

RedPort™

GMN
Global Marine
NETWORKS



RedPort Optimizer Enterprise

Advanced User Guide for Installers/Network Administrators

RedPort Router: wXa-524 (Optimizer Enterprise)

Revision History

Date	Version	Point of Contact
Nov 9, 2018	Draft Version (v1.0)	Aaron Dickson

Contents

1. About this Guide	6
2. Introduction to the Optimizer Enterprise	7
2.1. Key Features	7
2.2. Services Included	7
2.3. Premium Services Available	8
3. Things to Know Before Getting Started	9
3.1. More Than Just a Router	9
3.1.1. Captive Portal	9
3.1.2. Proxy Server(s)	9
3.1.3. Firewall	9
3.2. Designed Use of the Optimizer Enterprise	9
3.3. How It Works at First Launch (Out of the Box)	9
3.4. How Data Flows Through the Router	10
3.4.1. Default Configuration	10
3.4.2. Data Flow - All Paths	14
3.5. Navigating the User Interface	14
4. Getting Started - User Interface Access	15
4.1. Access the Home page	15
4.1.1. Onsite Administrator Login (Admin)	15
4.1.2. Installer/Network Administrator Login (Superadmin)	16
4.2. How to Use with Default Setup	18
4.3. Router Security	19
4.3.1. How to Secure Your Router	19
5. Services	21
5.1. Crew Internet Services (Captive Portal)	21
5.1.1. Captive Portal Settings	21
5.1.1.1. General Settings	21
5.1.1.2. Advanced Settings	22
5.1.1.3. Allowed Hosts	23
5.1.1.4. WPAD	24
5.1.2. Allowing Individuals Access to the Internet	25
5.1.2.1. Users with Username and Password	25
5.1.2.2. Pass-Through MAC	26
5.1.2.3. PIN-Codes	27
5.1.3. CDRs (Call Data Records)	29
5.1.4. Tools	30
5.1.4.1. Admin password	31
5.1.4.2. Reset Database to Factory Defaults	31
5.1.4.3. Purge Expired PIN-Codes	31
5.1.4.4. Purge Unused PIN-Codes	31
5.1.4.5. Manage PIN-Codes	31
5.2. Web Compression and Filtering	33
5.2.1. Settings	33
5.2.1.1. Compression	34
5.2.1.2. General Settings	35
5.2.1.3. Advanced Settings	36
5.2.2. Filters (Content Filtering through Diladele)	37
5.2.3. Cache Management	38
5.2.4. Traffic Management	39
5.2.5. Access Control	40
5.2.6. Logs	40
5.2.7. Help	41
5.3. RedPort Email	41
5.3.1. Enable and Configure RedPort Email	42
5.3.2. Primary Accounts	43
5.4. Remote Access	44

5.5. SMS Messaging	46
5.5.1. SMS Settings	46
5.5.2. Configure SIP Extensions to Receive SMS Messages	46
5.5.3. How to Send/Receive SMS Messages	47
5.5.4. SMS Management	48
5.6. GPS Tracking	48
5.6.1. Tracking powered by RedPort with GSatTrack	48
5.6.2. Tracking via SMS	50
5.7. GPS/NMEA Repeater	51
5.7.1. Equipment Setup	51
5.7.1.1. USB NMEA Device	51
5.7.1.2. RS-232 NMEA Device	51
5.7.1.3. Connecting Multiple NMEA Devices	52
5.7.2. Dynamic DNS	52
5.7.3. GPS/NMEA Repeater Parameters Configuration	53
5.8. VOICE PBX	54
5.8.1. Setup Extensions	55
5.8.1.1. How to Make/Receive Voice Calls	55
5.8.2. Voicemail	56
5.8.3. CDR (Call Data Records)	57
5.8.4. Logs	58
5.8.5. Sat SIP Trunk (for Sailor FBB terminal only)	59
5.8.6. RedPort VoIP Activation	60
5.9. SNMP	62
5.10. Network Shares	62
5.10.1. Create a Shared Directory	62
5.10.2. Add Users	63
5.10.3. How to Access the Shared Directory and Path Folders:	64
5.10.3.1. From a Mac PC	64
5.10.3.2. From a Windows PC	64
6. Status	67
7. System	68
7.1. System Settings	68
7.2. Administration	68
7.3. Profiles	69
7.3.1. Add a Profile	70
7.3.2. Change to Another Saved Profile	70
7.3.3. Tools - Export a Profile	71
7.3.4. Import a Profile	72
7.4. Backup/Flash Firmware	72
7.4.1. Backup/Restore	73
7.4.2. Flash New Firmware Image	73
7.4.3. Flash SD Drive Image	74
7.5. Reboot	75
8. Virtual Private Network (VPN)	76
8.1. Point-to-Point Tunneling Protocol PPTP	76
8.2. IPsec	76
8.3. OpenConnect VPN	77
8.4. OpenVPN	78
9. Network	80
9.1. Diagnostics	80
9.2. Interfaces Overview	80
9.2.1. Interface Actions	81
9.2.2. Add a New Interface	82
9.2.3. Select Interfaces Tabs	82
9.2.3.1. General Setup	83
9.2.3.2. Advanced Settings	83

