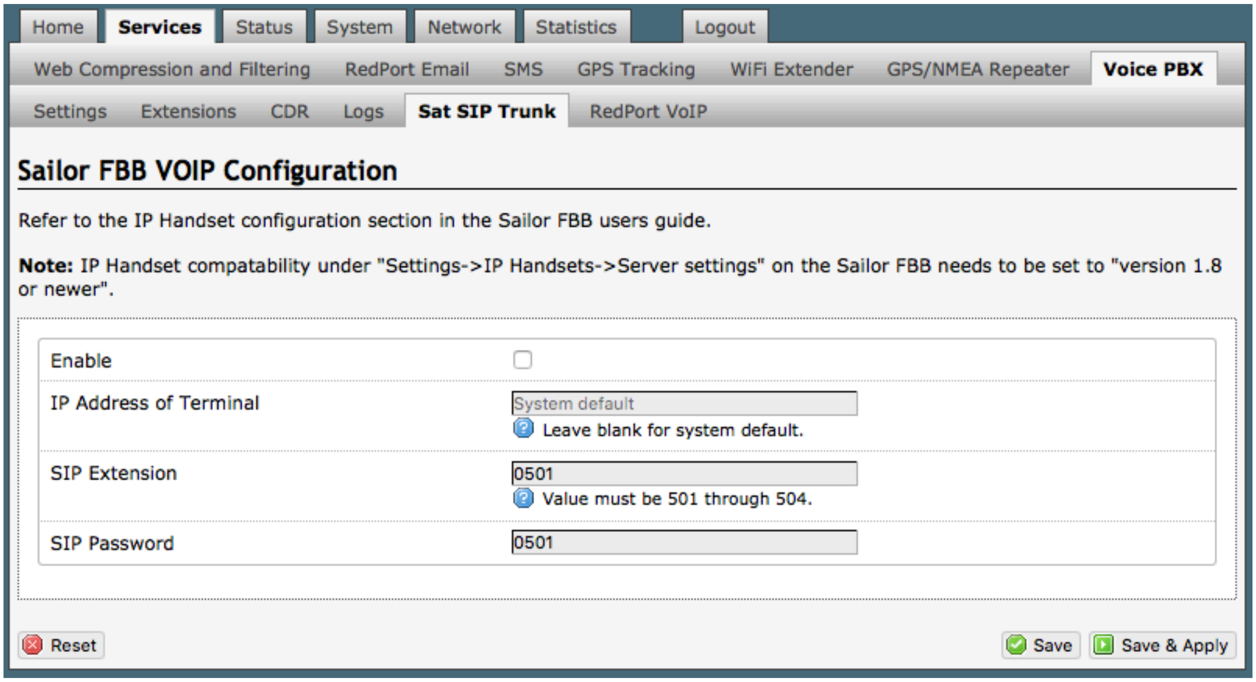
Log: Displays the current Log of PBX usage. Select <Clear> to remove the log content. Select <Download> to Open or Save the PBX Log.

RedPort

5.7.6 Sat SIP Trunk (for Sailor FBB terminal only)

Requires 'superadmin' login.

Use this screen to enable and configure SIP calling when using a Sailor FBB terminal.



Sailor FBB VOIP Configuration

Refer to the IP Handset configuration section in the Sailor FBB users guide.

Note: IP Handset compatability under "Settings->IP Handsets->Server settings" on the Sailor FBB needs to be set to "version 1.8 or newer".

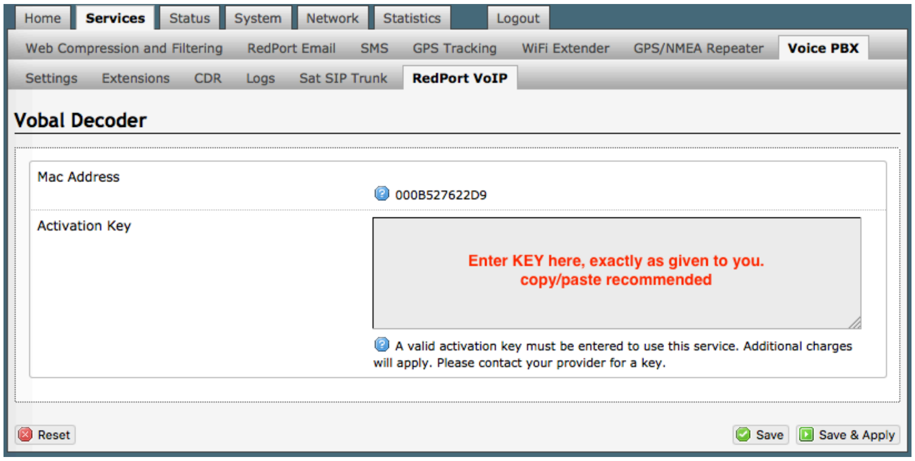
Enable	□
IP Address of Terminal	System default Leave blank for system default.
SIP Extension	0501 Value must be 501 through 504.
SIP Password	0501

NOTE: You may need to edit the IP Handset configuration in the Sailor FBB user interface. Settings > IP Handsets > Server Settings on the Sailor FBB must be set to version 1.8 or newer. (Refer to the Sailor FBB users guide for how to access the Sailor FBB Settings).

5.7.7 RedPort VoIP Activation

With optional RedPort VoIP service, up to four users can send/receive phone calls and/or text messages simultaneously. Outbound calls are typically less expensive VoIP calls than standard circuit switch (PSTN) calls at standard satellite airtime rates. Contact your satellite service provider to purchase the RedPort VoIP service.

When the service is activated, you will be given a "Key". This key is a long alpha-numeric string that must be entered into the Optimizer Voice user interface.



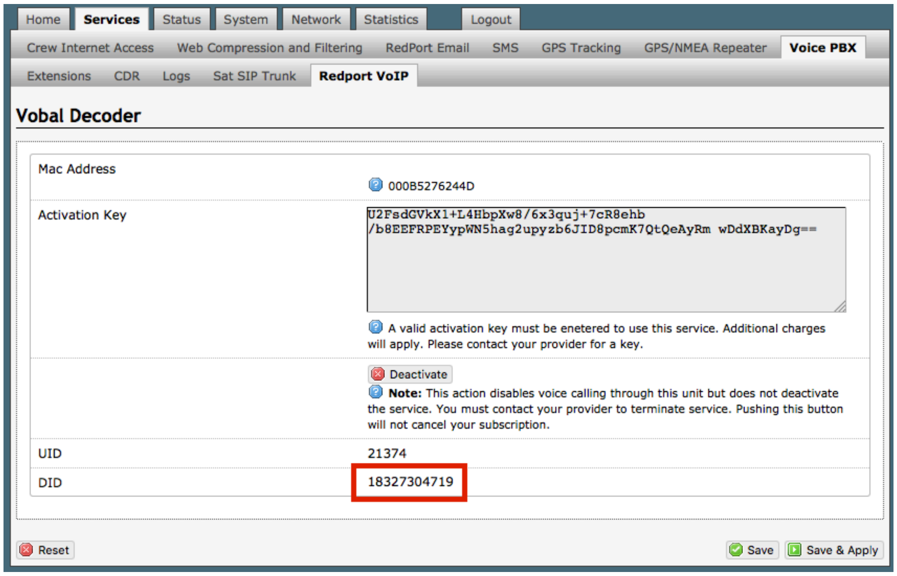
Vobal Decoder

Mac Address: 000B527622D9

Activation Key: Enter KEY here, exactly as given to you. copy/paste recommended

A valid activation key must be entered to use this service. Additional charges will apply. Please contact your provider for a key.

Enter the Key and select <Save & Apply>.



Vobal Decoder

Mac Address: 000B5276244D

Activation Key:

```
U2FsdGVkX1+L4HbpXw8/6x3quj+7cR8ehb
/b8EEFRPEYypWN5hag2upyzb6JID8pcmK7QtQeAyRm wDdXBKayDg==
```

A valid activation key must be enetered to use this service. Additional charges will apply. Please contact your provider for a key.

Note: This action disables voice calling through this unit but does not deactivate the service. You must contact your provider to terminate service. Pushing this button will not cancel your subscription.

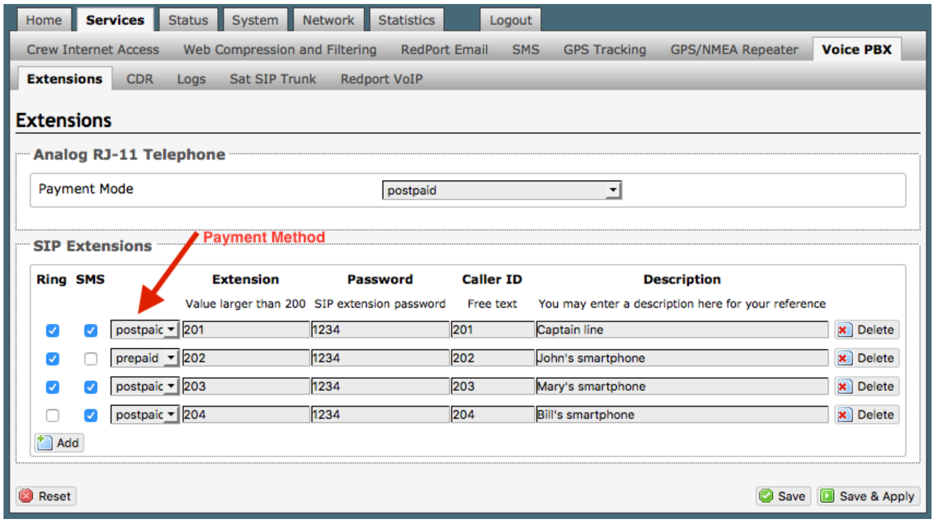
UID: 21374

DID: 18327304719

With RedPort VoIP service activated, the new RedPort VoIP telephone number is displayed.

Copyright © Global Marine Networks, LLC

Configure the SIP extensions for Ring and/or SMS by selecting the checkbox next to the SIP extension. *See Chapter 5.7.2.*



Extensions

Analog RJ-11 Telephone

Payment Mode: postpaid

SIP Extensions

Ring	SMS		Extension	Password	Caller ID	Description	
			Value larger than 200	SIP extension password	Free text	You may enter a description here for your reference	
☑	☑	postpaic	201	1234	201	Captain line	Delete
☑	□	prepaid	202	1234	202	John's smartphone	Delete
☑	☑	postpaic	203	1234	203	Mary's smartphone	Delete
□	☑	postpaic	204	1234	204	Bill's smartphone	Delete

Select the payment method of each SIP extension (prepaid or postpaid).

There must be at least one postpaid line.

By default, Line 1 always Postpaid.

On this page, you can also:

- change the SIP extension password
- change the outgoing CallerID display
- enter a desription for your reference

In the example above, when an incoming call arrives, only the phones of the Captain, John, and Mary will ring. Incoming SMS messages will appear on the phones of the Captain, Mary, and Bill.

When the configuration of the SIP extensions is complete, select <Save & Apply>

5.8 Network Shares

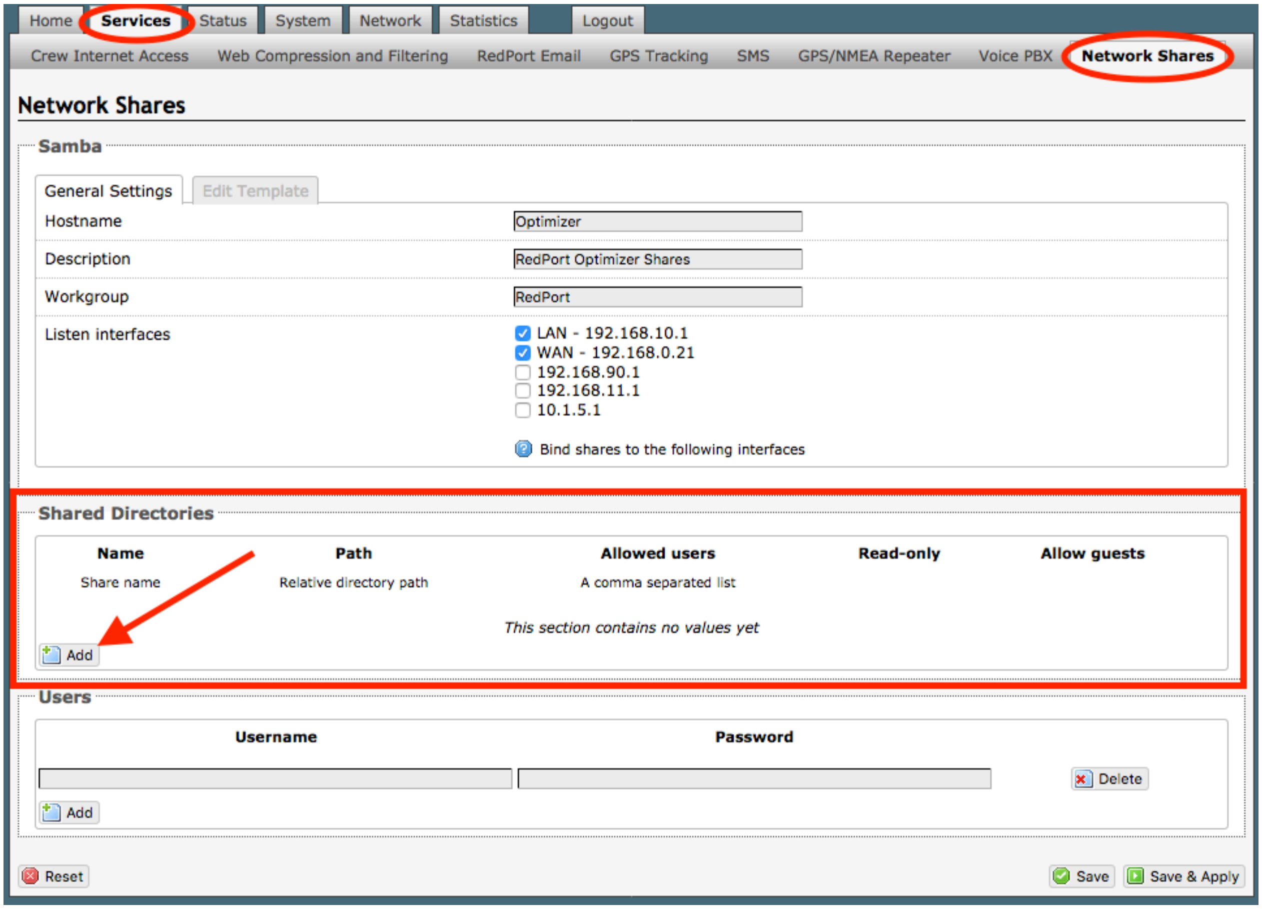
Available to both 'admin' and 'superadmin' login.

Network Shares allows the sharing of files without the requirement of a wired local network of computers. The Optimizer router can be configured with one or more Shared Directories that are available, with or without password protection, to any Windows or Mac PC that has access to the Optimizer's WiFi Hotspot.

Network Shares also allows the ability to automatically transfer files via inbound and outbound email *(see Optimizer-RedPort Email Guide > Appendix F: File Transfer Tab for details).*

5.8.1 Create a Shared Directory

Select <Add> to create a new Shared Directory:



Network Shares

Samba

Hostname	Optimizer
Description	RedPort Optimizer Shares
Workgroup	RedPort
Listen interfaces	☑ LAN - 192.168.10.1 ☑ WAN - 192.168.0.21 □ 192.168.90.1 □ 192.168.11.1 □ 10.1.5.1 Bind shares to the following interfaces

Shared Directories

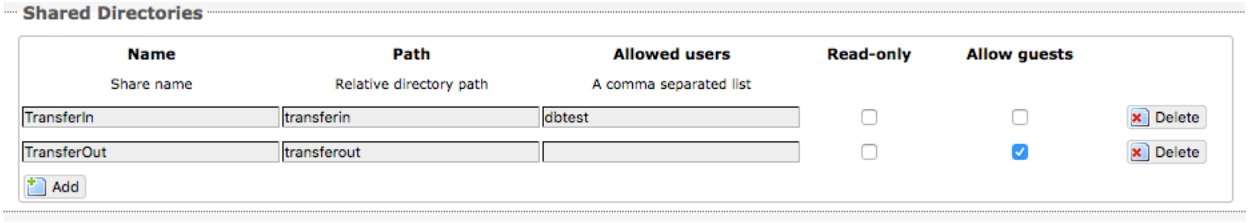
Name	Path	Allowed users	Read-only	Allow guests
Share name	Relative directory path	A comma separated list		

This section contains no values yet

Users

Username	Password	
		Delete

Copyright © Global Marine Networks, LLC



Shared Directories

Name Share name	Path Relative directory path	Allowed users A comma separated list	Read-only	Allow guests	
TransferIn	transferin	dbtest	□	□	Delete
TransferOut	transferout		□	☑	Delete

Name: This is the Share Name that is visible on the network. It is the 'volume' name that you will use when connecting to the shared directory.

Path: This is the name of the Folder that appears on the Optimizer that will be used to store files.

Allowed users: You can limit the users that have access to the files in the Path Folder by assigning usernames and passwords to selected individuals (see Add Users below). Enter the usernames here, separated by a comma if more than one user will have access to the files.

Read-only: Use this checkbox to protect the files in the Path Folder from being changed.

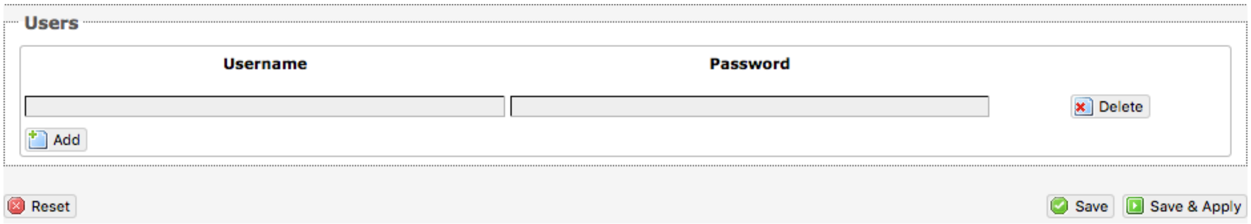
Allow guests: Use this checkbox to make the files available to anyone with network access. With this box checked, users will not be prompted to enter a username and password when accessing the Path Folder.

Delete: Use this to delete the Shared Directory.

Select <Save & Apply>.

5.8.2 Add Users

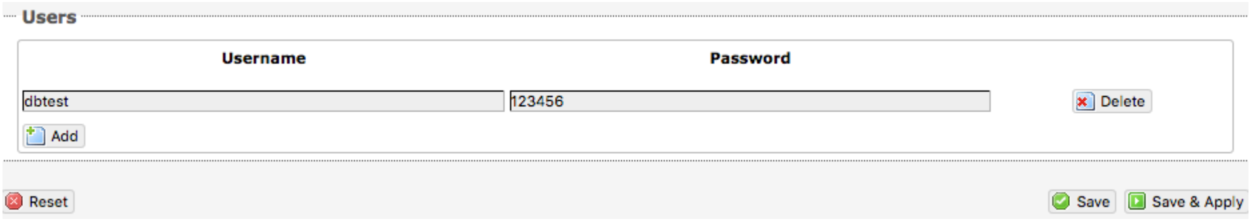
If you want to password protect access to the Shared Directories, you can assign usernames and passwords to each directory.



Users

Username	Password	
		Delete

Select <Add> to add a new username and password.



Users

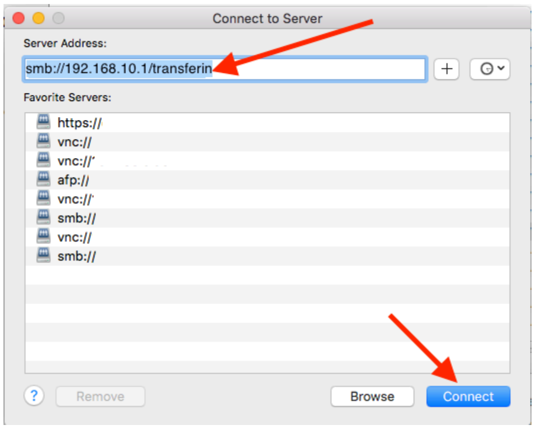
Username	Password
dbtest	123456

Select <Save & Apply>.

5.8.3 How to Access the Shared Directory and Path Folders:

5.8.3.1 From a Mac PC

Go to Finder > Go > Connect to Server



Connect to Server

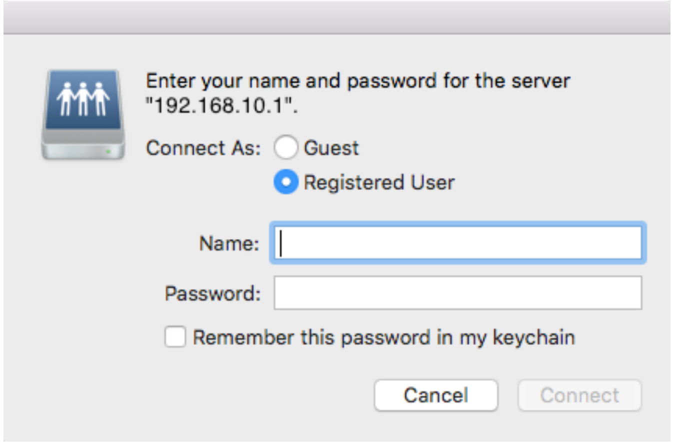
Server Address: smb://192.168.10.1/transferin

Favorite Servers:

- https://
- vnc://
- vnc://
- afp://
- vnc://
- smb://
- vnc://
- smb://

Enter the Server Address as the LAN address for the Optimizer / plus the Path Folder.

Select <Connect>



Enter your name and password for the server "192.168.10.1".

Connect As: ○ Guest
● Registered User

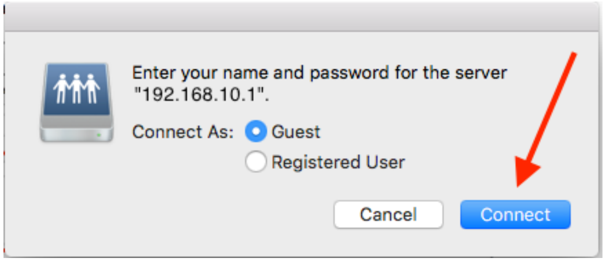
Name:

Password:

□ Remember this password in my keychain

If the Shared Directory is restricted (i.e. does not Allow Guests) you must enter a username and password to access the files.

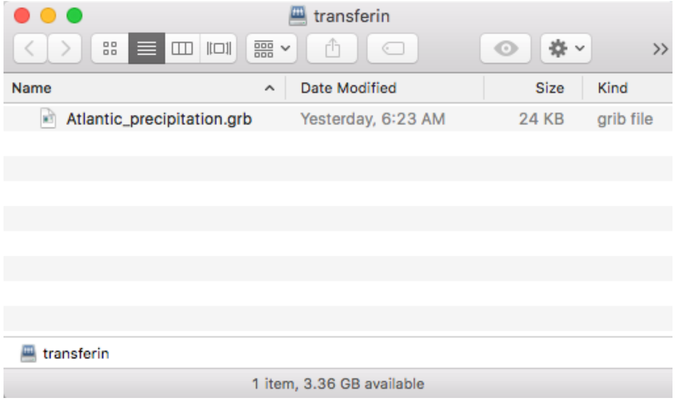
If the Shared Directory is not restricted (i.e. Allow Guests is checked in Network Shares) you can connect as a Guest without entering a username and password.



Enter your name and password for the server "192.168.10.1".

Connect As: ● Guest

○ Registered User



transferin

Name	Date Modified	Size	Kind
Atlantic_precipitation.grb	Yesterday, 6:23 AM	24 KB	grib file

transferin

1 item, 3.36 GB available

A Finder window opens to the selected Folder for access to the transferred file(s).

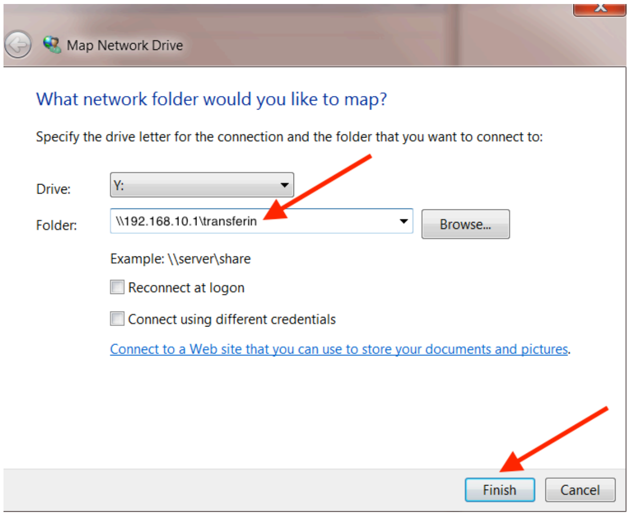
5.8.3.2 From a Windows PC

Map a Network drive to the appropriate location.

Go to Start Menu > Computer > Map Network Drive

In the Folder box, following the Example, enter \\the LAN address for the Optimizer\the Path Folder.

Select <Finish>.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

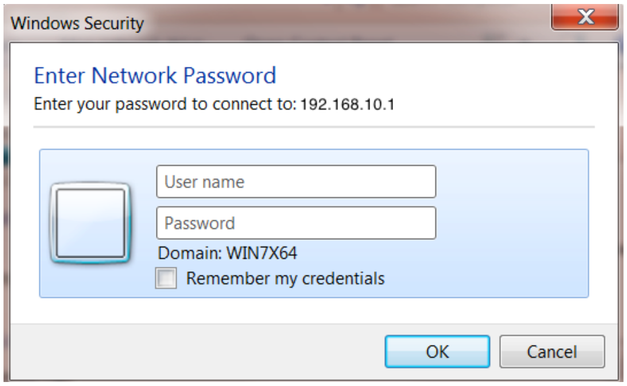
Folder: \\192.168.10.1\transferin

Example: \\server\share

□ Reconnect at logon

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.



Windows Security

Enter Network Password

Enter your password to connect to: 192.168.10.1

User name

Password

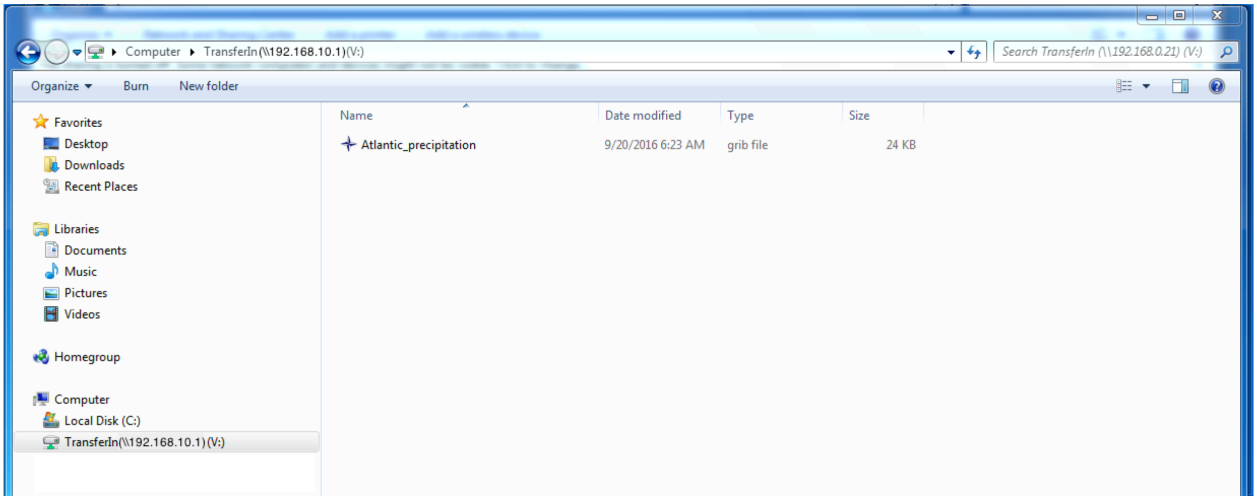
Domain: WIN7X64

□ Remember my credentials

If the Shared Directory is restricted (i.e. does not Allow Guests) you must enter a username and password to access the files.

If the Shared Directory is not restricted (i.e. Allow Guests is checked in Network Shares) you can connect as a Guest without entering a username and password.

An Explorer window opens to the selected Folder for access to the transferred file(s).



Computer ▸ TransferIn(\\192.168.10.1)(V:)

Search TransferIn (\\192.168.0.21) (V:)

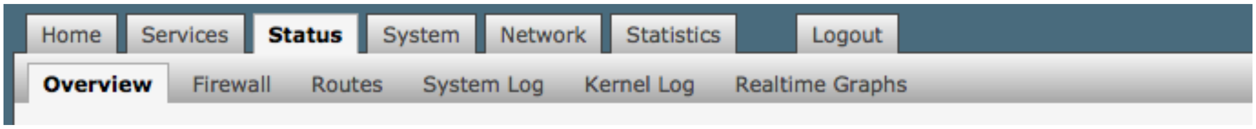
Name	Date modified	Type	Size
Atlantic_precipitation	9/20/2016 6:23 AM	grib file	24 KB

Copyright © Global Marine Networks, LLC

6.0 Status

Available to both 'admin' and 'superadmin' login.

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



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.

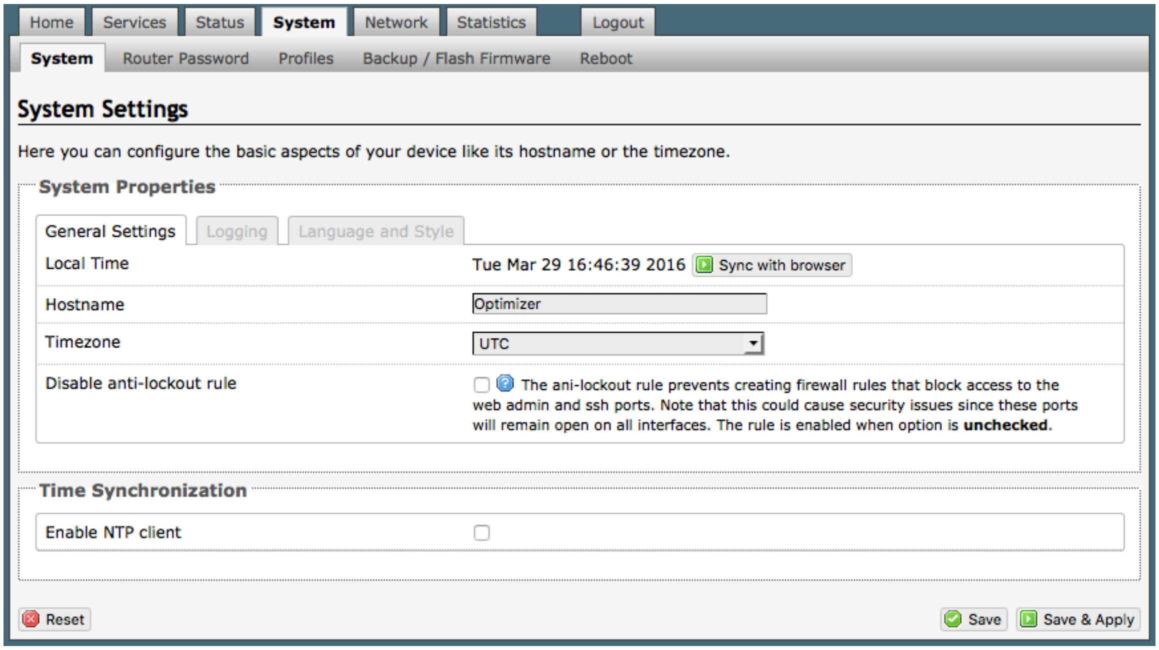
7.0 System

Requires 'superadmin' login.

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

7.1 System Settings

Use this section to configure the basic aspects of your device (i.e hostname and/or timezone).



System Settings

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time	Tue Mar 29 16:46:39 2016
Hostname	Optimizer
Timezone	UTC
Disable anti-lockout rule	□ The ani-lockout rule prevents creating firewall rules that block access to the web admin and ssh ports. Note that this could cause security issues since these ports will remain open on all interfaces. The rule is enabled when option is **unchecked**.

Time Synchronization

Enable NTP client	□

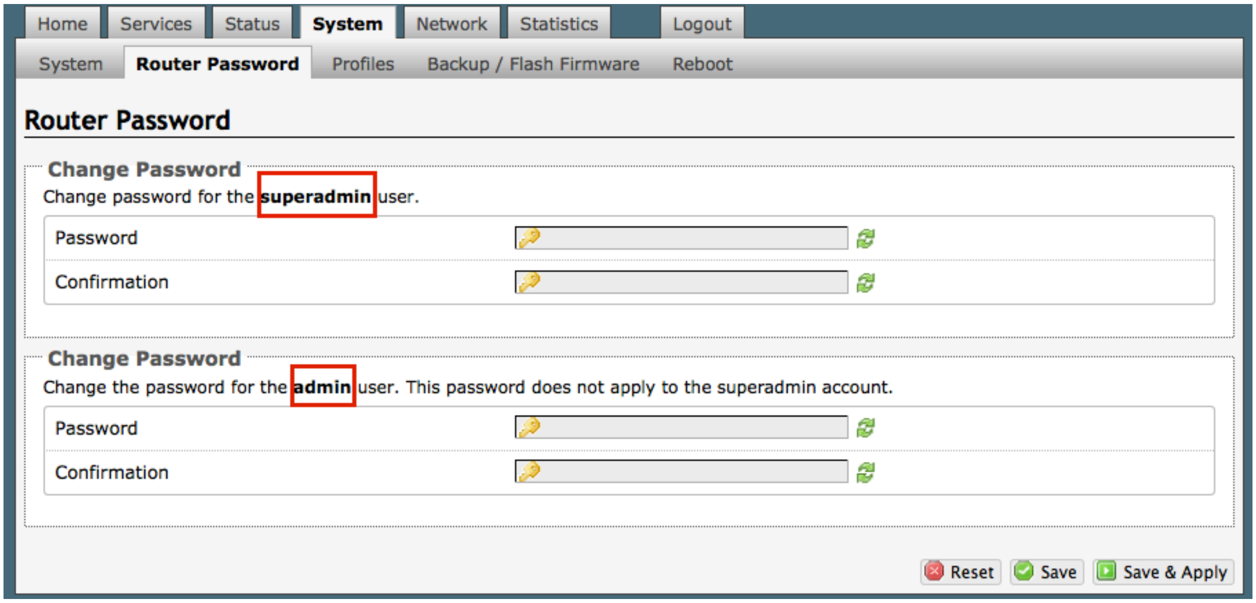
Disable anti-lockout rule: The anti-lock rule prevents you from creating a firewall rule that will lock you out of the router. The rule is Enabled when the box is Unchecked. ***Best Practice is to complete the router configuration, test it thoroughly to make sure everything works as intended, then disable the anti-lock role.***

For example, if you want to be able to login to the router from your office, once the router has been installed on a vessel; if you have WAN blocked and the Anti-Lock Rule is enabled, you will not be able to login. First you want to create a firewall rule to allow the office IP into the router, then "Disable anti-lock rule" by checking the checkbox and now you can Block WAN in the Firewall Rules, if desired.

CAUTION: If you lock yourself out of the router, you must perform a factory reset. This will eliminate your custom configuration requiring you to start a new configuration.

7.2 Router Password

The default password to access the Optimizer User Interface for both the "superadmin" login and the "admin" login are set to: "webxaccess". The onsite administrator using the "admin" login can change the password for the "admin" login only, from the Home Page. Anyone using the 'superadmin" login can change the password for both "admin" and "superadmin" login.



Router Password

Change Password

Change password for the **superadmin** user.

Password

Confirmation

Change Password

Change the password for the **admin** user. This password does not apply to the superadmin account.

Password

Confirmation

Use the top section to change the password for the 'superadmin' user; the bottom section to change the password for the 'admin' user.

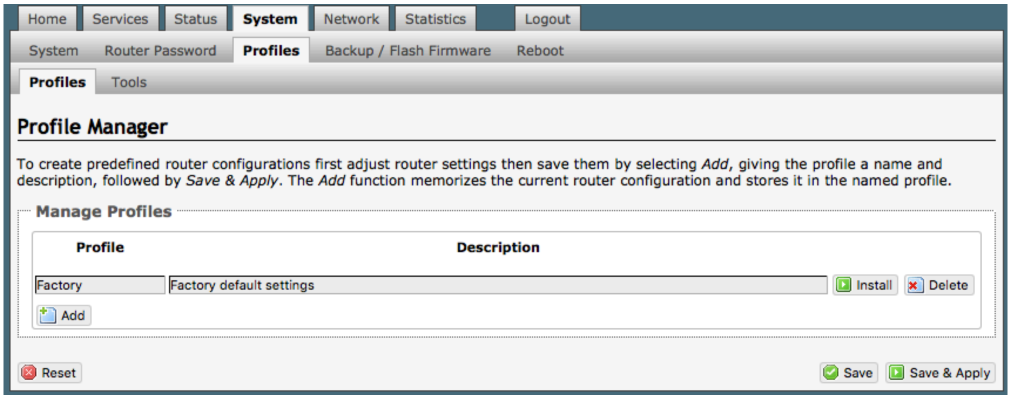
Step 1. Enter the new password in the password text box.
Step 2. Enter the same password again in the Confirmation text box.
Step 3. Click <Save & Apply>

This procedure changes the password for the Superadmin or the Admin login ONLY. When connecting a computer, iOS or Android device to the wireless network, do NOT use either of these login passwords. These passwords are used only to access the Optimizer User Interface.

7.3 Profiles

Requires 'superadmin' login.

Profiles is designed for users of multiple satellite devices and integrators of custom installations.



Profile Manager

To create predefined router configurations first adjust router settings then save them by selecting *Add*, giving the profile a name and description, followed by *Save & Apply*. The *Add* function memorizes the current router configuration and stores it in the named profile.

Manage Profiles

Profile	Description
Factory	Factory default settings

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 appropirate one for the satellite device being used.

Once a profile is saved it can be exported for use in another Optimizer Voice router.

7.3.1 Add a Profile

Before adding a Profile, complete the router configuration.

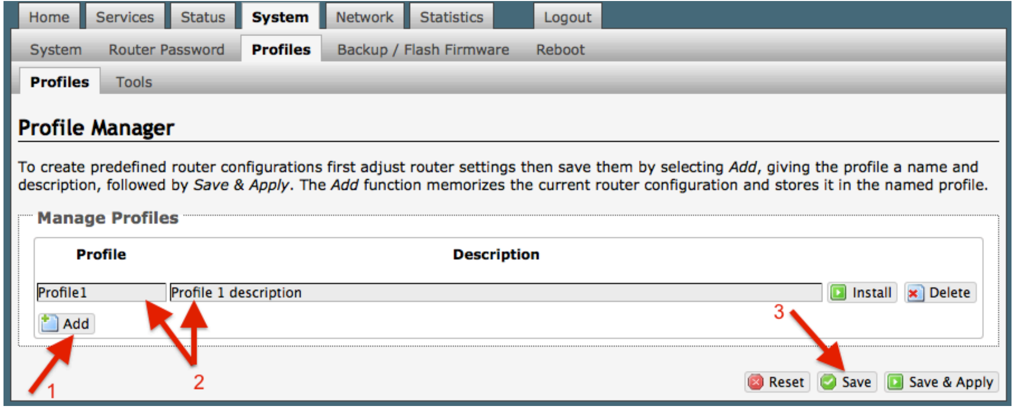
Then access the Profile Manager.

To create and use the new Profile:

1. Select <Add>

2. Enter a Name of the new profile and a description.

3. Select <Save & Apply>.



Profile Manager

To create predefined router configurations first adjust router settings then save them by selecting *Add*, giving the profile a name and description, followed by *Save & Apply*. The *Add* function memorizes the current router configuration and stores it in the named profile.

Manage Profiles

Profile	Description
Profile1	Profile 1 description

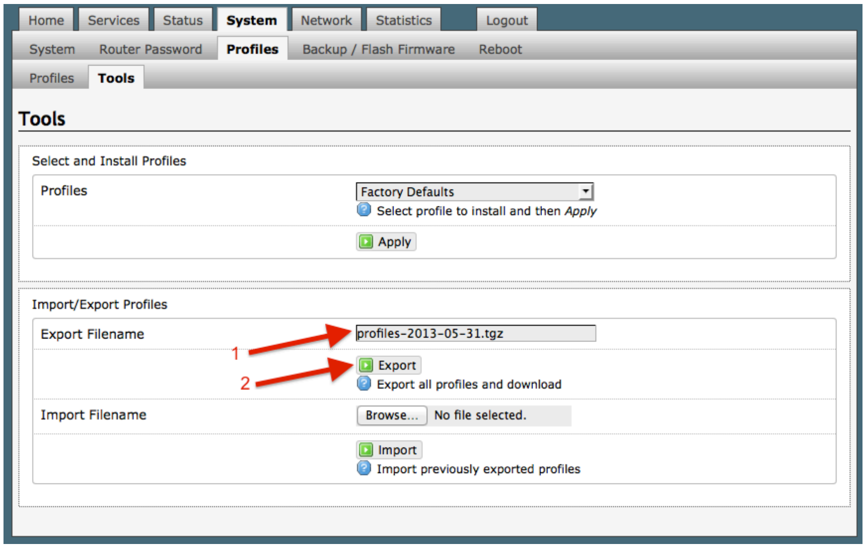
Copyright © Global Marine Networks, LLC

7.3.2 Change to Another Saved Profile

To change from using one profile to different profile, simply select <Install> for the desired profille, then <Save & Apply>

7.3.3 Export a Profile

You can export the profiles from the router and use the exported file to 'clone' another Optimizer Voice router in System > Profiles > Tools.



Profiles: Factory Defaults
Select profile to install and then *Apply*

Export Filename: profiles-2013-05-31.tgz
Export all profiles and download

Import Filename: No file selected.
Import previously exported profiles

1. Enter a filename or use the default name.

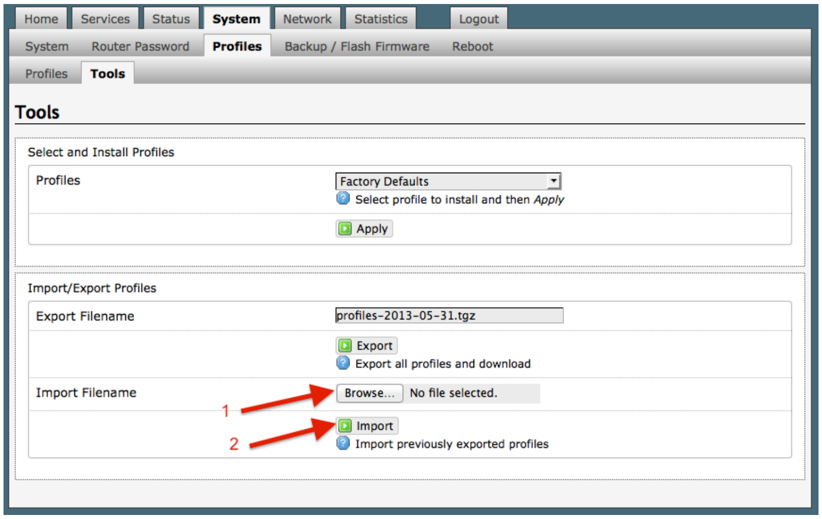
2. Select <Export> and save the file.

7.3.4 Import a Profile

You can import profiles from another Optimizer Voice router in System > Profiles > Tools.

1. Select <Browse> to locate the saved profiles .tgz file.

2. Select <Import>



Profiles: Factory Defaults
Select profile to install and then *Apply*

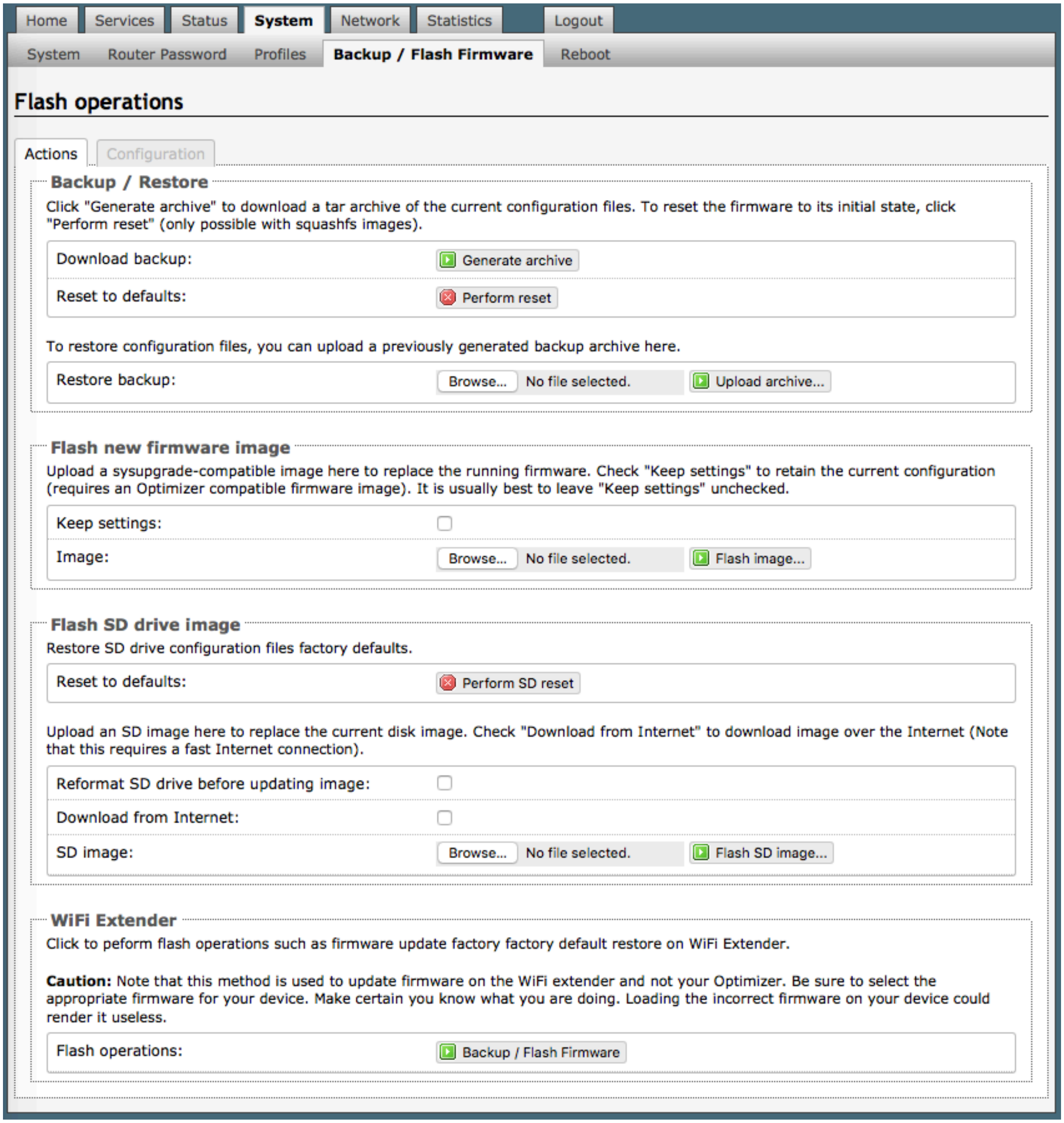
Export Filename: profiles-2013-05-31.tgz
Export all profiles and download

Import Filename: No file selected.
Import previously exported profiles

7.4 Backup/Flash Firmware

Requires 'superadmin' login.

Use this screen to generate backups of current configuration files, resets, restores, and firmware upgrades.



Flash operations

Actions | Configuration

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: [Generate archive]

Reset to defaults: [Perform reset]

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: [Browse...] No file selected. [Upload archive...]

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Optimizer compatible firmware image). It is usually best to leave "Keep settings" unchecked.

Keep settings: □

Image: [Browse...] No file selected. [Flash image...]

Flash SD drive image

Restore SD drive configuration files factory defaults.

Reset to defaults: [Perform SD reset]

Upload an SD image here to replace the current disk image. Check "Download from Internet" to download image over the Internet (Note that this requires a fast Internet connection).

Reformat SD drive before updating image: □

Download from Internet: □

SD image: [Browse...] No file selected. [Flash SD image...]

WiFi Extender

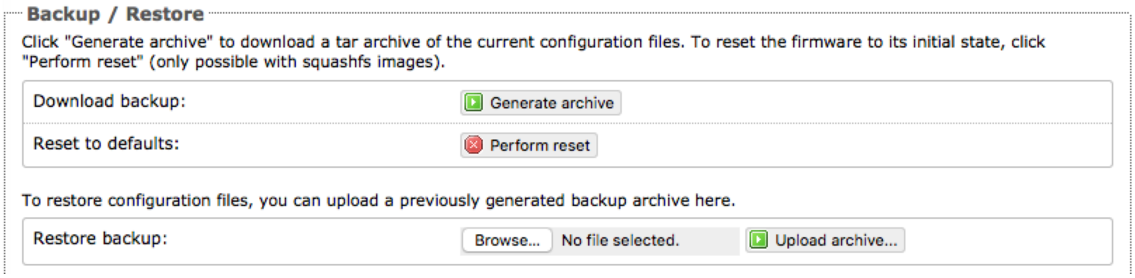
Click to peform flash operations such as firmware update factory factory default restore on WiFi Extender.

Caution: Note that this method is used to update firmware on the WiFi extender and not your Optimizer. Be sure to select the appropriate firmware for your device. Make certain you know what you are doing. Loading the incorrect firmware on your device could render it useless.