9.2.3.3. Physical Settings	84
9.2.3.4. Firewall Settings	85
9.2.3.5. DHCP Server - General Setup	86
9.2.3.6. DHCP Server Advanced	86
9.2.3.7. DHCP Server IPv6 Settings	87
9.3. WiFi	87
9.3.1. Rename the Wireless Network	88
9.3.2. Restrict Wireless Network Access	89
9.4. VLAN Switch	90
9.5. DHCP and DNS	90
9.6. Hostnames	91
9.6.1. Add Hostname	91
9.7. Static Routes	92
9.8. Firewall	92
9.8.1. General Settings	93
9.8.1.1. Add a Firewall Zone	94
9.8.1.2. Delete a Firewall Zone	95
9.8.2. Port Forwards	96
9.8.3. Firewall - Traffic Rules	97
9.8.3.1. Create a Custom Rule	97
9.8.4. IP Sets	99
9.8.5. IP Proxy	99
9.9. Packet Capture	99
9.10. PPP	100
9.10.1. PPP Settings Configuration for USB Connected Satellite Device	100
9.10.2. PPP Settings Configuration for LTE/GSM Modems	103
9.10.2.1. Using LTE/GSM	106
9.10.2.2. Changing from LTE/GSM service to satellite service	106
9.10.2.3. LTE/GSM capable OE	107
9.10.3. Signal Monitor	112
9.11. SQM QoS	112
9.12. DSCP QoS	113
9.13. Failover/Load Balancing	113
9.13.1. MWAN Overview	114
9.13.2. MWAN Configuration	116
9.13.2.1. Interfaces	117
9.13.2.2. Members	119
9.13.2.3. Creating New Member	120
9.13.2.4. Policies	121
9.13.2.5. Rules	123
9.13.3. Advanced	126
9.13.4. Failover Mode - Automatic or Manual	126
9.13.5. Failover/Load Balancing Scenarios	127
9.13.5.1. Scenario 1	127
9.13.5.2. Scenario 2	127
9.13.5.3. Block Skype or other P2P applications	128
10. Users	129
11. Statistics	132
11.1. Graphs	132
11.2. Setup	132
11.3. Bandwidth	133
12. Remote Support	135
13. Appendix A	137
14. Appendix B	139
15. Corporate Contact Information	140



1. About this Guide

This guide is intended for installers and network administrators of the RedPort Optimizer Enterprise wXa-524 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: generate PIN-Codes, create users, and look at call data records for the Captive Portal, create and manage crew email accounts, etc. See the Optimizer Enterprise Onsite Administrator Guide for details.

For information regarding the installation of the hardware, please see the RedPort Optimizer Enterprise Quickstart Guide.

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

2. Introduction to the Optimizer Enterprise

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

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

Optimizer Enterprise is a VoIP gateway and data router that provides an all-in-one solution for those looking to get the most out of all available data connections including long-range cellular and satellite broadband services.