Flash operations: [Backup / Flash Firmware]

Copyright © Global Marine Networks, LLC

7.4.1 Backup/Restore



Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

Reset to defaults:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:

No file selected.

Download backup: Create and save a Backup archive of the current configuration.

Restore backup: Restore the router to a previously saved configuration.

Reset to defaults: Reset the router to the default configuration.

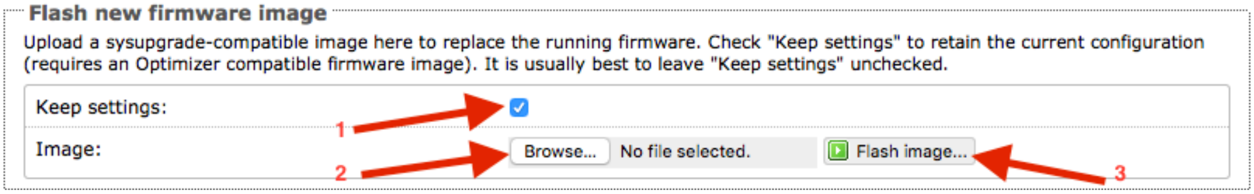
To apply the same configuration among several Optimizer Voice routers (for example in a fleet situation) create and save a Profile of the configuration that can be applied to other Optimizer Voice routers*. See Chapter 7.3.*

7.4.2 Flash New Firmware Image

Get the latest Optimizer firmware version from here:
http://www.redportglobal.com/support/technical-downloads/

Save the .bin file to your computer (pc or mac)

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



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Optimizer compatible firmware image). It is usually best to leave "Keep settings" unchecked.

Keep settings: ☑

Image: Browse... No file selected.

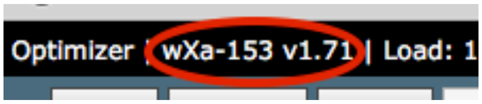
1. **Keep Settings**: check this box to maintain current settings if you have made changes to the congifuration. Failure to check this box will revert the Optimizer back to the default settings.

2. **<Browse>** to where you saved the .bin file and select that file. ***CAUTION: Loading incorrect firmware on your device could render it useless. Be sure to select the appropriate firmware for your device.***

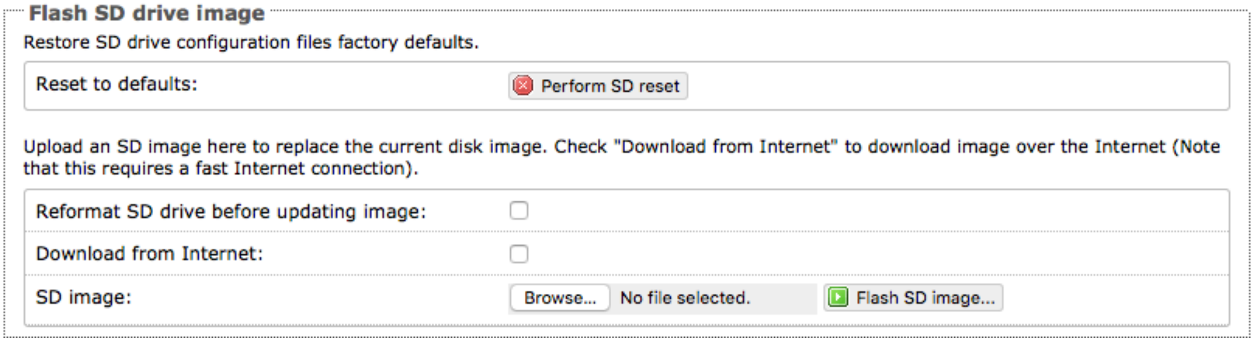
3. **<Flash Image>**

4. Wait for the lights on the front of the Optimizer to begin flashing. When the flashing lights stop, the firmware update is complete. 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.



7.4.3 Flash SD Drive Image



Flash SD drive image

Restore SD drive configuration files factory defaults.

Reset to defaults:	☒ Perform SD reset

Upload an SD image here to replace the current disk image. Check "Download from Internet" to download image over the Internet (Note that this requires a fast Internet connection).

Reformat SD drive before updating image:	□
Download from Internet:	□
SD image:	Browse... No file selected. Flash SD image...

Reset to defaults: Restores the SD drive configuration to its default state.

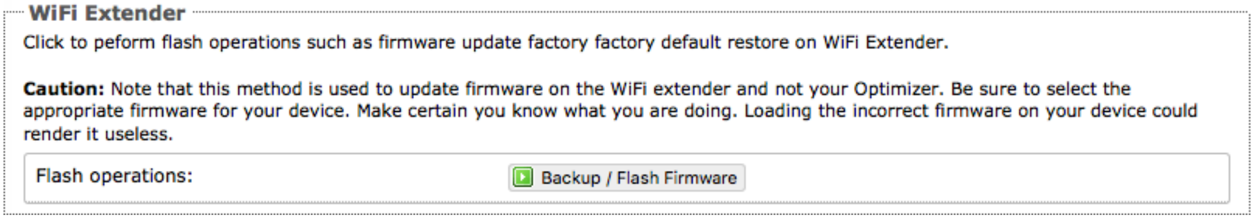
Reformat SD drive before updating image: If the SD drive goes bad, use this to reformat the drive before updating the image.

Download from Internet: Use this only if you have a fast Internet connection to obtain the file. As an alternative, you can obtain the disk image file from our website and save it for use: http://www.redportglobal.com/support/technical-downloads/

SD image: Select <Browse> if you have the file saved to your computer. Select <Flash SD Image> to start the flash process.

7.4.4 WiFi Extender

Requires 'superadmin' login.



WiFi Extender

Click to peform flash operations such as firmware update factory factory default restore on WiFi Extender.

Caution: Note that this method is used to update firmware on the WiFi extender and not your Optimizer. Be sure to select the appropriate firmware for your device. Make certain you know what you are doing. Loading the incorrect firmware on your device could render it useless.

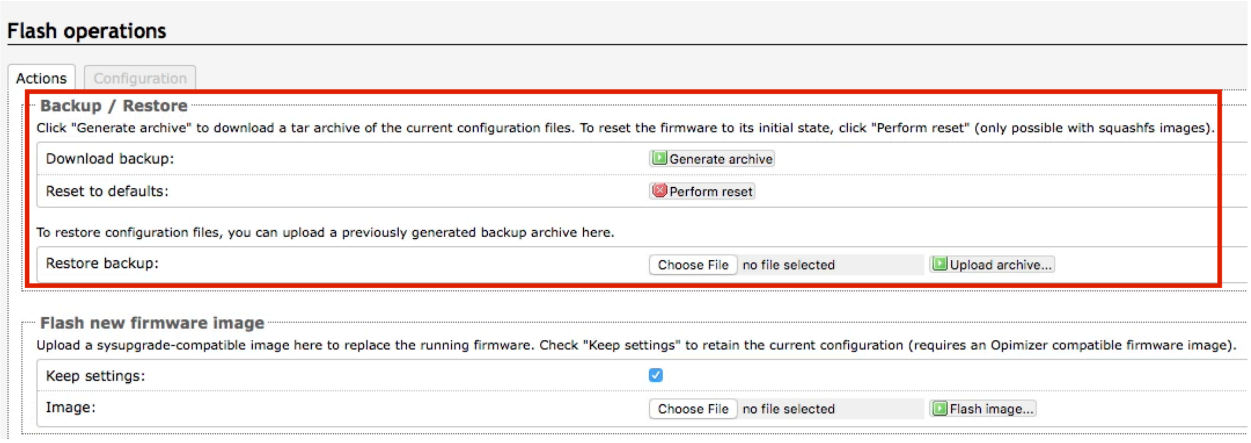
Flash operations:	Backup / Flash Firmware

Use this to backup the configuration settings and/or update the firmware for the RedPort WiFi Extender ONLY!

Select <Backup/Flash Firmware> to open the Flash operations screen.

Copyright © Global Marine Networks, LLC

7.4.4.1 Backup / Restore WiFi Extender



Flash operations

Actions | Configuration

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Choose File no file selected Upload archive...

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Opimizer compatible firmware image).

Keep settings: ☑

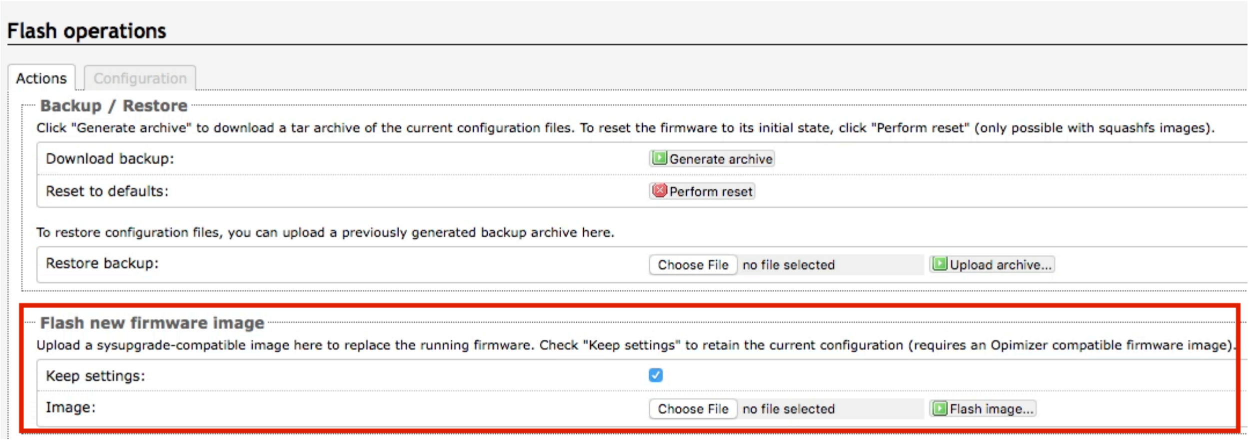
Image: Choose File no file selected Flash image...

Download Backup: select <Generate archive> to create a backup of the current configuration of the WiFi Extender. A backup file (.tar) will be generated and saved to your computer.

Reset to defaults: select <Perform reset> to reset the WiFi Extender to the factory defaults.

Restore backup: select <Choose File> to browse and select the .tar backup file. Select <Upload archive> to restore.

7.4.4.2 Flash New Firmware Image - WiFi Extender



Flash operations

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:	Generate archive
Reset to defaults:	Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:	Choose File no file selected Upload archive...

Flash new firmware image

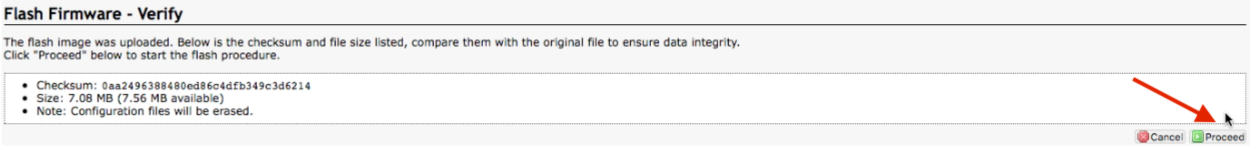
Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Opimizer compatible firmware image).

Keep settings:	☑
Image:	Choose File no file selected Flash image...

Keep Settings: select this only if you want to retain the current configuration.

Image: you must have the new firmware image saved to your computer. You can obtain the latest WiFi Extender Firmware image from our website: www.redportglobal.com/support/technical-downloads/

Select <Choose File> to browse and select the .bin firmware image file. Select <Flash Image> to start the flash operation.



Flash Firmware - Verify

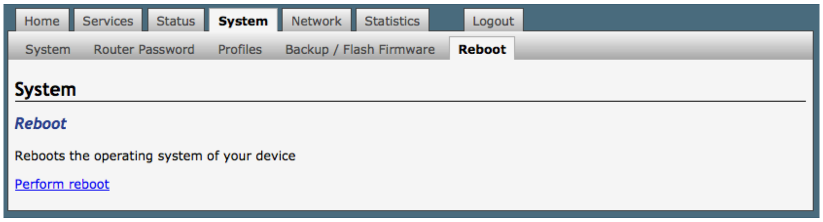
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Checksum: 0aa2496388480ed86c4dfb349c3d6214
- Size: 7.08 MB (7.56 MB available)
- Note: Configuration files will be erased.

Select <Proceed> to complete the process.

7.5 Reboot

You can reboot the Optimizer from within the user interface in lieu of using the reset button on the router itself.



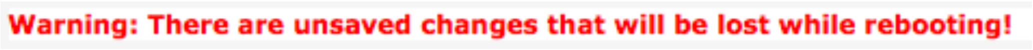
System

Reboot

Reboots the operating system of your device

Perform reboot

If you have made changes to the configuration without selecting <Save & Apply> you will receive a Warning message:



Warning: There are unsaved changes that will be lost while rebooting!

Copyright © Global Marine Networks, LLC

8.0 Network

Requires 'superadmin' login.

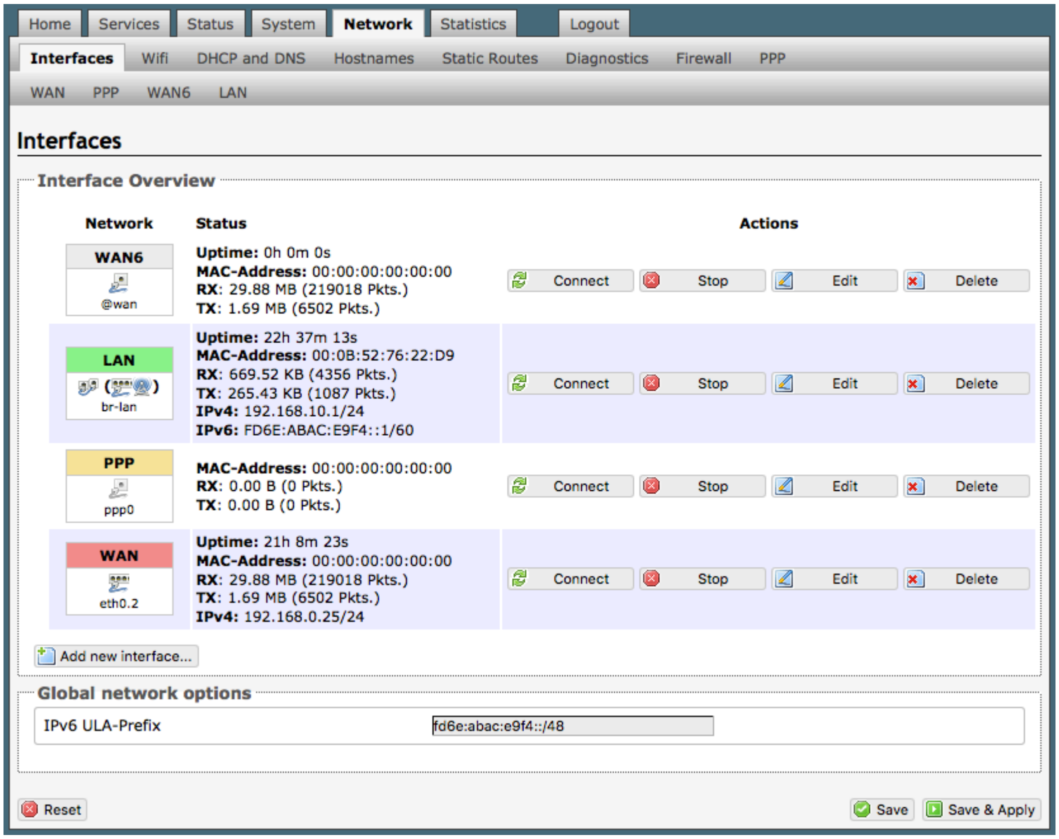
Use this section to configure network interfaces, run diagnostics, or modify the firewall.

CAUTION: This gives you complete control over the router behavior.

BEST PRACTICE: Modifications to the default configuration is best left to those with a full understanding of router/network behavior, firewall rules, etc. Creating conflicts in the configuration may render the router useless.

8.1 Interfaces Overview

This screen is an at-a-glance view of the current status of each network interface and provide easy access to edit the interface.



Interfaces

Interface Overview

Network	Status	Actions
WAN6 @wan	**Uptime:** 0h 0m 0s **MAC-Address:** 00:00:00:00:00:00 **RX**: 29.88 MB (219018 Pkts.) **TX**: 1.69 MB (6502 Pkts.)	Connect Stop Edit Delete
LAN br-lan	**Uptime:** 22h 37m 13s **MAC-Address:** 00:0B:52:76:22:D9 **RX**: 669.52 KB (4356 Pkts.) **TX**: 265.43 KB (1087 Pkts.) **IPv4:** 192.168.10.1/24 **IPv6:** FD6E:ABAC:E9F4::1/60	Connect Stop Edit Delete
PPP ppp0	**MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
WAN eth0.2	**Uptime:** 21h 8m 23s **MAC-Address:** 00:00:00:00:00:00 **RX**: 29.88 MB (219018 Pkts.) **TX**: 1.69 MB (6502 Pkts.) **IPv4:** 192.168.0.25/24	Connect Stop Edit Delete

Global network options

IPv6 ULA-Prefix: fd6e:abac:e9f4::/48

Copyright © Global Marine Networks, LLC

LAN: this is reserved for the local area network (onsite).

PPP: this is reserved for USB connected satellite phones and GSM or LTE modems.

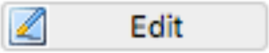
WAN: this is typically used for the primary satellite system.

WEXT: this is reserved for the RedPort WiFi Extender.

8.1.1 Interface Actions

Enable an interface.

Disable an interface.



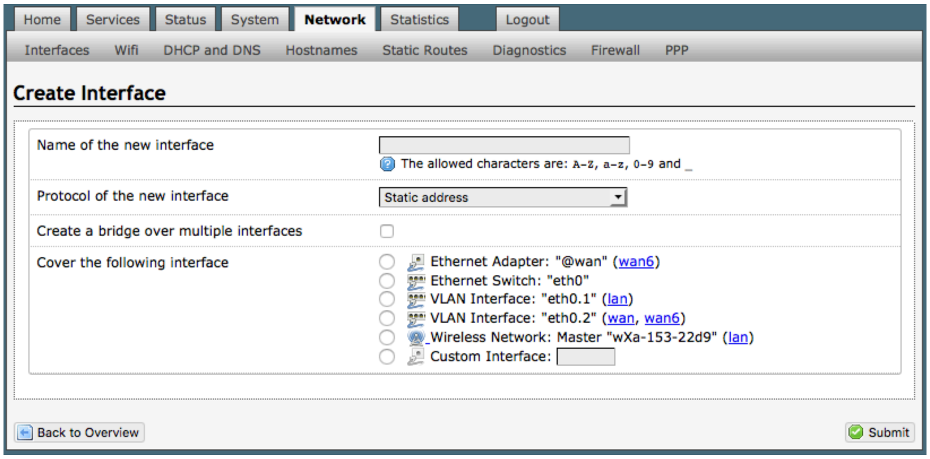
Modify the configuration of the interface.

Remove the interface. ***CAUTION: This action cannot be Undone!***

8.1.2 Add a New Interface

To add a new interface select the <Add new interface> button on the Interface Overview page.

Complete the Create Interface screen and select <Submit> to apply the change. Once configured, the new interface will show on the Interface Overview screen and it will have its own Tab at the top of the Interface Overview page.



Create Interface

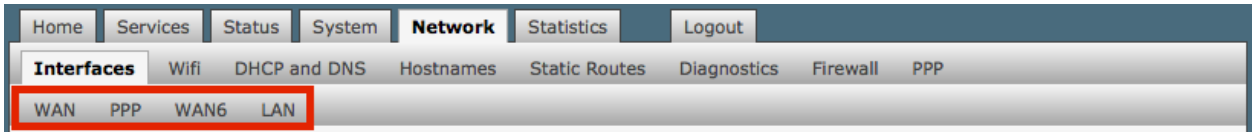
Name of the new interface	The allowed characters are: A-Z, a-z, 0-9 and _
Protocol of the new interface	Static address
Create a bridge over multiple interfaces	□
Cover the following interface	○ Ethernet Adapter: "@wan" (wan6) ○ Ethernet Switch: "eth0" ○ VLAN Interface: "eth0.1" (lan) ○ VLAN Interface: "eth0.2" (wan, wan6) ○ Wireless Network: Master "wXa-153-22d9" (lan) ○ Custom Interface:

The name of the new interface must not match the name of a current interface or rule.

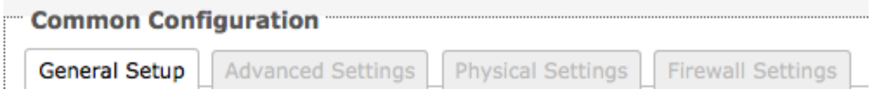
If adding a new WAN Interface, be sure to Edit the Interface to complete the configuration.

8.1.3 Select Interfaces Tabs

Use these tabs to select an interface for configuration and/or modification.



Use these pages to configure the network interfaces.

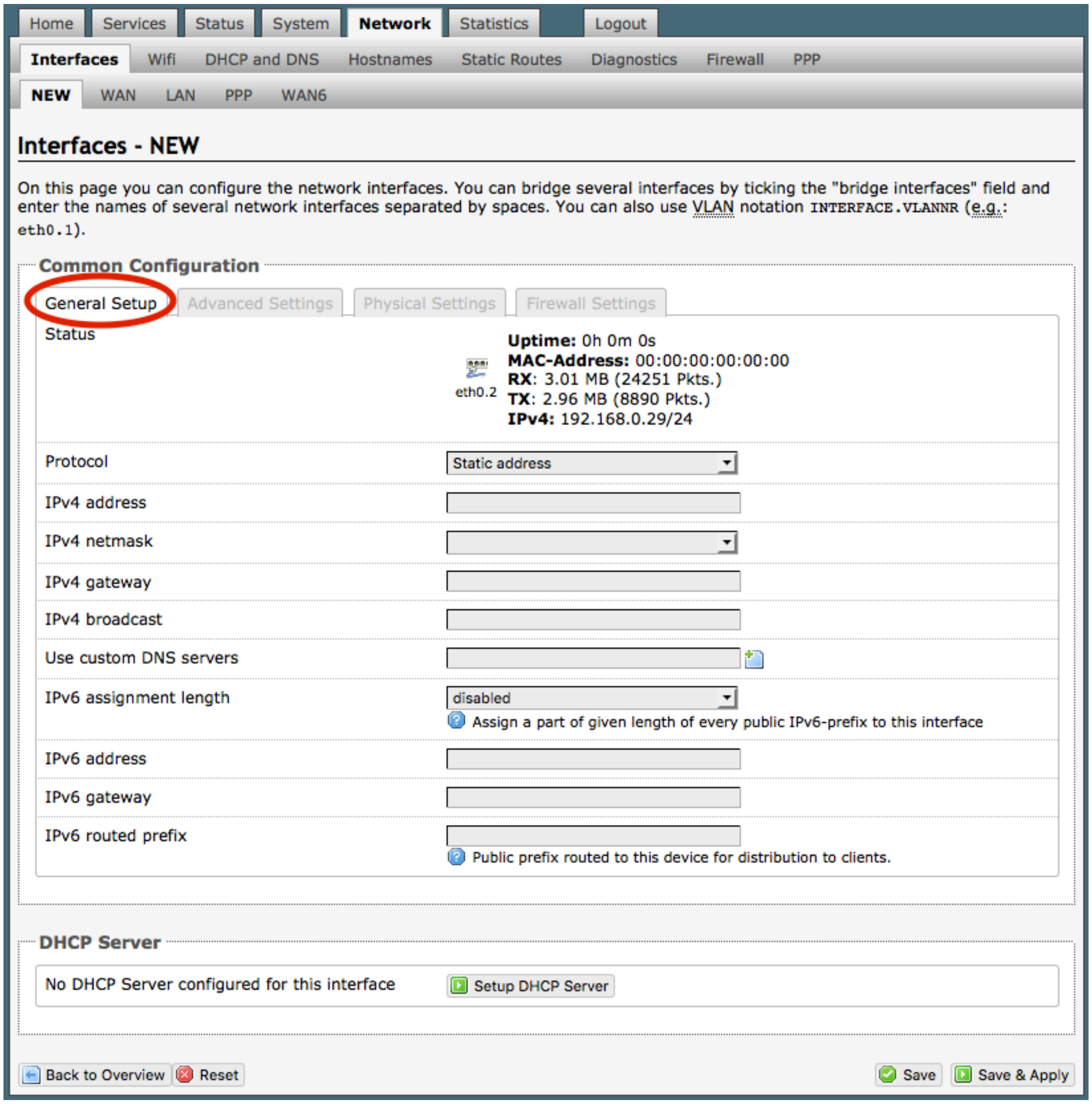


The information and selections available will depend upon the Protocol selection for that interface.

Copyright © Global Marine Networks, LLC

8.1.3.1 General Setup

Use General Setup to switch the protocol for the interface and configure the setup for that protocol including Static IP Addresses, DHCP Server Setup, etc.:



Interfaces - NEW

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status

eth0.2

Uptime: 0h 0m 0s
MAC-Address: 00:00:00:00:00:00
RX: 3.01 MB (24251 Pkts.)
TX: 2.96 MB (8890 Pkts.)
IPv4: 192.168.0.29/24

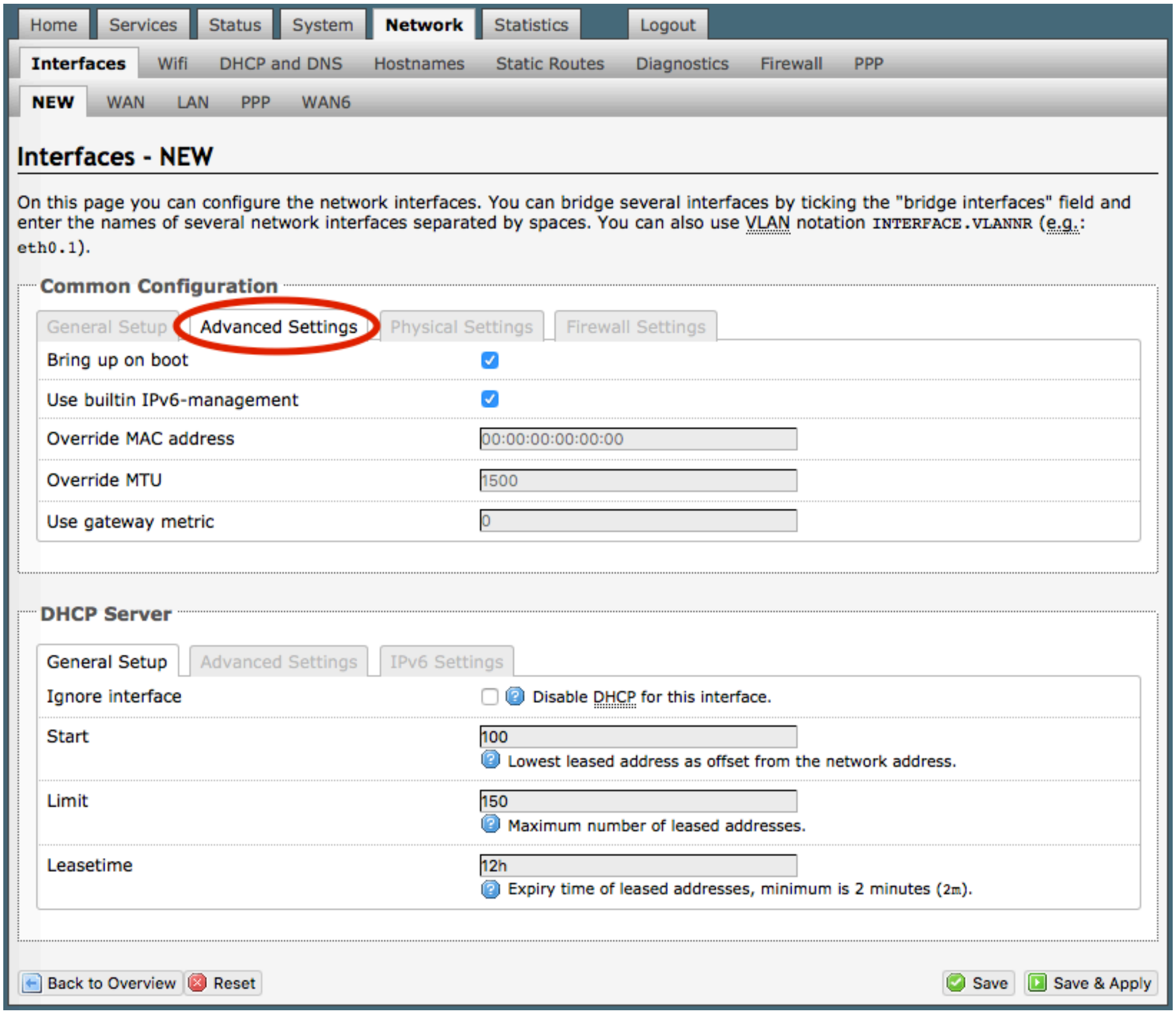
Protocol	Static address
IPv4 address	
IPv4 netmask	
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	
IPv6 assignment length	disabled Assign a part of given length of every public IPv6-prefix to this interface
IPv6 address	
IPv6 gateway	
IPv6 routed prefix	Public prefix routed to this device for distribution to clients.

DHCP Server

No DHCP Server configured for this interface

8.1.3.2 Advanced Settings

Use Advanced Settings if you want to bring up the interface automatically on boot up of the router and to configure the DHCP Server Settings.



Interfaces - NEW

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

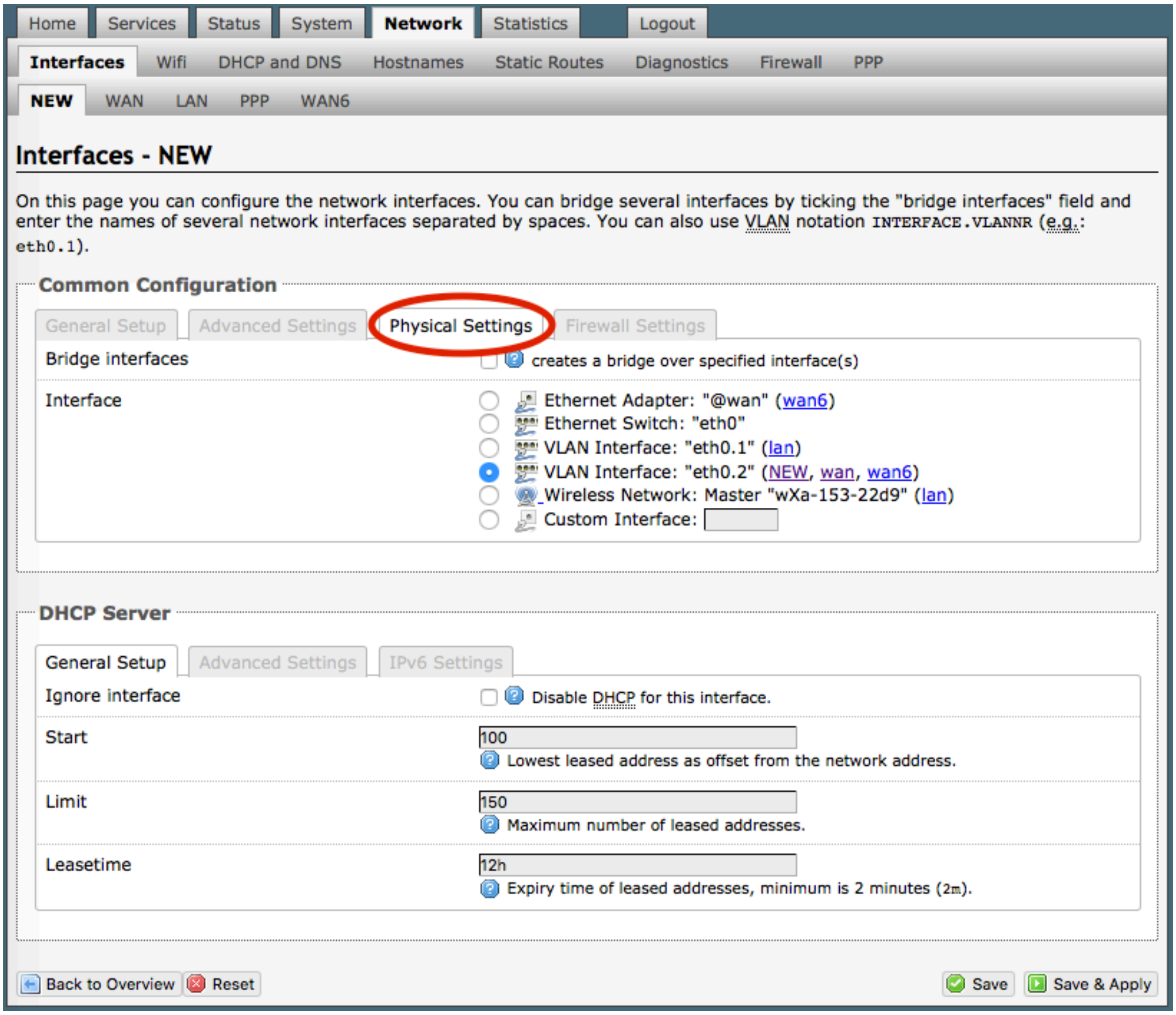
Bring up on boot	☑
Use builtin IPv6-management	☑
Override MAC address	00:00:00:00:00:00
Override MTU	1500
Use gateway metric	0

DHCP Server

Ignore interface	☐ Disable DHCP for this interface.
Start	100 Lowest leased address as offset from the network address.
Limit	150 Maximum number of leased addresses.
Leasetime	12h Expiry time of leased addresses, minimum is 2 minutes (`2m`).

8.1.3.3 Physical Settings

Use this page to bridge interfaces and configure the DHCP Server Settings.



Interfaces - NEW

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bridge interfaces □ creates a bridge over specified interface(s)

Interface
- ○ Ethernet Adapter: "@wan" (wan6)
- ○ Ethernet Switch: "eth0"
- ○ VLAN Interface: "eth0.1" (lan)
- ● VLAN Interface: "eth0.2" (NEW, wan, wan6)
- ○ Wireless Network: Master "wXa-153-22d9" (lan)
- ○ Custom Interface:

DHCP Server

Ignore interface □ Disable DHCP for this interface.

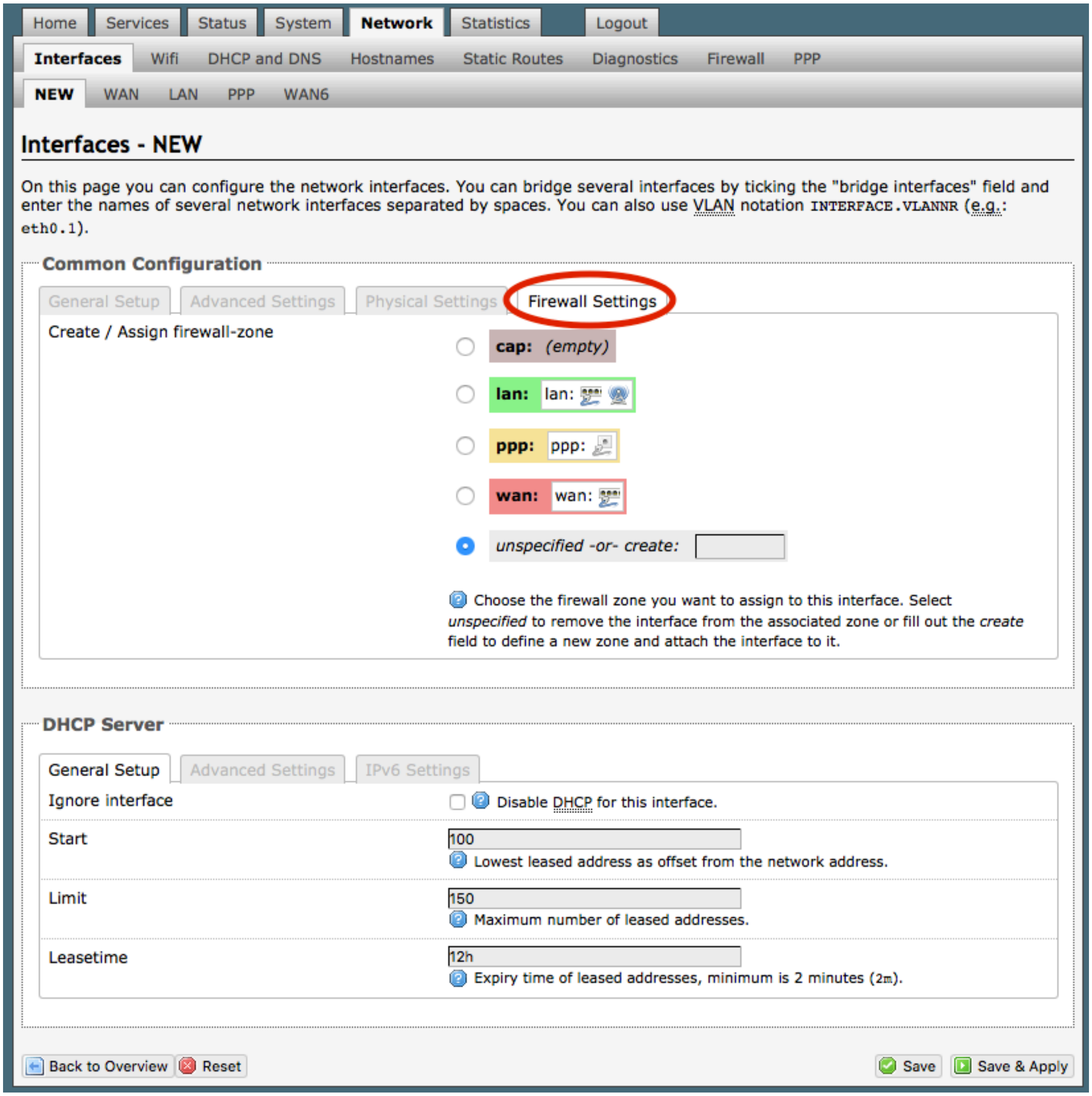
Start: 100
Lowest leased address as offset from the network address.

Limit: 150
Maximum number of leased addresses.

Leasetime: 12h
Expiry time of leased addresses, minimum is 2 minutes (`2m`).

8.1.3.4 Firewall Settings

Use this to select the Firewall Zone you want to assign to the Interface. *See Chapter 8.7 for Firewall Zone details.* You can also configure the DHCP Server Settings from this page.



Interfaces - NEW

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Create / Assign firewall-zone

○ **cap:** *(empty)*

○ **lan:** lan:

○ **ppp:** ppp:

○ **wan:** wan:

● *unspecified -or- create:*

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

DHCP Server

Ignore interface □ Disable DHCP for this interface.

Start 100
Lowest leased address as offset from the network address.

Limit 150
Maximum number of leased addresses.

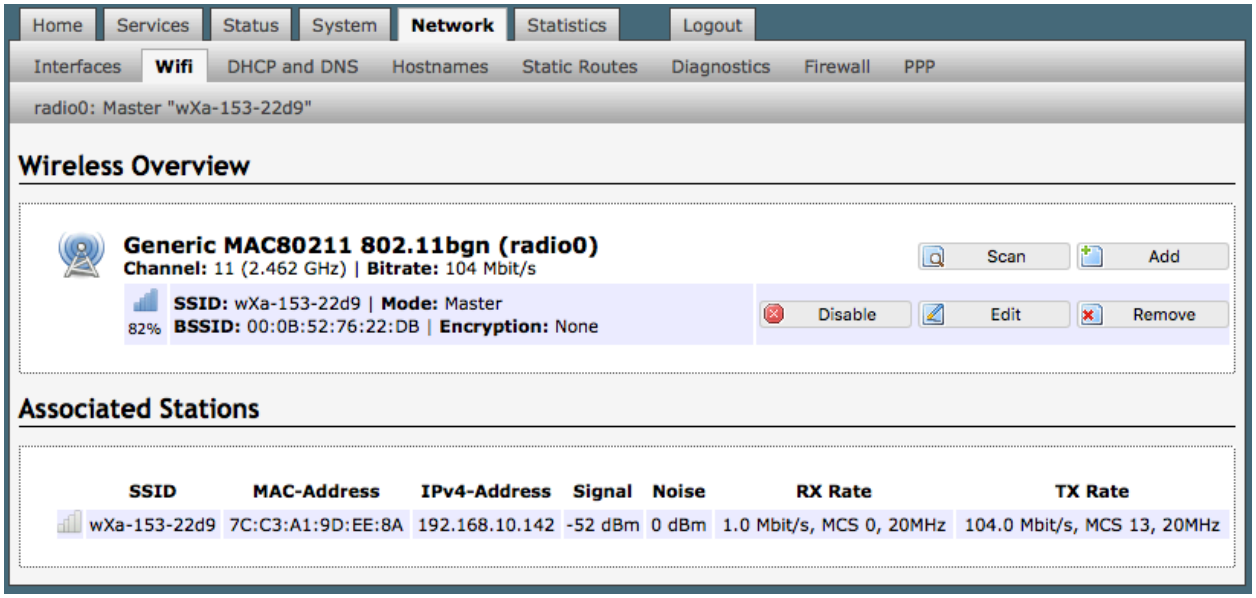
Leasetime 12h
Expiry time of leased addresses, minimum is 2 minutes (`2m`).

Copyright © Global Marine Networks, LLC

8.2 Wifi

Requires "superadmin" login.

This screen shows the current status of the wireless hotspot created by the Optimizer Premier.



radio0: Master "wXa-153-22d9"

Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 104 Mbit/s

SSID: wXa-153-22d9 | **Mode:** Master
BSSID: 00:0B:52:76:22:DB | **Encryption:** None

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
wXa-153-22d9	7C:C3:A1:9D:EE:8A	192.168.10.142	-52 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	104.0 Mbit/s, MCS 13, 20MHz

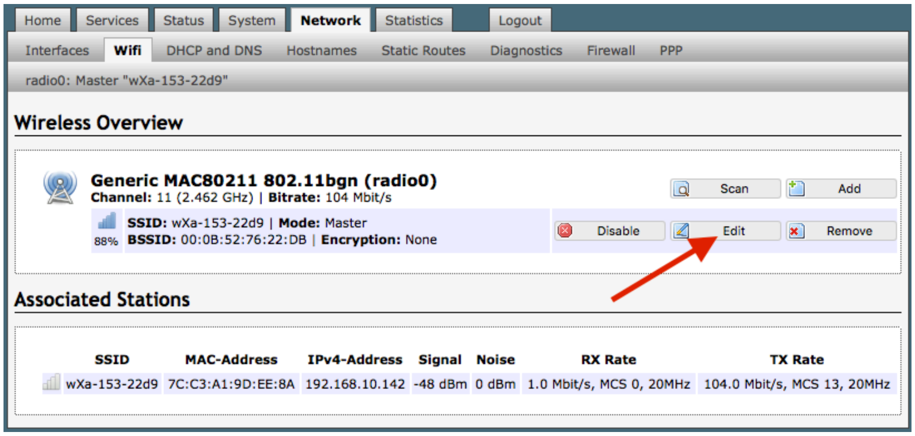
Scan: scans for other wireless hotspot signals available in the area.
Add: Add a new Wifi interface.
Disable: Disable the selected Wifi interface but it remains on the list.
Edit: Edit the selected Wifi interface
Remove: Remove the selected Wifi interface

Copyright © Global Marine Networks, LLC

8.2.1 Rename the Wireless Network

The default name of the Optimizer Premier's wireless network is wXa-153-xxxx where the xxxx represents a unique number. This is the name of the wireless network that you connect to using your computer or iOS or Android device.

It is possible to change the name of your wireless network. Locate the wXa wifi network and select <Edit>



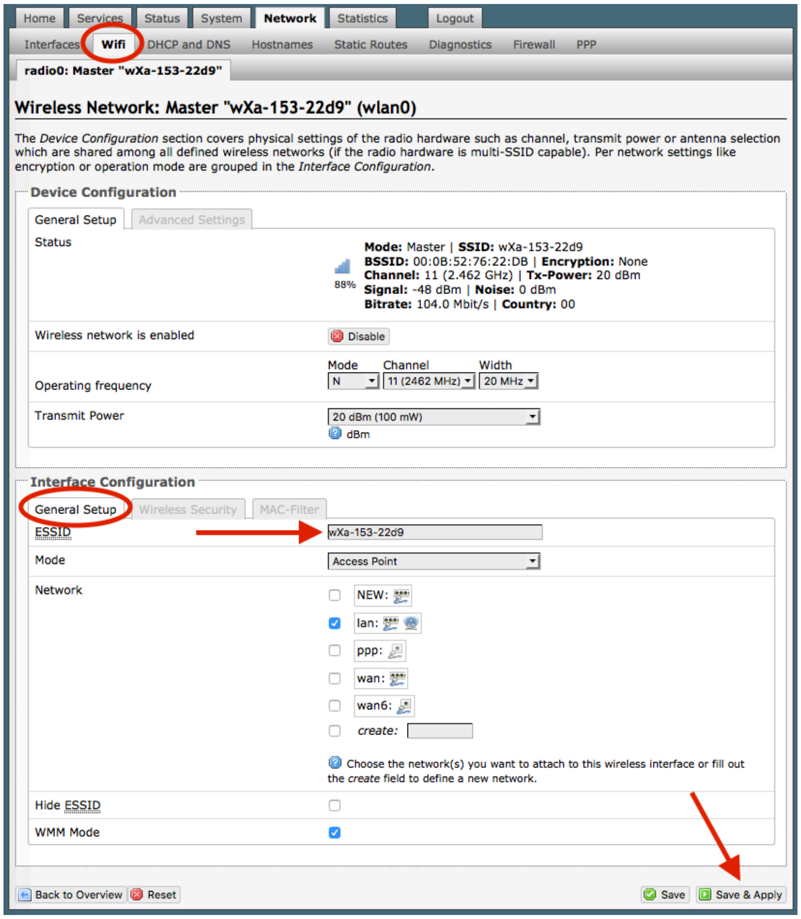
Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 104 Mbit/s

88% **SSID:** wXa-153-22d9 | **Mode:** Master
BSSID: 00:0B:52:76:22:DB | **Encryption:** None

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
wXa-153-22d9	7C:C3:A1:9D:EE:8A	192.168.10.142	-48 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	104.0 Mbit/s, MCS 13, 20MHz



Wireless Network: Master "wXa-153-22d9" (wlan0)

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

Status: 88% **Mode:** Master | **SSID:** wXa-153-22d9
BSSID: 00:0B:52:76:22:DB | **Encryption:** None
Channel: 11 (2.462 GHz) | **Tx-Power:** 20 dBm
Signal: -48 dBm | **Noise:** 0 dBm
Bitrate: 104.0 Mbit/s | **Country:** 00

Wireless network is enabled: Disable

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

Transmit Power: 20 dBm (100 mW)
dBm

Interface Configuration

ESSID: wXa-153-22d9

Mode: Access Point

Network:
☐ NEW:
☑ lan:
☐ ppp:
☐ wan:
☐ wan6:
☐ *create:*

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID: ☐

WMM Mode: ☑

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

2. Click <Save & Apply>

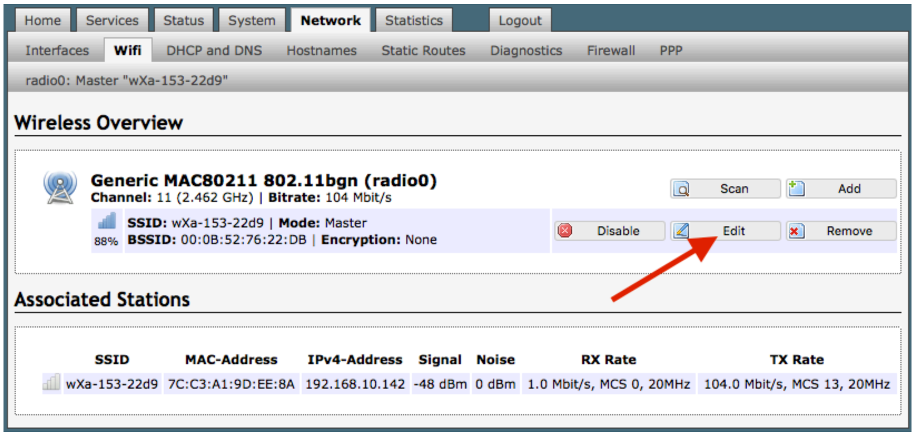
This procedure changes the name for the WiFi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the network name that will appear in the wireless network list. This name does not change the router superadmin or admin name when logging in to access the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

Copyright © Global Marine Networks, LLC

8.2.2 Restrict Wireless Network Access

When in public locations, for example, a busy port, you may want to restrict access to the WiFi hotspot created by your satellite device and the Optimizer. You can password protect the WiFi hotspot so others cannot use it.