2.1. Key Features

- Configurable to automatically select among available data connections to choose the lower-cost or preferred available service. Full-featured load balancing and least-cost routing.
- VoIP to circuit-switch conversion allows calls using a smartphone over the satellite connection. Some SatCom systems may require additional hardware.
- Compatible with RedPort VoIP service for voice call savings and controlled use.
- Flexible Routing to manage even the most complex network.
- Proxy Server enables HTTP filtering: whitelist/blacklist of URLs, domains, and rudimentary content filtering.
- Powerful firewall accommodates virtually any installation scenario, with advanced features including block or allow any range of port, IP address and protocols; port forwarding, network address translation and detailed whitelisting and blacklisting of websites and services.
- LTE/GSM Compatibility with optional LTE/GSM modem (and your own SIM card) and optional LTE/GSM external antenna and/or amplification.
- Remote Router Access available to manage the network from any Internet connection
- Supports Shared Web Compression with transparent proxy service.
- Captive Portal included for locally controlled access by crew and passenger.
- Supports RedPort XGate Email Service via included full POP/SMTP RedPort Mail Server for easy local email access.
- Supports GPS Tracking.
- Multi-Interface Failover and Load Balancing support.
- GPS NMEA Repeater reads the built-in GPS in any satellite broadband terminal and rebroadcasts via WiFi for access by an NMEA compliant device.
- Broadcasts data connection for use with WiFi enabled devices.
- Compatible with virtually any IP-based satellite broadband terminal.

2.2. Services Included

The following services are included:

- **Captive Portal for Crew Internet Access** – generate PIN codes that can be given away or sold to crew and/or passengers to control web access. **See Chapter 5.1.**
- **GPS NMEA Repeater** – allows other devices on-board/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 5.7.**
- **SMS Messaging** - allows smartphones to send SMS messages to others on the local area network for free, or over the satellite link at standard satellite airtime rates. Requires a supported satellite terminal. **See Chapter 5.5.**
- **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 5.8.**
- **GPS SMS Tracking** via satellite provider's SMS service with compatible satellite device. **See Chapter 5.6.**
- **Transparent Proxy** to redirect HTTP traffic for filtering. **See Chapter 5.2.**

- **LTE/GSM Support** with optional LTE/GSM modem and your own LTE/GSM SIM card. **See Chapter 9.10.**
- **Automatic Failover** as LTE/GSM > Sat1 > Sat2. Easily configurable to meet your needs. **See Chapter 9.13.**

2.3. Premium Services Available

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

- **RedPort VoIP Service** - Transform your satellite device into a multi-user unit. Up to four users can send and 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 5.8.**
- **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 Chapter 5.3** and the Optimizer RedPort Email Administrator's 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 5.2.**
- **GPS Tracking** - Using a GPS-enabled device, submit position reports to a RedPort Tracking central database for viewing on the tracking website. **See Chapter 5.6.**
- **Shared Captive Portal Pincode Service** - Upgrade the Captive Portal to our upstream pincode server for shared pincode service for your crew/team. These pincodes can be used at any of your installations with the Optimizer Enterprise router and Shared Pincode Service enabled. **See Chapter 5.1.**
- **Integrated LTE/GSM Capability** - **See Chapter 9.10.**
- **Internal Transparent Proxy for Web Filtering** (Including optional pay service for QL dialadele.com) - **See Chapter 5.2.**

3. Things to Know Before Getting Started

3.1. More Than Just a Router

The Optimizer Enterprise is more than just a router. It has some enhanced proxy services in addition to basic routing capabilities. There are three major data components:

3.1.1. Captive Portal

When enabled, it blocks access to the Internet without authentication. Authentication can be via username and password or Pin-Code or Mac address of a specific PC. The Captive Portal is enabled by default.

3.1.2. 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.

3.1.3. 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. In a multi-wan environment, each interface can have separate rules applied.

CAUTION: This router is shipped to you with all WAN ports open, POP and SMTP are open to the WAN if you enable Email, if you enable the 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**.