Locate the wXa wifi network and select <Edit>.



radio0: Master "wXa-153-22d9"

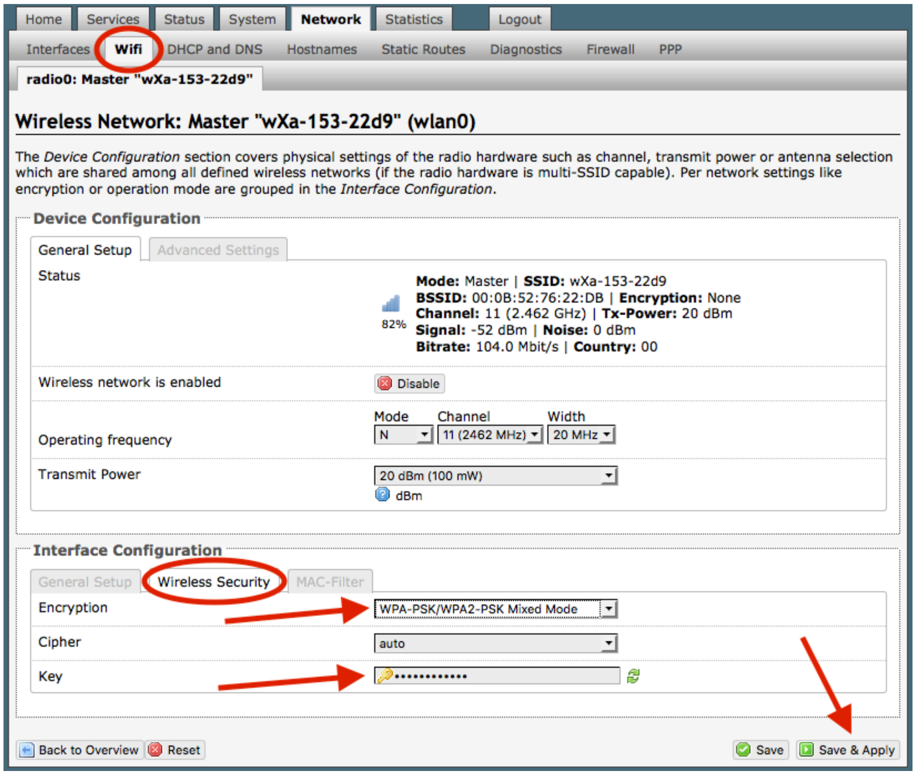
Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 104 Mbit/s

88% **SSID:** wXa-153-22d9 | **Mode:** Master
BSSID: 00:0B:52:76:22:DB | **Encryption:** None

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
wXa-153-22d9	7C:C3:A1:9D:EE:8A	192.168.10.142	-48 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	104.0 Mbit/s, MCS 13, 20MHz



radio0: Master "wXa-153-22d9"

Wireless Network: Master "wXa-153-22d9" (wlan0)

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

Status: 82% **Mode:** Master | **SSID:** wXa-153-22d9
BSSID: 00:0B:52:76:22:DB | **Encryption:** None
Channel: 11 (2.462 GHz) | **Tx-Power:** 20 dBm
Signal: -52 dBm | **Noise:** 0 dBm
Bitrate: 104.0 Mbit/s | **Country:** 00

Wireless network is enabled: Disable

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

Transmit Power: 20 dBm (100 mW) dBm

Interface Configuration

Encryption: WPA-PSK/WPA2-PSK Mixed Mode

Cipher: auto

Key: ••••••••••••

1. Select the Encryption mode from the drop down menu.

2. Enter your desired password in the Key field.

3. Click <Save & Apply>

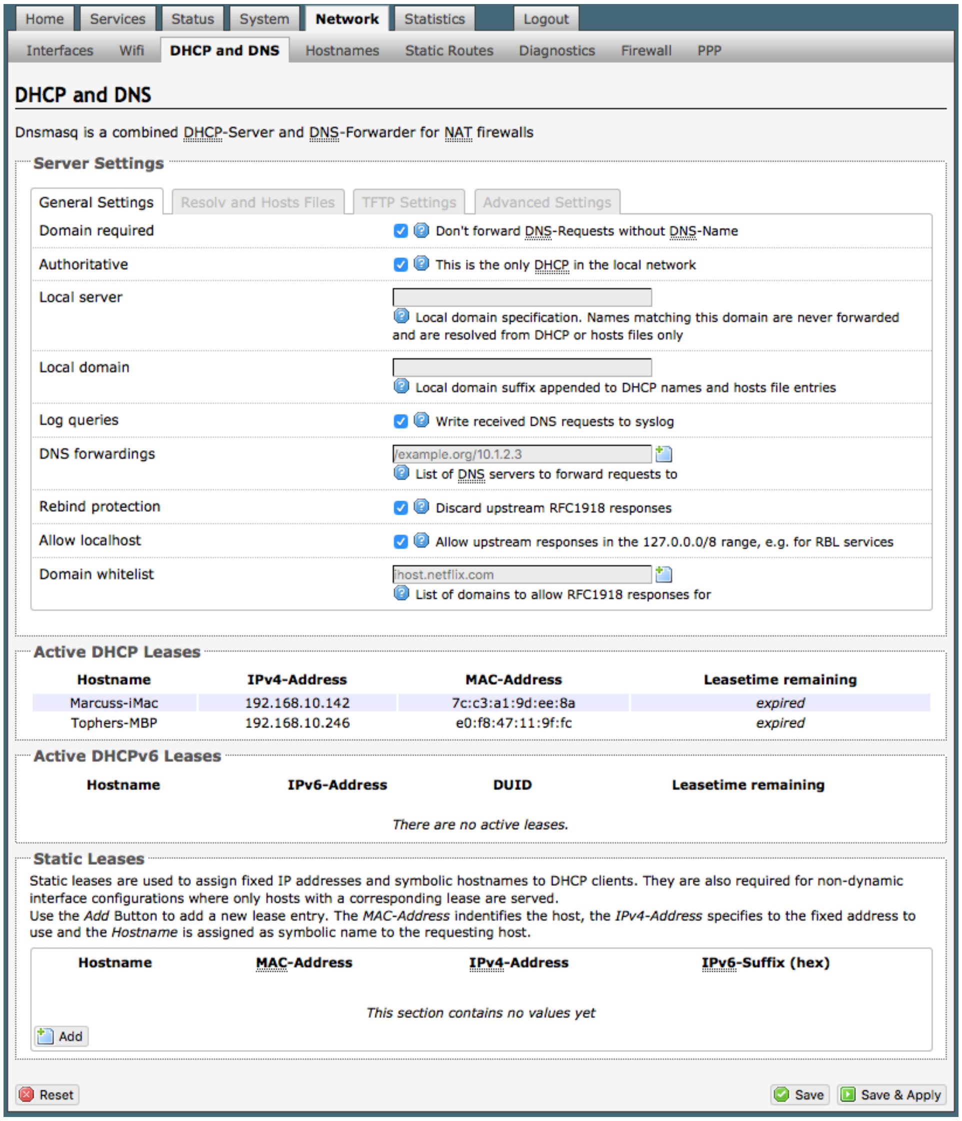
This procedure adds/changes the password for the WiFi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the password you will use. This password does not change the router superadmin or admin password when logging in to access the Optimizer user interface.

Copyright © Global Marine Networks, LLC

8.3 DHCP and DNS

Requires "superadmin" login.

The Optimizer Voice is a DNS server. Under normal operating conditions you should not need to change anything here. If necessary, use this screen to modify the settings, if necessary.



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Domain required	☑ Don't forward DNS-Requests without DNS-Name
Authoritative	☑ This is the only DHCP in the local network
Local server	Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only
Local domain	Local domain suffix appended to DHCP names and hosts file entries
Log queries	☑ Write received DNS requests to syslog
DNS forwardings	/example.org/10.1.2.3 List of DNS servers to forward requests to
Rebind protection	☑ Discard upstream RFC1918 responses
Allow localhost	☑ Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services
Domain whitelist	ihost.netflix.com List of domains to allow RFC1918 responses for

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Marcuss-iMac	192.168.10.142	7c:c3:a1:9d:ee:8a	*expired*
Tophers-MBP	192.168.10.246	e0:f8:47:11:9f:fc	*expired*

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)

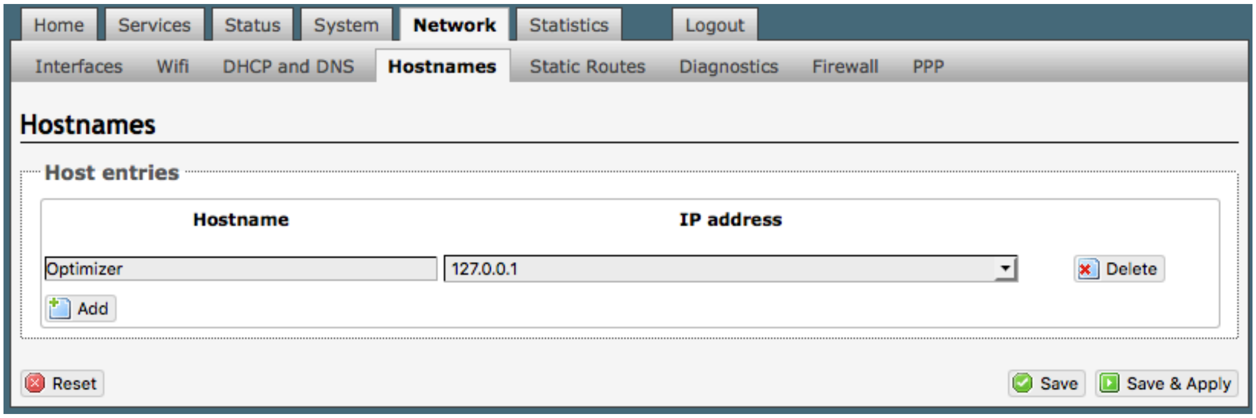
This section contains no values yet

Copyright © Global Marine Networks, LLC

8.4 Hostnames

Requires "superadmin" login.

Use this page to associate a hostname with an IP address.



Hostnames

Host entries

Hostname	IP address
Optimizer	127.0.0.1

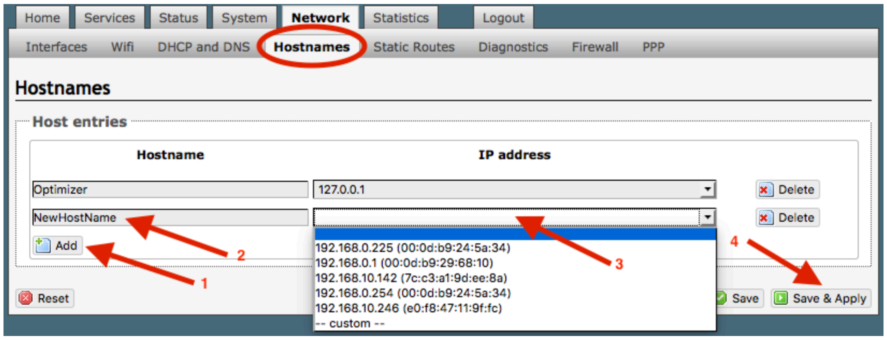
8.4.1 Add Hostname

1. Select <Add>.

2. Enter the new Hostname.

3. Select the IP address from the drop-down list OR select custom to enter the IP address.

4. Select Save & Apply.



Hostnames

Host entries

Hostname	IP address
Optimizer	127.0.0.1
NewHostName	

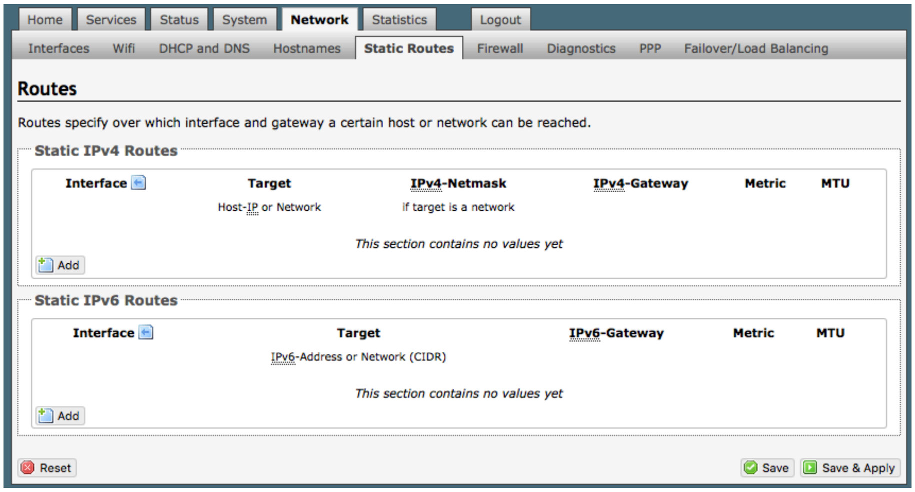
192.168.0.225 (00:0d:b9:24:5a:34)
192.168.0.1 (00:0d:b9:29:68:10)
192.168.10.142 (7c:c3:a1:9d:ee:8a)
192.168.0.254 (00:0d:b9:24:5a:34)
192.168.10.246 (e0:f8:47:11:9f:fc)
-- custom --

Copyright © Global Marine Networks, LLC

8.5 Static Routes

Requires "superadmin" login.

This Static Routes table is available for those with a complex network that may include multiple routers. Use this page to specify how a certain host or network can be reached.



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	MTU

This section contains no values yet

Static IPv6 Routes

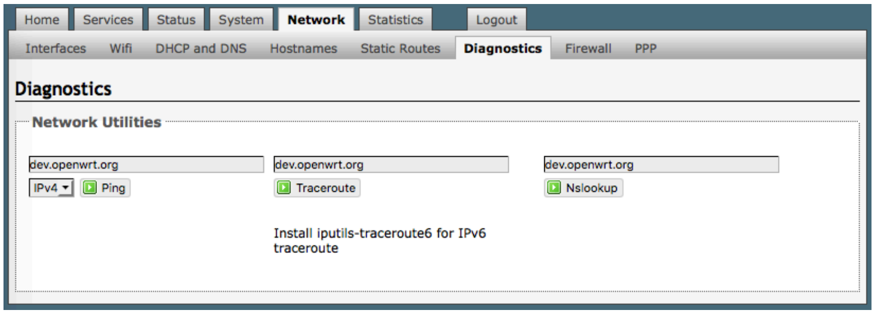
Interface	Target IPv6-Address or Network (CIDR)	IPv6-Gateway	Metric	MTU

This section contains no values yet

8.6 Diagnostics

Requires "superadmin" login.

There are several Diagnostic tools available:



Diagnostics

Network Utilities

dev.openwrt.org

dev.openwrt.org

dev.openwrt.org

Install iputils-traceroute6 for IPv6 traceroute

Ping: tells if you have ip connectivity

Traceroute: returns all ip addresses in a hop to the final destination.

Nslookup: returns the ip address of whatever is entered into the text box.

Copyright © Global Marine Networks, LLC

8.7 Firewall

Requires "superadmin" login.

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.

CAUTION: It is important to have an in-depth understanding of network administration including managment and maintenance of routers, firewalls, etc. before attempting to modify the firewall settings of the Optimizer Premier. USE WITH CAUTION AND AT YOUR OWN RISK!

8.7.1 General Settings

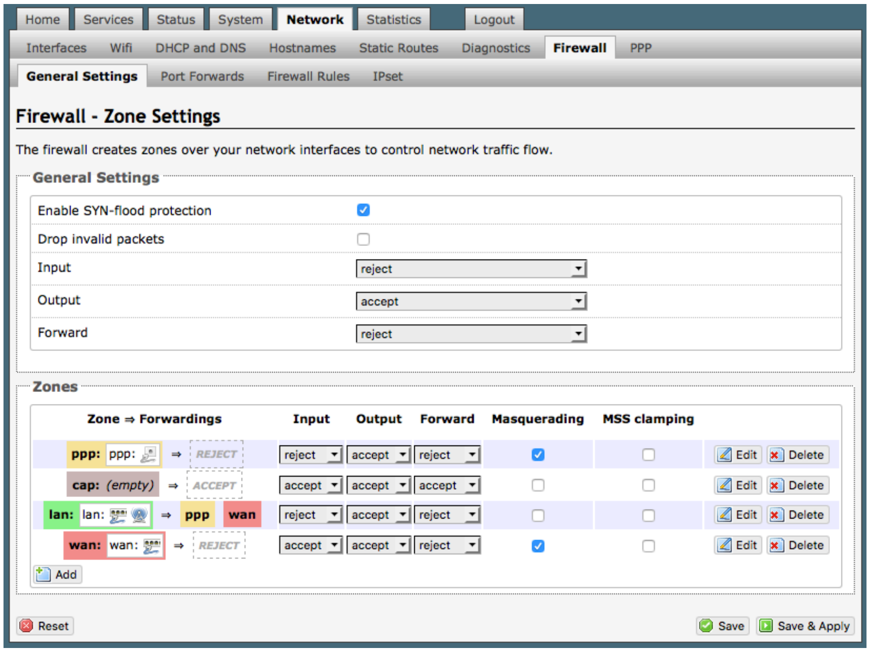
Use this screen to create and edit Firewall zones. Each Firewall Zone can have its own firewall rules. Each Interface must be assigned a Firewall Zone *(see Chapter 8.1).*

It is important to understand the following before considering modifications:

Input: this is accessing the router itself.

Output: this is the router accessing the "lan". **DO NOT MODIFY**.

Forward: this is traffic thru the router via an interface and out of the router. If Forward is allowed you must configure the Inter-Zone Forwarding. *(see Chapter 8.1.1)*



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

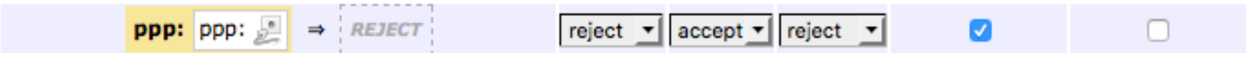
Enable SYN-flood protection	☑
Drop invalid packets	□
Input	reject
Output	accept
Forward	reject

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
ppp: ppp: ⇒ REJECT	reject	accept	reject	☑	□	Edit Delete
cap: (empty) ⇒ ACCEPT	accept	accept	accept	□	□	Edit Delete
lan: lan: ⇒ ppp wan	reject	accept	reject	□	□	Edit Delete
wan: wan: ⇒ REJECT	accept	accept	reject	☑	□	Edit Delete

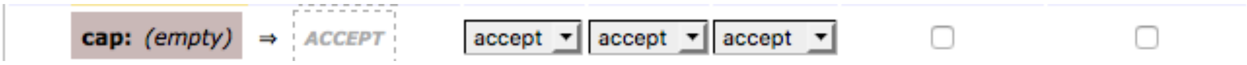
Accept: this setting allows traffic unless there is a Rule to block it.
Reject: this setting blocks traffic unless there is a Rule to allow it. An error is displayed to the end user.
Drop: this setting drops the traffic with no indication to the end user.

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



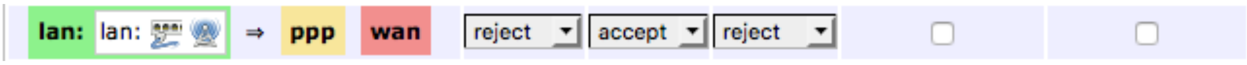
ppp: ppp: ⇒ REJECT reject accept reject ☑ □

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 is rejected.



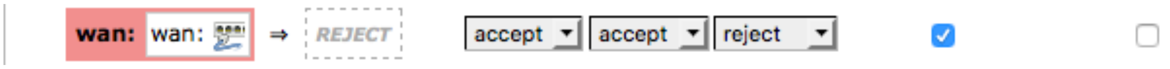
cap: (empty) ⇒ ACCEPT accept accept accept □ □

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



lan: lan: ⇒ ppp wan reject accept reject □ □

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.



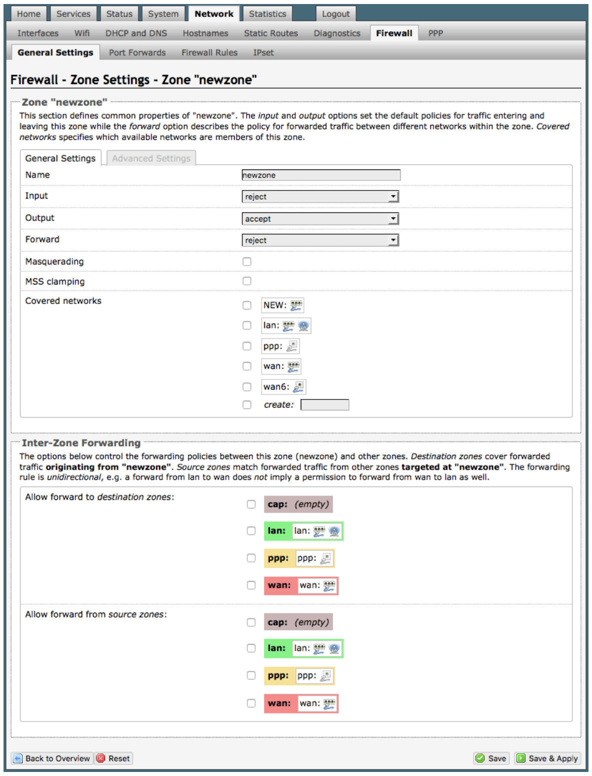
wan: wan: ⇒ REJECT accept accept reject ☑ □

The "wan" firewall zone has the wan interface assigned to it. This is the zone for satellite connections and wifi extenders. In this default configuration, only Output traffic is allowed.

8.7.1.1 Add a Firewall Zone

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

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



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.

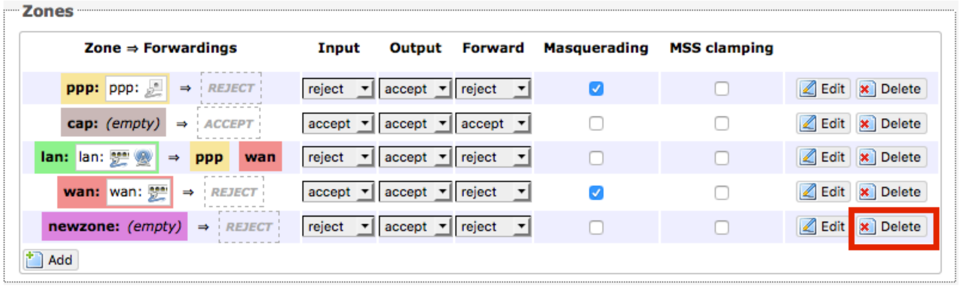
Name	newzone
Input	reject
Output	accept
Forward	reject
Masquerading	☐
MSS clamping	☐
Covered networks	☐ NEW: ☐ lan: ☐ ppp: ☐ wan: ☐ wan6: ☐ *create:*

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 *destination zones*:	☐ **cap:** *(empty)* ☐ **lan:** lan: ☐ **ppp:** ppp: ☐ **wan:** wan:
Allow forward from *source zones*:	☐ **cap:** *(empty)* ☐ **lan:** lan: ☐ **ppp:** ppp: ☐ **wan:** wan:

8.7.1.2 Delete a Firewall Zone



Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
ppp: ppp: ⇒ *REJECT*	reject	accept	reject	☑	☐	Edit Delete
cap: *(empty)* ⇒ *ACCEPT*	accept	accept	accept	☐	☐	Edit Delete
lan: lan: ⇒ **ppp** **wan**	reject	accept	reject	☐	☐	Edit Delete
wan: wan: ⇒ *REJECT*	accept	accept	reject	☑	☐	Edit Delete
newzone: *(empty)* ⇒ *REJECT*	reject	accept	reject	☐	☐	Edit Delete

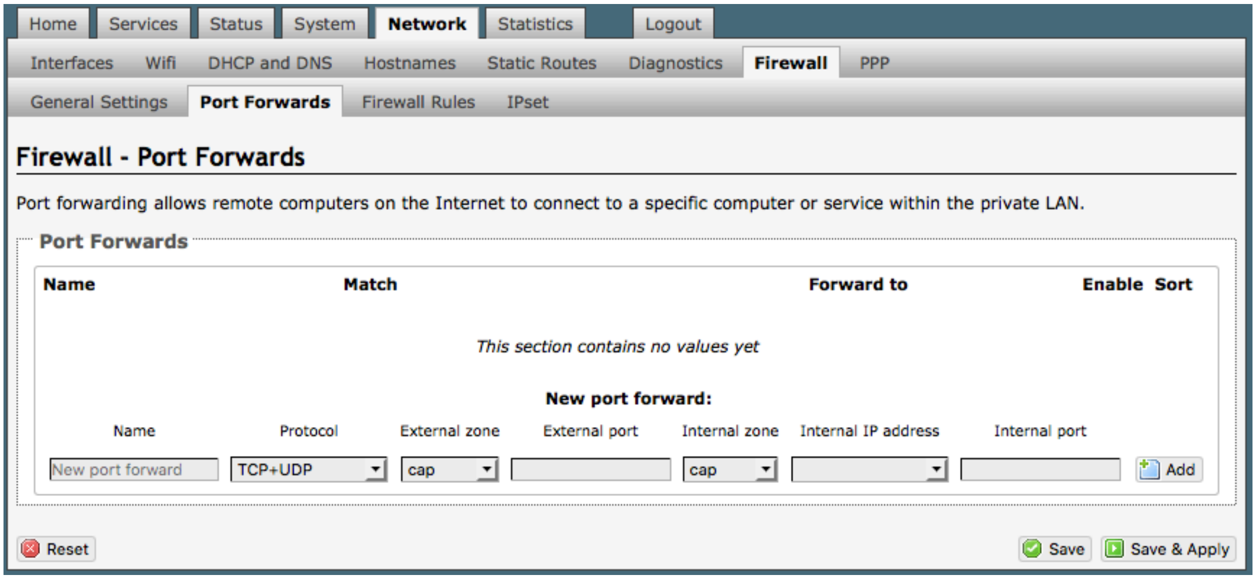
To permanently remove a firewall zone, select the Delete icon.

CAUTION: This action CANNOT be undone.

8.7.2 Port Forwards

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

CAUTION: It is important to understand networking before making changes to Port Forwards.



Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

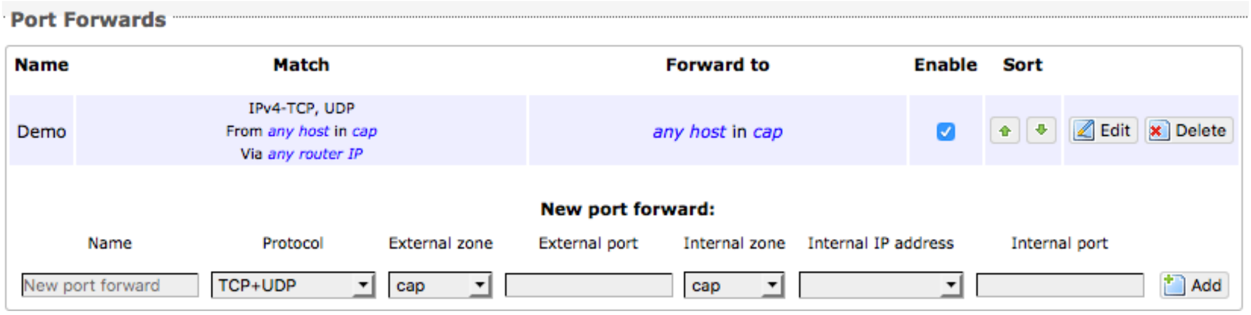
Name	Match	Forward to	Enable	Sort

This section contains no values yet

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
New port forward	TCP+UDP	cap		cap			Add

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



Port Forwards

Name	Match	Forward to	Enable	Sort	
Demo	IPv4-TCP, UDP From *any host* in *cap* Via *any router IP*	*any host* in *cap*	☑	↑ ↓	Edit Delete

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
New port forward	TCP+UDP	cap		cap			Add

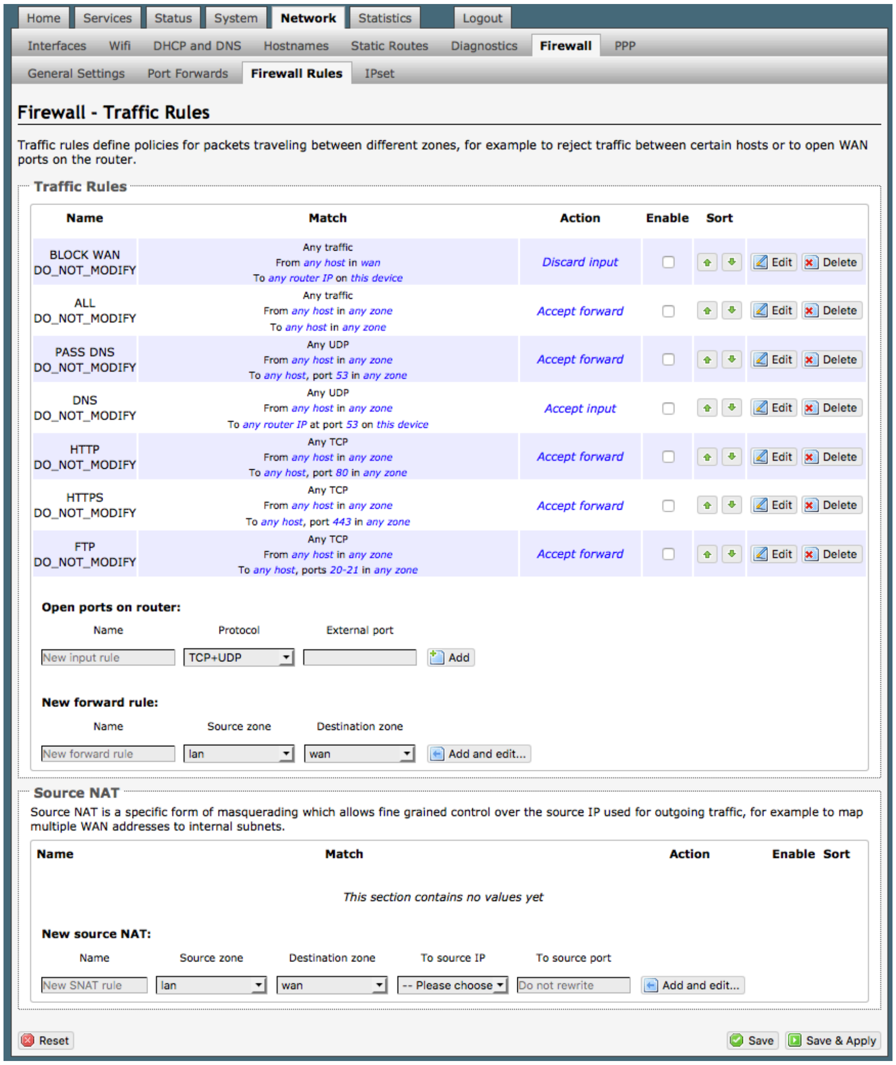
You can now enable/disable them, change the sort order, and edit the parameters.

CAUTION: The Delete function cannot be undone.

8.7.3 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 Voice 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.



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.

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*	□	⇧ ⇩	Edit Delete
ALL DO_NOT_MODIFY	Any traffic From *any host* in *any zone* To *any host* in *any zone*	*Accept forward*	□	⇧ ⇩	Edit Delete
PASS DNS DO_NOT_MODIFY	Any UDP From *any host* in *any zone* To *any host*, port *53* in *any zone*	*Accept forward*	□	⇧ ⇩	Edit Delete
DNS DO_NOT_MODIFY	Any UDP From *any host* in *any zone* To *any router IP* at port *53* on *this device*	*Accept input*	□	⇧ ⇩	Edit Delete
HTTP DO_NOT_MODIFY	Any TCP From *any host* in *any zone* To *any host*, port *80* in *any zone*	*Accept forward*	□	⇧ ⇩	Edit Delete
HTTPS DO_NOT_MODIFY	Any TCP From *any host* in *any zone* To *any host*, port *443* in *any zone*	*Accept forward*	□	⇧ ⇩	Edit Delete
FTP DO_NOT_MODIFY	Any TCP From *any host* in *any zone* To *any host*, ports *20-21* in *any zone*	*Accept forward*	□	⇧ ⇩	Edit Delete

Open ports on router:

Name	Protocol	External port	
New input rule	TCP+UDP		Add

New forward rule:

Name	Source zone	Destination zone	
New forward rule	lan	wan	Add and edit...

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 --	Do not rewrite	Add and edit...

Reset   Save   Save & Apply

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. *See Chapter 4.3 for details.*

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 hit <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.

Copyright © Global Marine Networks, LLC

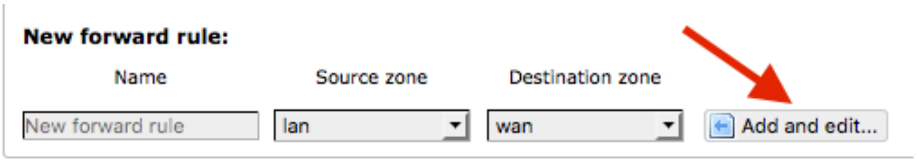
- Disable (uncheck) the rule "HTTP-DO NOT MODIFY". This blocks http traffic from passing through the firewall.

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.

8.7.3.1 Create a Custom Rule

Scroll down to the bottom of the page to the section "New forward rule". Select <Add and edit>.



New forward rule:

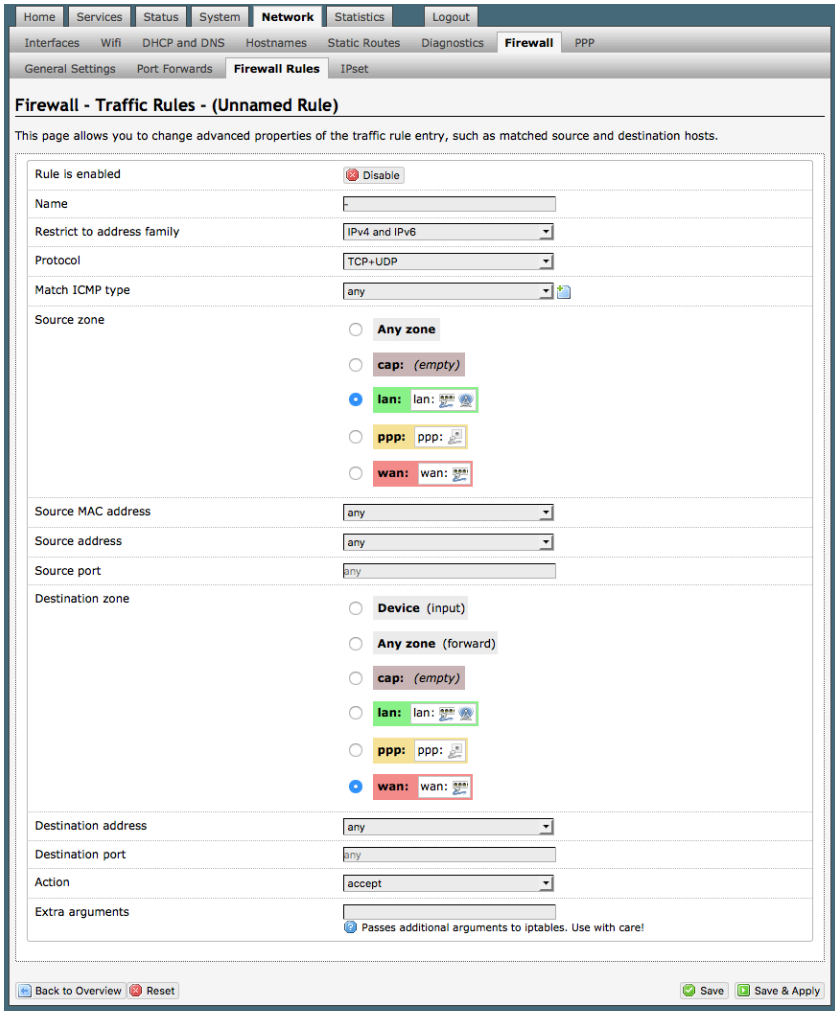
Name	Source zone	Destination zone	
New forward rule	lan	wan	Add and edit...

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, select <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 *(Chapter 8.6.4)* for creating block and allow rules by domain name instead of ip address.



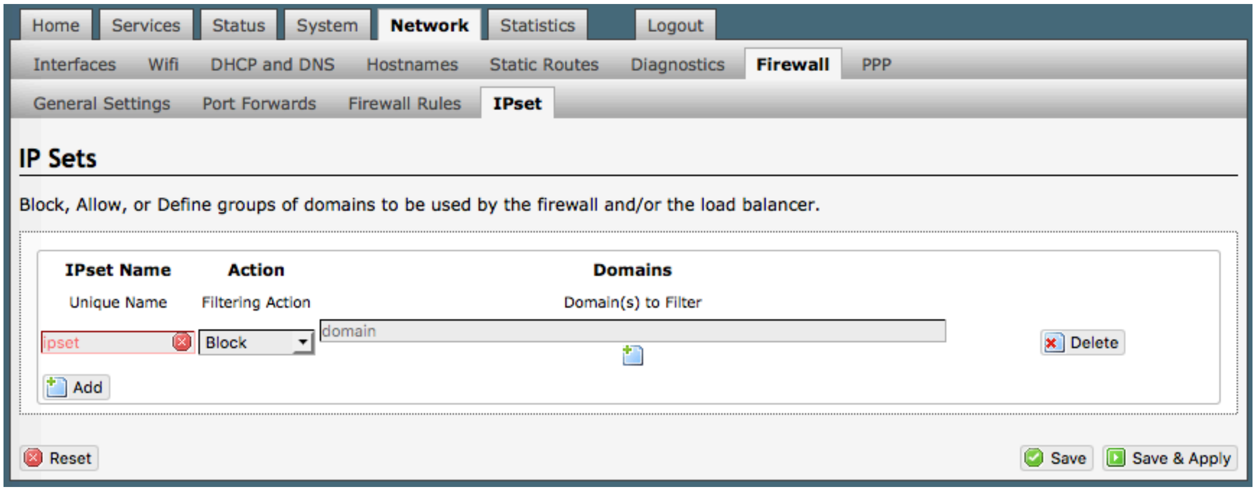
Firewall - Traffic Rules - (Unnamed Rule)

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

Rule is enabled	Disable
Name	
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	○ Any zone ○ cap: *(empty)* ● lan: lan: ○ ppp: ppp: ○ wan: wan:
Source MAC address	any
Source address	any
Source port	any
Destination zone	○ Device (input) ○ Any zone (forward) ○ cap: *(empty)* ○ lan: lan: ○ ppp: ppp: ● wan: wan:
Destination address	any
Destination port	any
Action	accept
Extra arguments	Passes additional arguments to iptables. Use with care!

8.7.4 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.



IP Sets

Block, Allow, or Define groups of domains to be used by the firewall and/or the load balancer.

IPset Name	Action	Domains
Unique Name	Filtering Action	Domain(s) to Filter
ipset	Block	domain

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

Action Definitions:

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

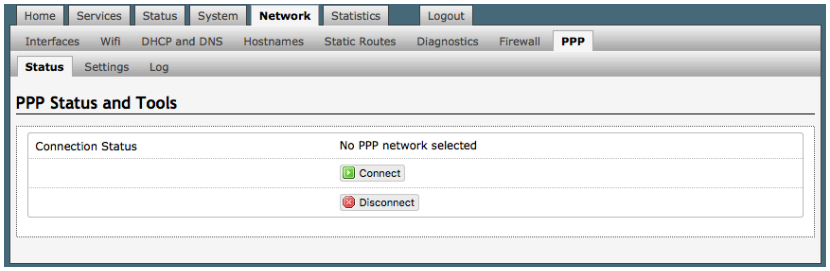
You can group multiple domain names into one IP set rule.

8.8 PPP

Requires "superadmin" login.

It is possible to use a USB connected satellite phone or GSM modem that does PPP to connect for email and web browsing (for example: IsatPhone Pro or Iridium handheld). (Please note: web browsing is not recommended when using a low bandwidth device.)

With PPP configured, you can bring up the connection manually; it will stay connected until you disconnect or the idle timeout is reached. If not using the Demand feature, you must bring up the PPP connection manually. *See Chapters 8.8.1 and 8.8.2.*

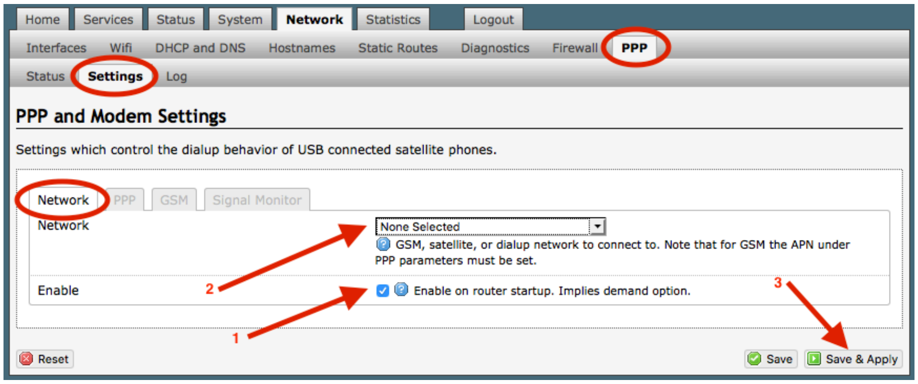


PPP Status and Tools

Connection Status	No PPP network selected

8.8.1 PPP Settings Configuration for USB Connected Satellite Device

Use the following to configure the PPP interface for use with a USB connected satellite phone.



PPP and Modem Settings

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

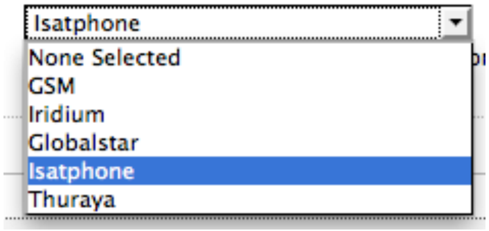
Network: None Selected — GSM, satellite, or dialup network to connect to. Note that for GSM the APN under PPP parameters must be set.

Enable: ☑ Enable on router startup. Implies demand option.

1. Select the Enable checkbox to maintain this setting during the router startup. Otherwise, you must re-configure for PPP use each time you start the router.

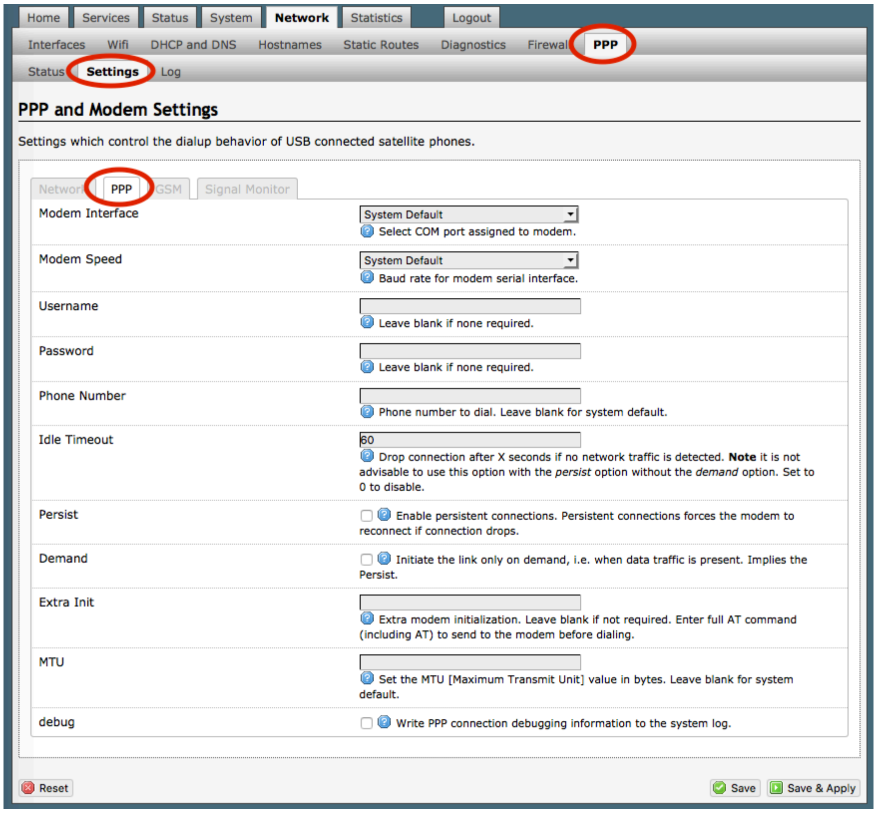
2. Using the drop-down menu, select the appropriate satellite network.

3. Select <Save & Apply> to apply the change.



Copyright © Global Marine Networks, LLC

Move to the Settings > PPP Tab:



PPP and Modem Settings

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

Modem Interface	System Default Select COM port assigned to modem.
Modem Speed	System Default Baud rate for modem serial interface.
Username	Leave blank if none required.
Password	Leave blank if none required.
Phone Number	Phone number to dial. Leave blank for system default.
Idle Timeout	60 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	□ Enable persistent connections. Persistent connections forces the modem to reconnect if connection drops.
Demand	□ Initiate the link only on demand, i.e. when data traffic is present. Implies the Persist.
Extra Init	Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before dialing.
MTU	Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.
debug	□ Write PPP connection debugging information to the system log.

Configure the PPP Settings as necessary. These PPP Settings apply to both USB connected satellite phones and GSM (cellular) modems.

Modem Interface: Do not modify from "System Default" unless you have trouble connecting. If required, use the drop-down list, select the COM port assigned to the USB connected satphone.

Modem Speed: Do not modify from "System Default" unless you have trouble connecting. If required, use the drop-down list, select the baud rate for the USB connected satphone.

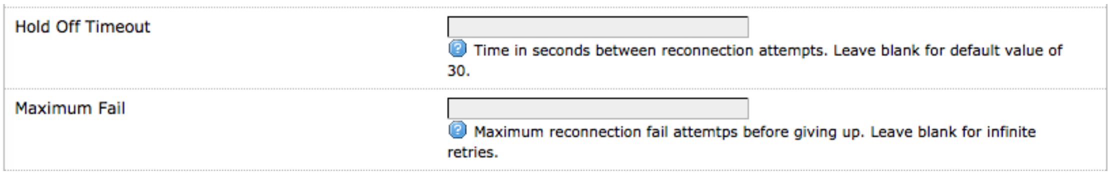
Username: If the satellite network provider requires a username in order to connect to their network, enter it here. (If you use the APN Wizard, this will be completed automatically.)

Password: If the satellite network provider requires a password in order to connect to their network, enter it here. (If you use the APN Wizard, this will be completed automatically.

Phone number: The Optimizer is pre-configured with the standard number to dial for the different satellite networks. Unless your satellite airtime provider requires an alternate phone number, this field can be left blank in order to use the default dialup number.

Idle Timeout: The default is set to 60 seconds. If no network traffic is detected during this Idle Timeout period, the connection will drop. To disable the Idle Timeout feature, set to 0. *Note: If Persist is enabled with Demand disabled, the Idle Timeout is ignored.*

Persist: Check this box to enable persistent connections. If the connection drops the modem will attempt to reconnect. With Persist selected, two additional settings appear:



Hold Off Timeout	Time in seconds between reconnection attempts. Leave blank for default value of 30.
Maximum Fail	Maximum reconnection fail attemtps before giving up. Leave blank for infinite retries.

Copyright © Global Marine Networks, LLC

Hold Off Timeout: The default is 30 seconds. If the link is dropped, this is the time it will wait to try connection again.

Maximum Fail: The default is never. This is the number of times it will try to re-connect. If re-connection does not happen within this number, it will stop trying.

Demand: Check this box to bring up the link only on demand, such as when data traffic is present. The satphone or GSM modem that does PPP, the link remains down until it detects network traffic. It will bring up the link automatically and stay up when there is traffic or until the Idle Timeout setting reached. With Demand selected, Persist is implied. See Persist above.

Extra Init: If required, enter the full AT command to send to the modem before dialing.

MTU (Maximum Transmit Unit): This should be blank to use the system default; or, you can set the limit here, in bytes. Only change this setting if required to do so by your satellite provider.

debug: If you are having trouble with the PPP connection this debug log may help you diagnose the problem.

Select <Save & Apply>.

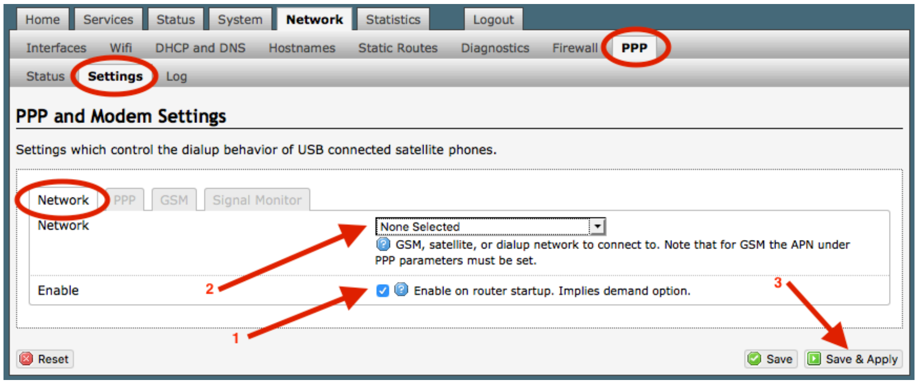
8.8.2 PPP Settings Configuration for GSM Modems

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 connection. If you run into any difficulties you must contact your cellular network provider for support.

If you have a GSM-based or LTE-based cellular phone, it may be possible to use the GSM network, when available, for Email and Web Browsing 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 and LTE-based service can be configured here. CDMA-based service will NOT work. If you are unsure of which service you have, contact your cellular provider before attempting to configure for connection.

Use the following to configure the PPP interface for use with a GSM modem.



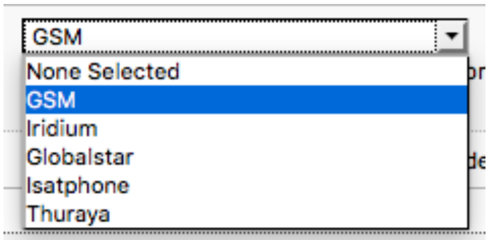
PPP and Modem Settings

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

Network: None Selected
GSM, satellite, or dialup network to connect to. Note that for GSM the APN under PPP parameters must be set.

Enable: ☑ Enable on router startup. Implies demand option.