3.2. Designed Use of the Optimizer Enterprise

This router is designed for use in a multi-comm device environment for one or more users with the convenience of BYOD (bring your own device) for crew and passenger access to Email, Web Browsing and Voice. 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.

CAUTION: Prior to installation, review **Chapter 4.3.1 How to Secure Your Router**.

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: generate PIN-Codes, create users, look at call data records for the Captive Portal, create and manage crew email accounts, etc.

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 Enterprise Onsite Administrator Guide.

3.3. How It Works at First Launch (Out of the Box)

We ship the router ready for use with Captive Portal enabled for Crew Internet Access, Voice and SMS are enabled for use with compatible satellite devices, and Automatic Failover is configured in the order of LTE/GSM > WAN1 (Sat1) > WAN2(Sat2) to take advantage of the typically lower cost connections of LTE/GSM, if/when it is available.

NOTE: Prior to making modifications to the router configuration, please see [Section 3.4 How Data Flows Through the Router](#) to determine the customization required to best meet your needs.

BEST PRACTICE: Have a knowledgeable technician (someone who knows about proxy servers, firewalls, and routers) go through and generate a custom configuration.

Using the guidelines in Appendix A, the installer will want to address the following areas prior to first use:

- Configure the Captive Portal for Crew Internet Access.
- Configure the internal proxy server (Transparent Proxy).
- Configure LTE/GSM (requires configuration of PPP interface).
- Configure automatic failover/load balancing.
- Configure SMS.
- Configure Voice PBX.

OPTIONAL:

- Enable the upstream proxy for the benefit and cost savings of Shared Web Compression Service.
- Enable RedPort VoIP Service for savings on voice calls.
- Configure GPS interface.

In a fleet environment, the custom configuration can be recorded and used on other Optimizer Enterprise routers within the organization.

CAUTION: This router is shipped with all WAN ports open, POP and SMTP are open to the WAN if you enable Email, if you enable the 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**.

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.