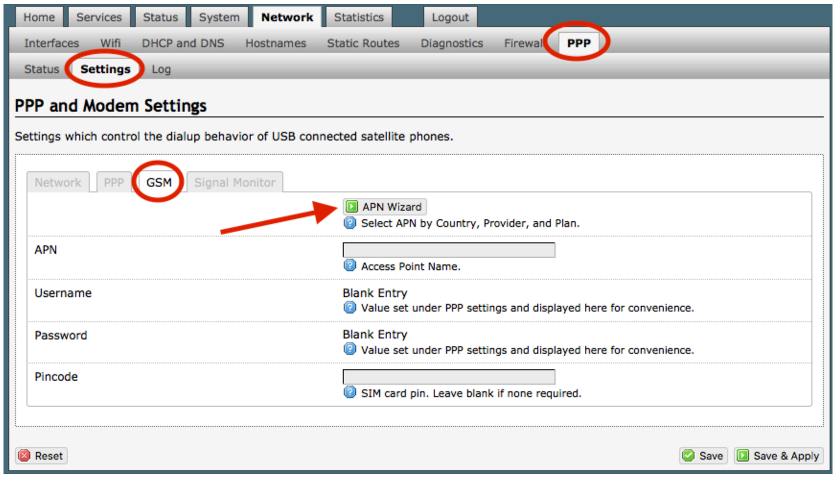
1. Select the Enable checkbox to maintain this setting during router startup. Otherwise, you must re-configure for PPP use with each router startup.



2. Using the drop-down menu, select GSM.

3. Select <Save & Apply> to apply the change.

Move to the Settings > GSM Tab:



PPP and Modem Settings

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

Select APN by Country, Provider, and Plan.

APN: Access Point Name.

Username: Blank Entry
Value set under PPP settings and displayed here for convenience.

Password: Blank Entry
Value set under PPP settings and displayed here for convenience.

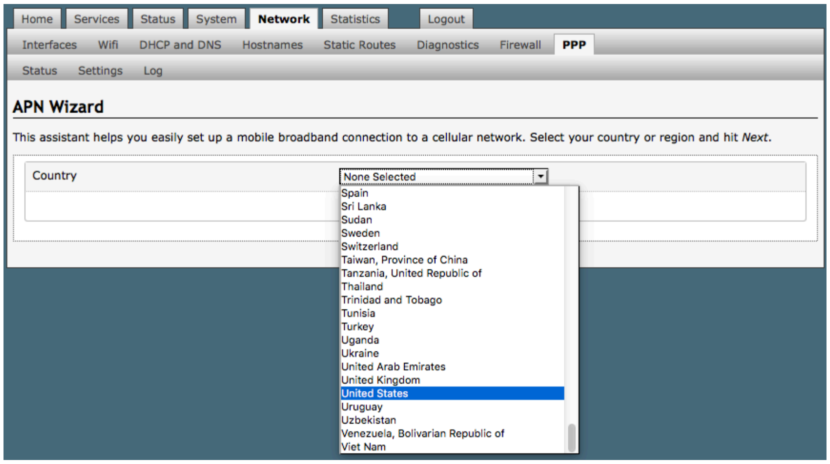
Pincode: SIM card pin. Leave blank if none required.

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.

The APN Wizard contains many providers and plans. Using it will automatically set the configuration for you. Select <APN Wizard> to start the configuration:

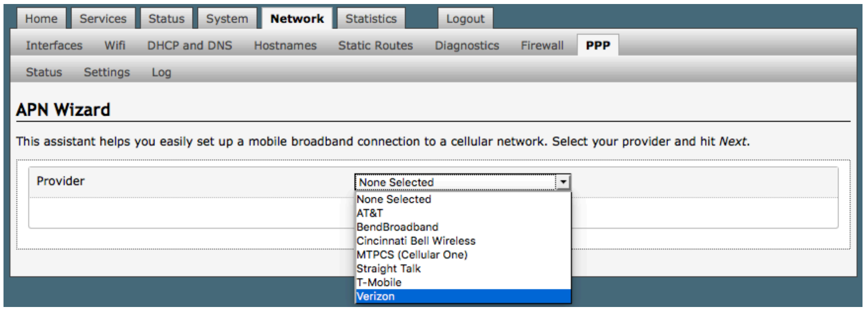
Select the appropriate country from the drop down list and then, <Next>.



APN Wizard

This assistant helps you easily set up a mobile broadband connection to a cellular network. Select your country or region and hit *Next*.

Country: None Selected



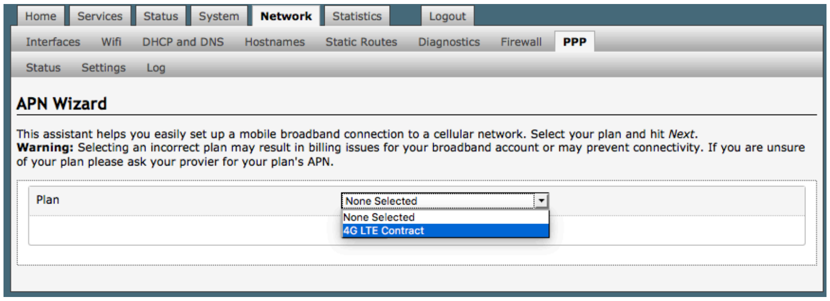
APN Wizard

This assistant helps you easily set up a mobile broadband connection to a cellular network. Select your provider and hit *Next*.

Provider: None Selected

Select your Cell Provider from the drop down list and then, <Next>.

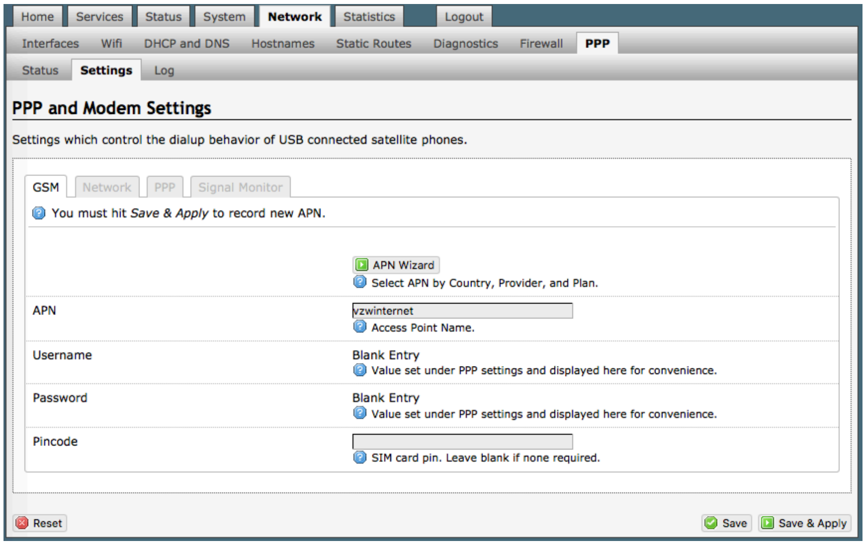
Select your Plan from the drop down list and then, <Next>.



APN Wizard

This assistant helps you easily set up a mobile broadband connection to a cellular network. Select your plan and hit *Next*.
Warning: Selecting an incorrect plan may result in billing issues for your broadband account or may prevent connectivity. If you are unsure of your plan please ask your provier for your plan's APN.

Plan: None Selected



PPP and Modem Settings

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

You must hit *Save & Apply* to record new APN.

Select APN by Country, Provider, and Plan.

APN: vzwinternet
Access Point Name.

Username: Blank Entry
Value set under PPP settings and displayed here for convenience.

Password: Blank Entry
Value set under PPP settings and displayed here for convenience.

Pincode:
SIM card pin. Leave blank if none required.

If you have protected your cellular SIM card with a PIN-Code, enter the PIN-Code in the Pincode text box.

Select <Save & Apply> to complete the configuration.

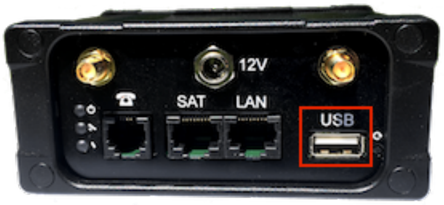
NOTE: If the APN Wizard does not contain the information for your provider or plan, contact your cellular provider to obtain the information required to connect to their GSM network. The information may include:

- Access Point Name (APN)
- Username required for access to the APN
- Password required for access to the APN

Enter the required information in the PPP Settings pages.

See Section 8.8.1 for additional PPP Settings.

8.8.2.1 Using GSM



When you want to use GSM service instead of satellite service we recommend that you disconnect the satellite terminal from the Optimizer before attempting a GSM connection.

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

8.8.2.2 Changing from GSM service to satellite service

When you travel beyond GSM range you must:

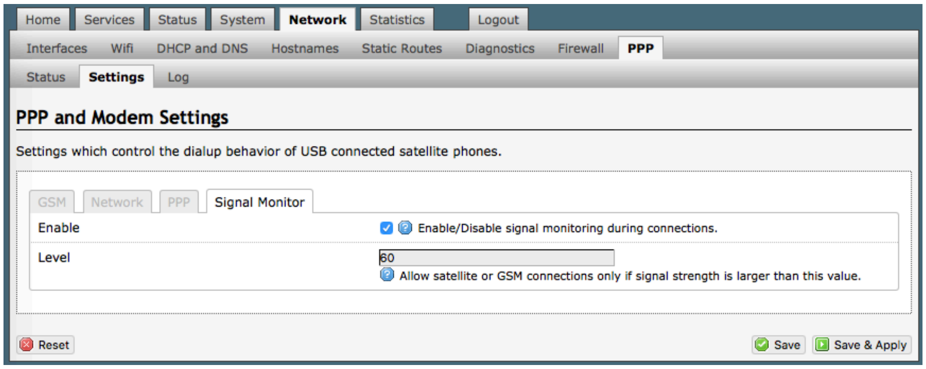
- Remove the GSM data dongle from the Optimizer's USB port.
- Reconnect your satellite phone/terminal to the Optimizer.

IMPORTANT: We are not able to support the GSM feature. If you experience any connection difficulties when using this feature, you must contact your GSM network provider for support.

8.8.3 Signal Monitor

Signal monitor queries your satellite device or GSM modem 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 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.



PPP and Modem Settings

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

Enable ☑ Enable/Disable signal monitoring during connections.

Level 60
Allow satellite or GSM connections only if signal strength is larger than this value.

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

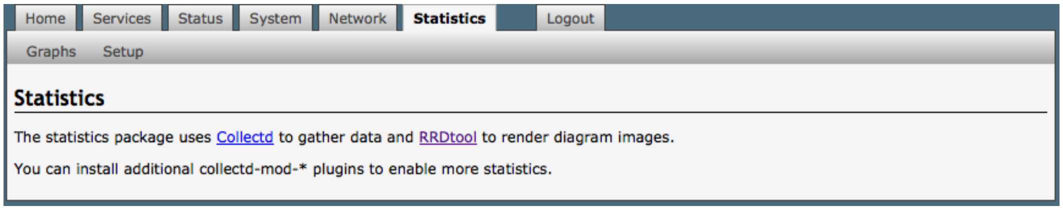
You can change the level of the Signal Monitor. Keep in mind that 60% is typically the minimum required for a successful data connection. If you must change the Signal Monitor, we recommend lowering the Level vs. disabling it. Many IsatPhonePro users have had success by lowering the level to 40 or 30.

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>.

9.0 Statistics

Requires "superadmin" login



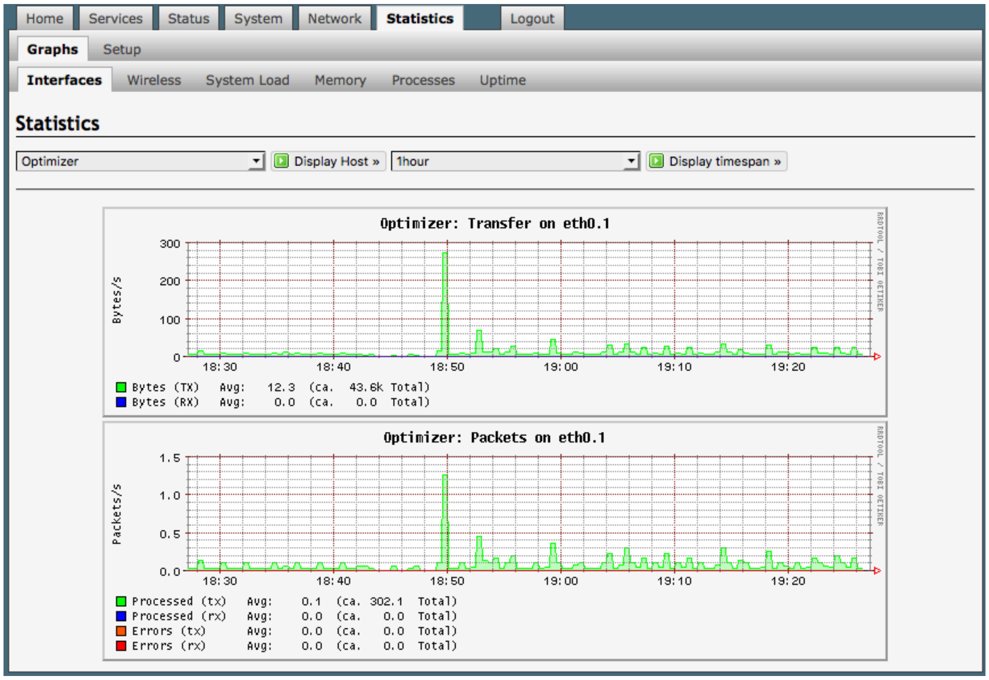
Statistics

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.

9.1 Graphs

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



Statistics

Optimizer | 1hour

```
🟩 Bytes (TX)   Avg:   12.3  (ca.  43.6k Total)
🟦 Bytes (RX)   Avg:    0.0  (ca.    0.0 Total)
```

```
🟩 Processed (tx)   Avg:   0.1  (ca. 302.1  Total)
🟦 Processed (rx)   Avg:   0.0  (ca.   0.0  Total)
🟧 Errors (tx)      Avg:   0.0  (ca.   0.0  Total)
🟥 Errors (rx)      Avg:   0.0  (ca.   0.0  Total)
```

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

Copyright © Global Marine Networks, LLC

APPENDIX A

Setup and Use with Inmarsat IsatHub (iSavi)

Information and easy-to-follow instructions on hos to setup the Optimizer Voiceand iSavi IsatHub terminal to connect to the Internet, send and receive email, send and receive SMS messages and phone calls, and enable VoIP service.

Table of Contents

Copyright © Global Marine Networks, LLC

A.1.0 Overview

Out-of-the-box, the iSavi allows you some basic control over data usage by configuring firewall rules (up to 10) and by setting caps on data consumption. However, it does not allow you to configure what programs or software can have access to the Internet and it does not compress any data.

The Optimizer Voice paired with the iSavi allows you greater flexibility to control your satellite airtime. Its built-in firewall blocks all Internet activity except XGate

A.2.0 Setup Requirements

The following hardware and software is required:

- Inmarsat iSavi satellite terminal
- RedPort Optimizer Voice
- Optimizer Voice WiFi Bridge plugged into the USB port of the Optimizer Voice (this may have already been done by your dealer).
- IsatHub Control App for your iOS or Android device
- XGate Phone App for your iOS or Android device (Required to use RedPort VoIP service. Without the XGate phone app, you can only connect to the iSavi for standard Inmarsat voice calling).
- XGate and XWeb apps (optional)

For iSavi operational information please refer to the iSavi User Guide.

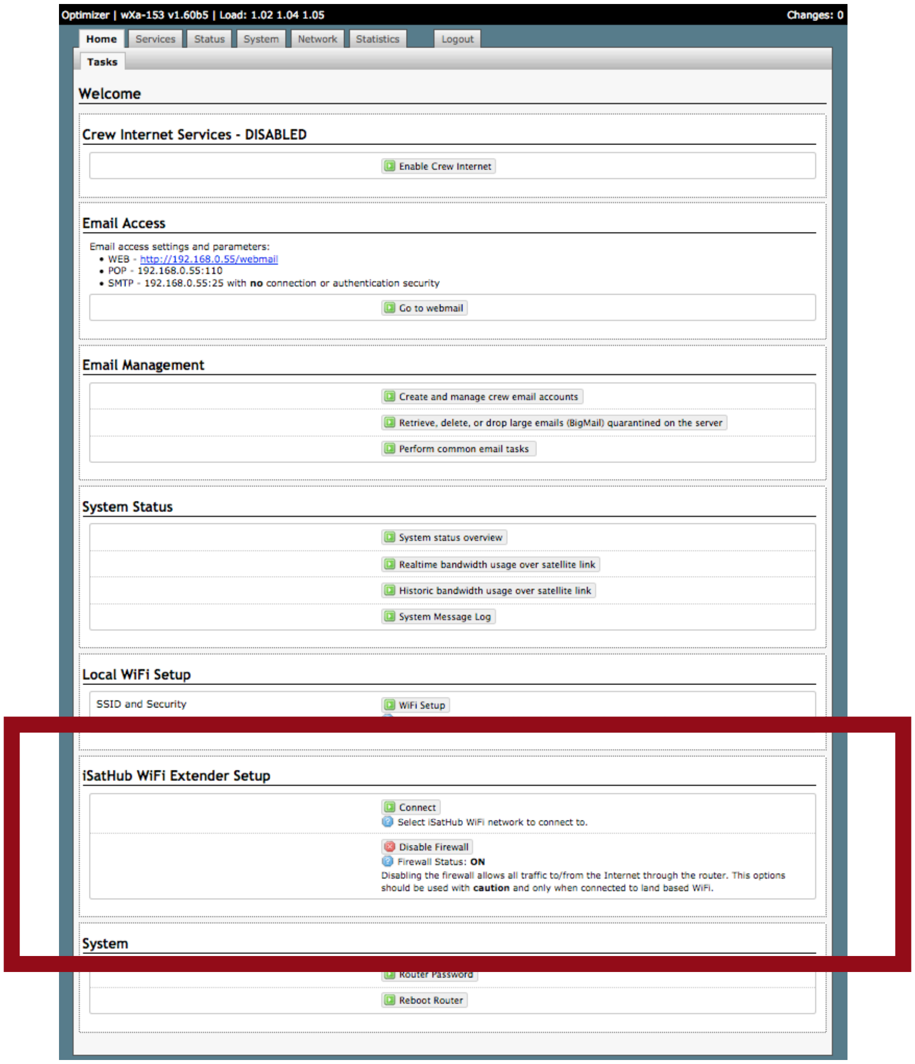
NOTE: The Optimizer Voice ships pre-configured for use with XGate and RedPort Email service and XWeb Web Browsing service. These services are not included with your Optimizer Voice and must be purchased separately. Contact your satellite service provider for details.

A.3.0 Configure Optimizer Voice to Pair with iSavi

You must first access the Home Page of the Optimizer Voice. *See Chapter 4.1 for details.*

Scroll down to the iSatHub WiFi Extender Setup section.

Select <Connect> to access the Wireless Overview tab.



Optimizer | wXa-153 v1.60b5 | Load: 1.02 1.04 1.05 Changes: 0

Home
Services
Status
System
Network
Statistics
Logout
Tasks

Welcome

Crew Internet Services - DISABLED

Email Access

Email access settings and parameters:

- WEB - http://192.168.0.55/webmail
- POP - 192.168.0.55:110
- SMTP - 192.168.0.55:25 with **no** connection or authentication security

Email Management

Create and manage crew email accounts
Retrieve, delete, or drop large emails (BigMail) quarantined on the server
Perform common email tasks

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

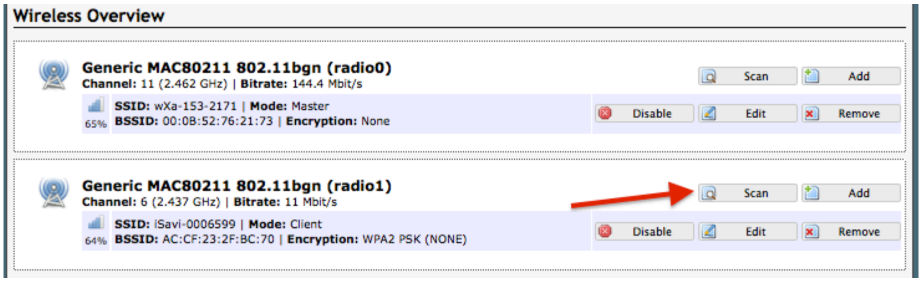
iSatHub WiFi Extender Setup

Select iSatHub WiFi network to connect to.

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



Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 144.4 Mbit/s

65% **SSID:** wXa-153-2171 | **Mode:** Master
BSSID: 00:0B:52:76:21:73 | **Encryption:** None

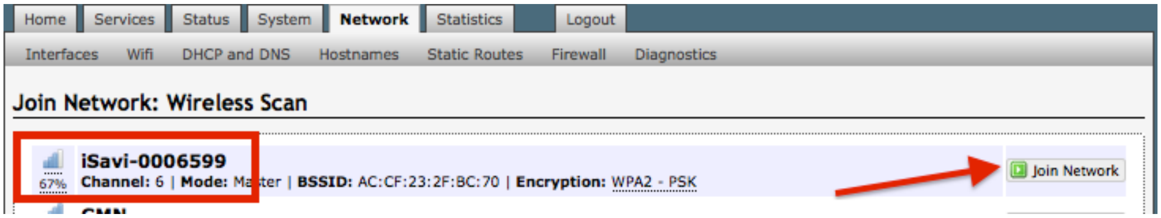
Generic MAC80211 802.11bgn (radio1)
Channel: 6 (2.437 GHz) | **Bitrate:** 11 Mbit/s

64% **SSID:** iSavi-0006599 | **Mode:** Client
BSSID: AC:CF:23:2F:BC:70 | **Encryption:** WPA2 PSK (NONE)

Select <Scan>

Copyright © Global Marine Networks, LLC

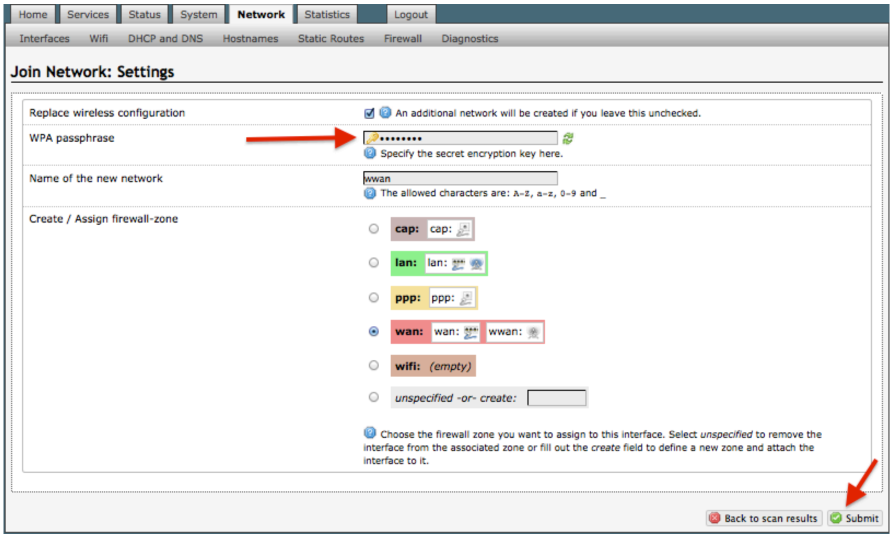
Once the scan has completed, locate the iSavi Wireless Network and select <Join Network>.



Join Network: Wireless Scan

67% **iSavi-0006599**
Channel: 6 | **Mode:** Master | **BSSID:** AC:CF:23:2F:BC:70 | **Encryption:** WPA2 - PSK

Enter the password to access the iSavi (the default password appears on the iSavi unit). Select <Submit>.



Join Network: Settings

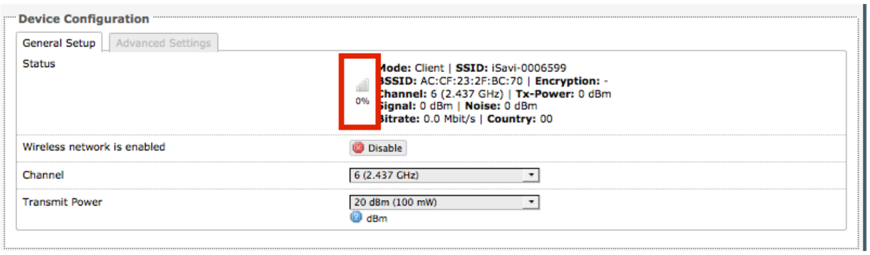
Replace wireless configuration ☑ An additional network will be created if you leave this unchecked.

WPA passphrase ••••••••
Specify the secret encryption key here.

Name of the new network: wwan
The allowed characters are: A-Z, a-z, 0-9 and _

Create / Assign firewall-zone
○ cap: cap:
○ lan: lan:
○ ppp: ppp:
● wan: wan: wwan:
○ wifi: *(empty)*
○ *unspecified -or- create:*

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.



Device Configuration

Status: 0%
Mode: Client | **SSID:** iSavi-0006599
BSSID: AC:CF:23:2F:BC:70 | **Encryption:** -
Channel: 6 (2.437 GHz) | **Tx-Power:** 0 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** 00

Wireless network is enabled

Channel: 6 (2.437 GHz)

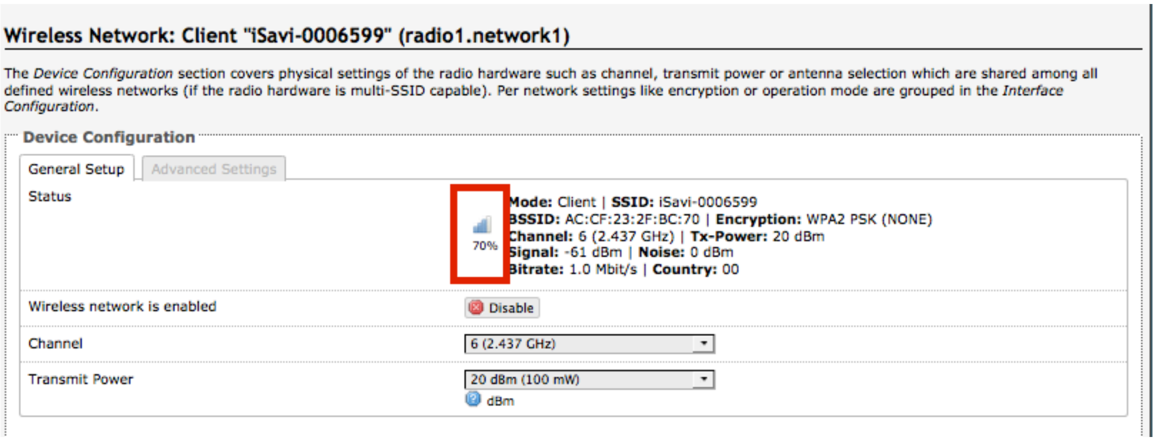
Transmit Power: 20 dBm (100 mW)
dBm

Notice the signal strength is 0% as you are not yet connected to the iSavi network. Select <Save & Apply>

NOTE: If the signal status remains 0% or is blinking from 0% to 100% this typically means that the WPA Passphrase was entered incorrectly. Return to the Join Network Settings page and enter the correct password and <Submit>.

Copyright © Global Marine Networks, LLC

Once you've successfully connected to the iSavi, you'll see that the signal strength now registers greater than 0%.



Wireless Network: Client "iSavi-0006599" (radio1.network1)

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

Status	70% **Mode:** Client | **SSID:** iSavi-0006599 **BSSID:** AC:CF:23:2F:BC:70 | **Encryption:** WPA2 PSK (NONE) **Channel:** 6 (2.437 GHz) | **Tx-Power:** 20 dBm **Signal:** -61 dBm | **Noise:** 0 dBm **Bitrate:** 1.0 Mbit/s | **Country:** 00
Wireless network is enabled	Disable
Channel	6 (2.437 GHz)
Transmit Power	20 dBm (100 mW) dBm

Now that the Optimizer Voice and the iSavi are paired, you are protected against runaway airtime. In this state, you will use:

- IsatHub Control App to establish your data connection.
- XGate Satellite Email App or RedPort Email for sending/receiving email.
- XGate XWeb or RedPort Web Compression for web browsing.
- XGate Phone App for voice calls and SMS messaging.

NOTE: The Optimizer Voice ships pre-configured for use with XGate and RedPort Email service and XWeb Web Browsing service. These services are not included with the Optimizer and must be purchased separately. Contact your satellite service provider for details.

A.4.0 Changing the VoIP Protocol on iSavi

IMPORTANT NOTE re: iSavi units with firmware version 1.0.2 or earlier

If your iSavi unit has firmware version 1.0.2 or earlier and you are planning to make voice calls over the Optimizer Voice, you must modify the voice codec in the iSavi unit.

Access the user interface of your iSavi device from any web browser using the URL: http://192.168.1.35.
Login to the unit. The default credentials are: username = admin, password = 1234.
Select the Telephony Tab > SIP Settings > Sip Server.
Select the codec: g711u

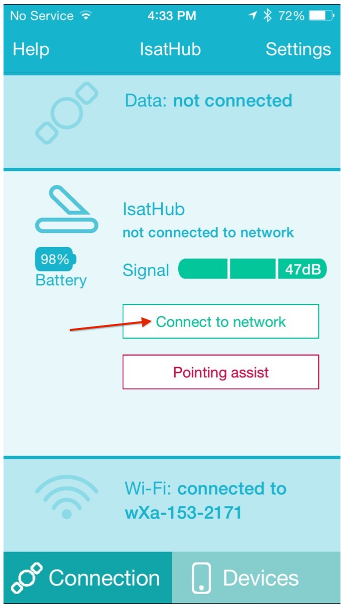
NOTE: This is required only if you plan to use the calling features. It is not applicable if you are only going to be transferring data (email and web browsing) over the iSavi; or, if your iSavi unit is running a later firmware version.

Copyright © Global Marine Networks, LLC

A.5.0 Connecting to the Network

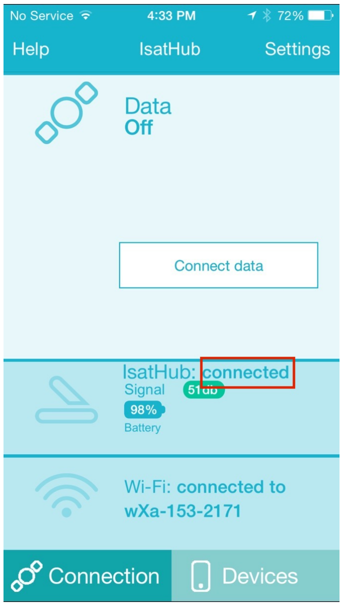
A data connection starts with connecting to the Network. Using your smartphone or tablet Settings, connect to the Optimizer Voice wireless network 'wxa-153-xxxx'.

Open the IsatHub Control App on your smartphone or tablet. (At first launch, you must enter a username and password. The default credentials are: username = admin, password = 1234

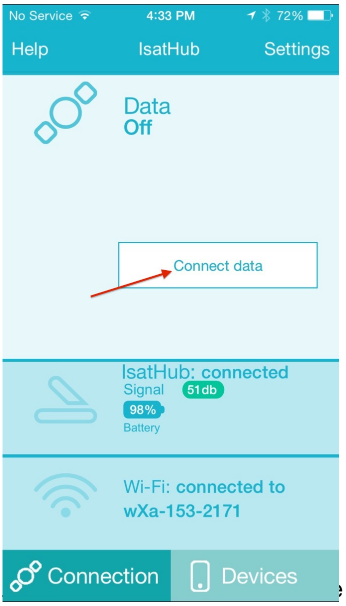


Select <Connect to network>.

Wait for display of IsatHub: connected

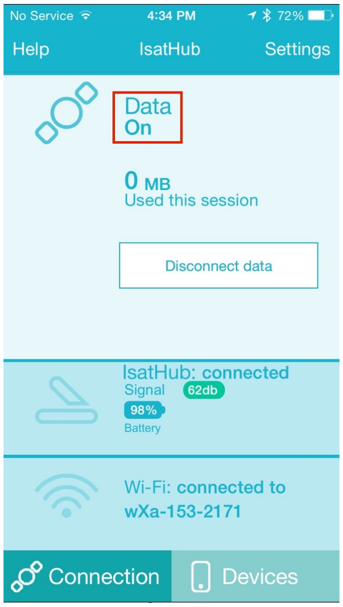


A.6.0 How to Start a Data Connection

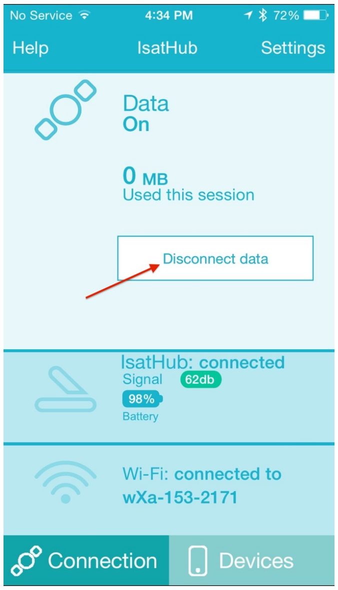


Select <Connect data>.

Wait for display of Data On.

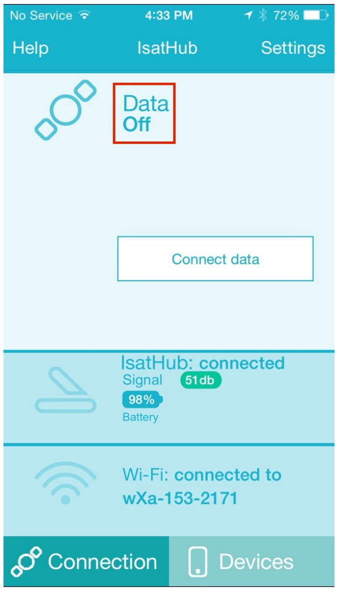


A.7.0 How to Stop a Data Connection



Select <Disconnect data>.

Wait for display of Data Off.



A.8.0 How to Send/Receive Email

Using the IsatHub Control App, connect to the network (see A.5.0 above) and start a data connection (see A.6.0 above).

Open the XGate App and send/receive email.

Close the data session when complete (see A.7.0 above).

Remember, email can be created and read offline. It is only necessary to initiate a Data Session when you are ready to connect to the mail server over your satellite link.

(Note: there is a 100kb billing increment for the iSavi – you may find it economical to leave your data connection open if you will use it again in short notice).

A.9.0 How to Web Browse

Using the IsatHub Control App, connect to the network (see A.5.0 above) and start a data connection (see A.6.0 above).

Open the XGate App and select <Web> to start a browsing session.

Close the data session when complete (see A.7.0 above).

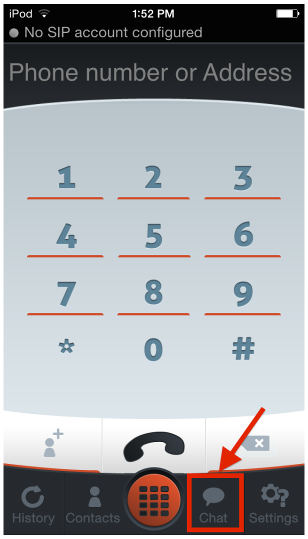
A.10.0 How to Send/Receive SMS Messages

Configure the Optimizer Voice for SMS. See Chapter 5.3 for details.

Using the IsatHub Control App, connect to the network (see A.5.0 above).

Open the XGate PHONE App. Select <Chat> to send an SMS message or to view the SMS message received.

Note: Only one SMS message can be sent at a time. Standard SMS message rates apply. (For multi-users see Multi-User Voice and SMS with RedPort VoIP service below)



A.11.0 How to Make/Receive Voice Calls

Configure the Optimizer Voice for Voice Calling. See Chapter 5.7 for details.

Using the IsatHub Control App, connect to the network (see A.5.0 above).

Open the XGate PHONE App to make and receive calls.

Note: standard voice calling rates apply

Copyright © Global Marine Networks, LLC

A.12.0 Multi-User Voice and SMS with Optional RedPort VoIP Service

Out of the box, the iSavi allows one phone call or one SMS message at a time. Phone calls via the smartphone app are standard circuit switch (PSTN) calls, not VoIP, therefore standard satellite airtime rates apply.

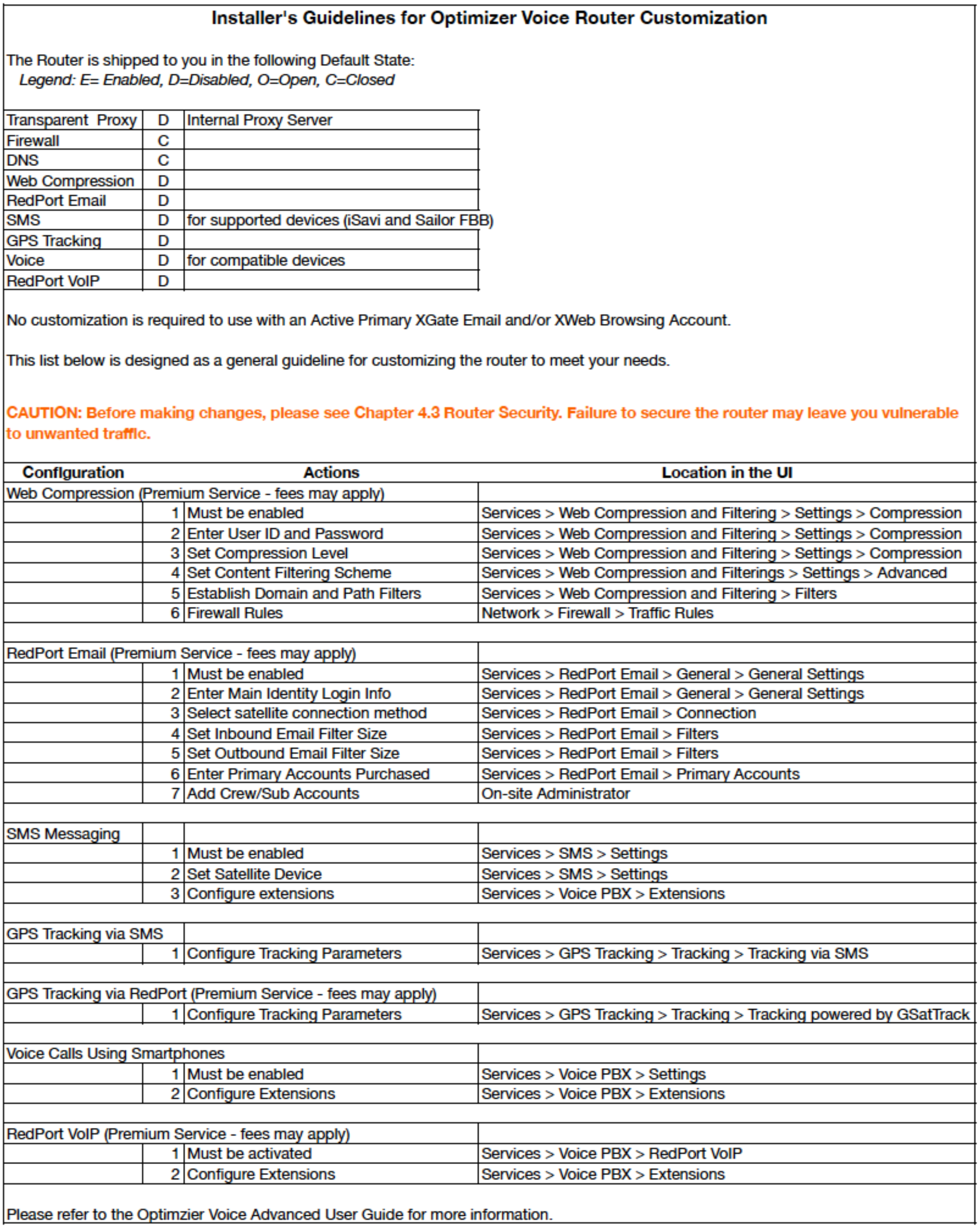
With RedPort VoIP Service, up to four people can be on calls or sending SMS messages at the same time. 15 minutes of talk time = about 1 Mbyte of data per channel (SIP extension).

Call payment methods include:

- Prepaid pincodes to help you stay on budget and/or support revenue generation. Pincodes can be given away or sold to crew/guests.
- Postpaid lines are billed monthly for actual usage.
- No charge for calls and text among local SIP extensions within on the Optimizer Voice WiFi network.

See Chapter 5.7 for activation and setup details.

APPENDIX B Installer Guidelines



Installer's Guidelines for Optimizer Voice Router Customization

The Router is shipped to you in the following Default State:
Legend: E= Enabled, D=Disabled, O=Open, C=Closed

Transparent Proxy	D	Internal Proxy Server
Firewall	C	
DNS	C	
Web Compression	D	
RedPort Email	D	
SMS	D	for supported devices (iSavi and Sailor FBB)
GPS Tracking	D	
Voice	D	for compatible devices
RedPort VoIP	D	

No customization is required to use with an Active Primary XGate Email and/or XWeb Browsing Account.

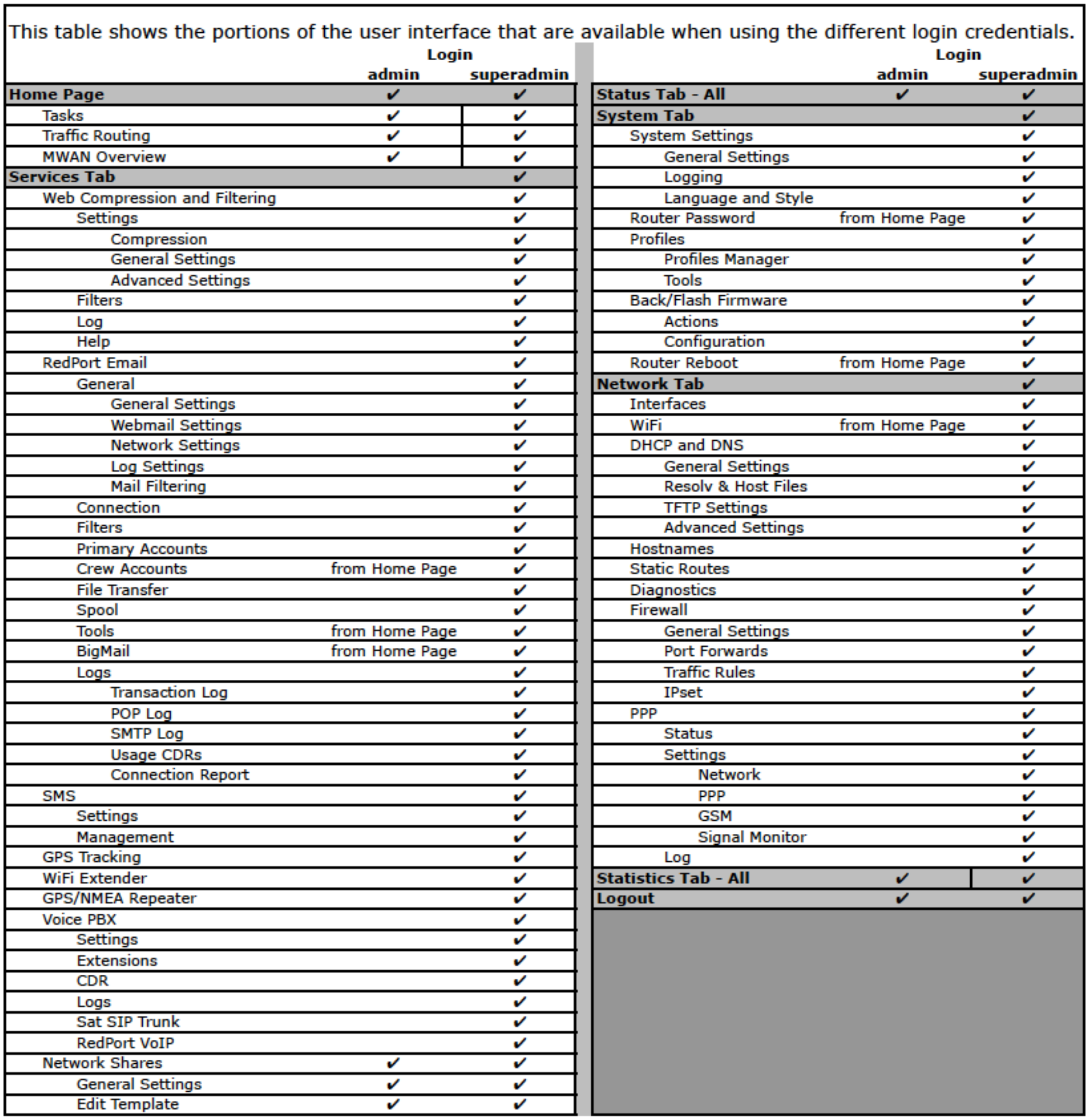
This list below is designed as a general guideline for customizing the router to meet your needs.

CAUTION: Before making changes, please see Chapter 4.3 Router Security. Failure to secure the router may leave you vulnerable to unwanted traffic.

Configuration		Actions	Location in the UI
Web Compression (Premium Service - fees may apply)			
	1	Must be enabled	Services > Web Compression and Filtering > Settings > Compression
	2	Enter User ID and Password	Services > Web Compression and Filtering > Settings > Compression
	3	Set Compression Level	Services > Web Compression and Filtering > Settings > Compression
	4	Set Content Filtering Scheme	Services > Web Compression and Filterings > Settings > Advanced
	5	Establish Domain and Path Filters	Services > Web Compression and Filtering > Filters
	6	Firewall Rules	Network > Firewall > Traffic Rules
RedPort Email (Premium Service - fees may apply)			
	1	Must be enabled	Services > RedPort Email > General > General Settings
	2	Enter Main Identity Login Info	Services > RedPort Email > General > General Settings
	3	Select satellite connection method	Services > RedPort Email > Connection
	4	Set Inbound Email Filter Size	Services > RedPort Email > Filters
	5	Set Outbound Email Filter Size	Services > RedPort Email > Filters
	6	Enter Primary Accounts Purchased	Services > RedPort Email > Primary Accounts
	7	Add Crew/Sub Accounts	On-site Administrator
SMS Messaging			
	1	Must be enabled	Services > SMS > Settings
	2	Set Satellite Device	Services > SMS > Settings
	3	Configure extensions	Services > Voice PBX > Extensions
GPS Tracking via SMS			
	1	Configure Tracking Parameters	Services > GPS Tracking > Tracking > Tracking via SMS
GPS Tracking via RedPort (Premium Service - fees may apply)			
	1	Configure Tracking Parameters	Services > GPS Tracking > Tracking > Tracking powered by GSatTrack
Voice Calls Using Smartphones			
	1	Must be enabled	Services > Voice PBX > Settings
	2	Configure Extensions	Services > Voice PBX > Extensions
RedPort VoIP (Premium Service - fees may apply)			
	1	Must be activated	Services > Voice PBX > RedPort VoIP
	2	Configure Extensions	Services > Voice PBX > Extensions

Please refer to the Optimzier Voice Advanced User Guide for more information.

APPENDIX C Login Access Table



This table shows the portions of the user interface that are available when using the different login credentials.

	Login	
	admin	superadmin
Home Page	✓	✓
Tasks	✓	✓
Traffic Routing	✓	✓
MWAN Overview	✓	✓
Services Tab		✓
Web Compression and Filtering		✓
Settings		✓
Compression		✓
General Settings		✓
Advanced Settings		✓
Filters		✓
Log		✓
Help		✓
RedPort Email		✓
General		✓
General Settings		✓
Webmail Settings		✓
Network Settings		✓
Log Settings		✓
Mail Filtering		✓
Connection		✓
Filters		✓
Primary Accounts		✓
Crew Accounts	from Home Page	✓
File Transfer		✓
Spool		✓
Tools	from Home Page	✓
BigMail	from Home Page	✓
Logs		✓
Transaction Log		✓
POP Log		✓
SMTP Log		✓
Usage CDRs		✓
Connection Report		✓
SMS		✓
Settings		✓
Management		✓
GPS Tracking		✓
WiFi Extender		✓
GPS/NMEA Repeater		✓
Voice PBX		✓
Settings		✓
Extensions		✓
CDR		✓
Logs		✓
Sat SIP Trunk		✓
RedPort VoIP		✓
Network Shares	✓	✓
General Settings	✓	✓
Edit Template	✓	✓

	Login	
	admin	superadmin
Status Tab - All	✓	✓
System Tab		✓
System Settings		✓
General Settings		✓
Logging		✓
Language and Style		✓
Router Password	from Home Page	✓
Profiles		✓
Profiles Manager		✓
Tools		✓
Back/Flash Firmware		✓
Actions		✓
Configuration		✓
Router Reboot	from Home Page	✓
Network Tab		✓
Interfaces		✓
WiFi	from Home Page	✓
DHCP and DNS		✓
General Settings		✓
Resolv & Host Files		✓
TFTP Settings		✓
Advanced Settings		✓
Hostnames		✓
Static Routes		✓
Diagnostics		✓
Firewall		✓
General Settings		✓
Port Forwards		✓
Traffic Rules		✓
IPset		✓
PPP		✓
Status		✓
Settings		✓
Network		✓
PPP		✓
GSM		✓
Signal Monitor		✓
Log		✓
Statistics Tab - All	✓	✓
Logout	✓	✓

Copyright © Global Marine Networks, LLC

If you have questions that are not answered in this guide, please email your service provider for assistance or you can contact us at: support@redportglobal.com and we will direct your inquiry to your service provider.