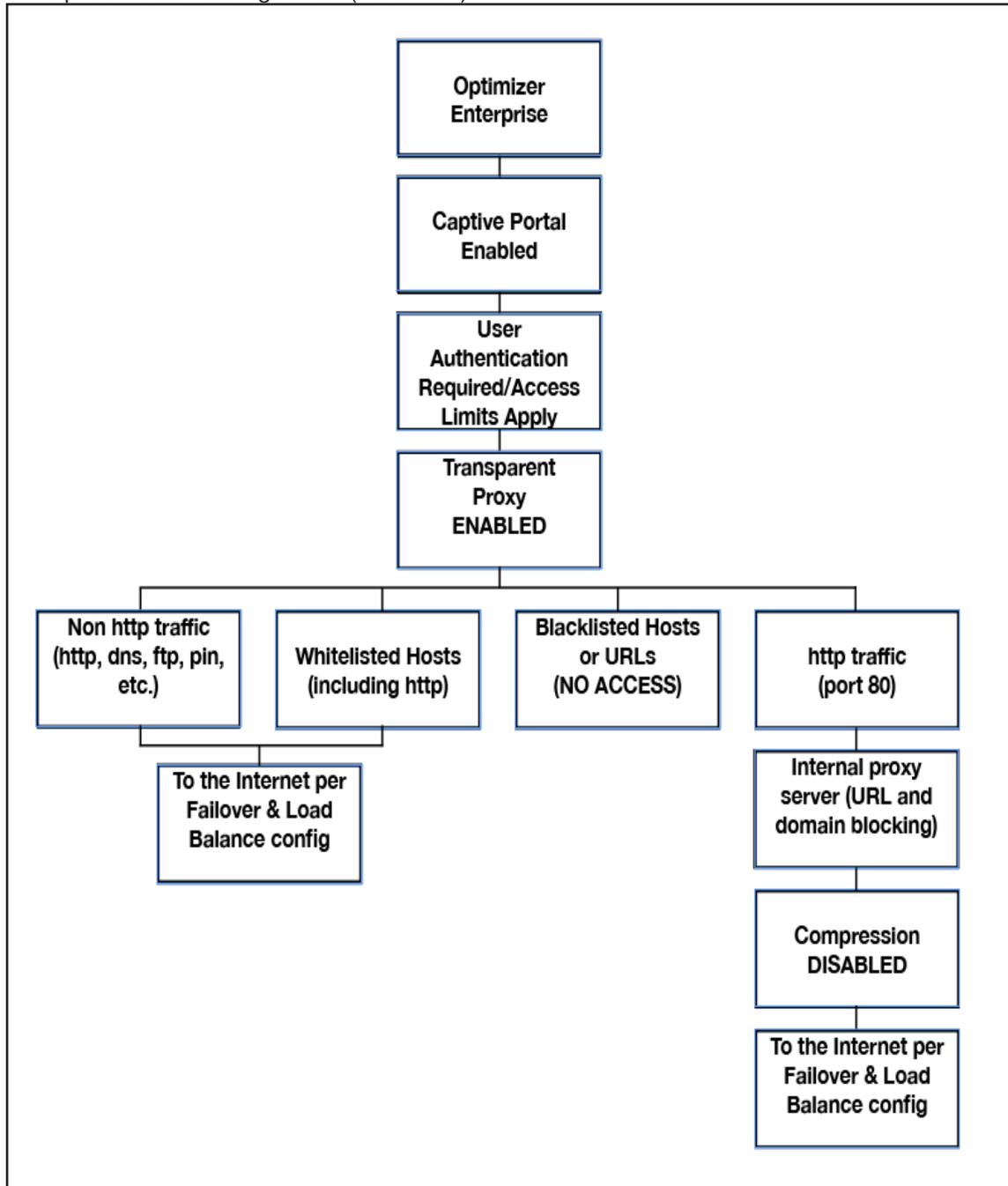
3.4.1. Default Configuration

- Captive Portal (Crew Internet Access) - enabled.
- Internal Transparent Proxy for http URL and content filtering - enabled Firewall - open.
- DNS - open.
- SMS - enabled, for compatible satellite devices.
- Voice Capability - for compatible satellite devices, disabled.
- Automatic Failover/Load Balance (All Traffic) - LTE/GSM > WAN1 > WAN2 Web Compression Service - disabled.
- RedPort Email Service - disabled GPS Tracking Service - disabled RedPort VoIP Service - disabled.

With the Captive Portal enabled, the firewall is automatically modified to allow data traffic through the router and users must 'authenticate' in order to access the Internet. You have several methods available for controlling user access to the Internet: you can whitelist and/or blacklist hosts and URLs; you can modify the firewall, you can modify the load balance to allow only certain traffic types through a certain interface, and you can require the use of PIN-Codes.

When generating PIN-Codes you can set the amount of data the user can download, you can limit access to certain hours of the day, and you can limit the speed of their connection.

Optimizer Enterprise Default Configuration (Data Flow)



Once a user logs in to the Captive Portal, data can take one of three paths:

1. Non-http traffic goes straight to the Internet: https, dns lookups, ftp, ping, scp, etc. The firewall rules are totally open so there is nothing blocking full access to the Internet. You can limit access through the Captive Portal. **See Chapter 5.1.1.**
2. Traffic to a Whitelisted Host in the Captive Portal, including http, goes straight to the Internet, bypassing the internal proxy server. If you whitelist a web-server, 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 web-server; however, you may want to whitelist a mail server, or a vpn. **See Chapter 5.1.1.**
3. All http traffic (on port 80), that is not Whitelisted, and only http (not https or secure traffic) is intercepted and

redirected to the internal proxy server. This is known as 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.

- In the default state of compression DISABLED, all traffic goes straight to the Internet.
- With compression enabled, all the http traffic goes to the upstream compression proxy server and returns a compressed page. Ads are stripped out, text is compressed, images are re-sampled 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.
- With compression enabled, Whitelisted Hosts or URLs bypass the upstream compression proxy server and go straight to the Internet, bypassing compression.

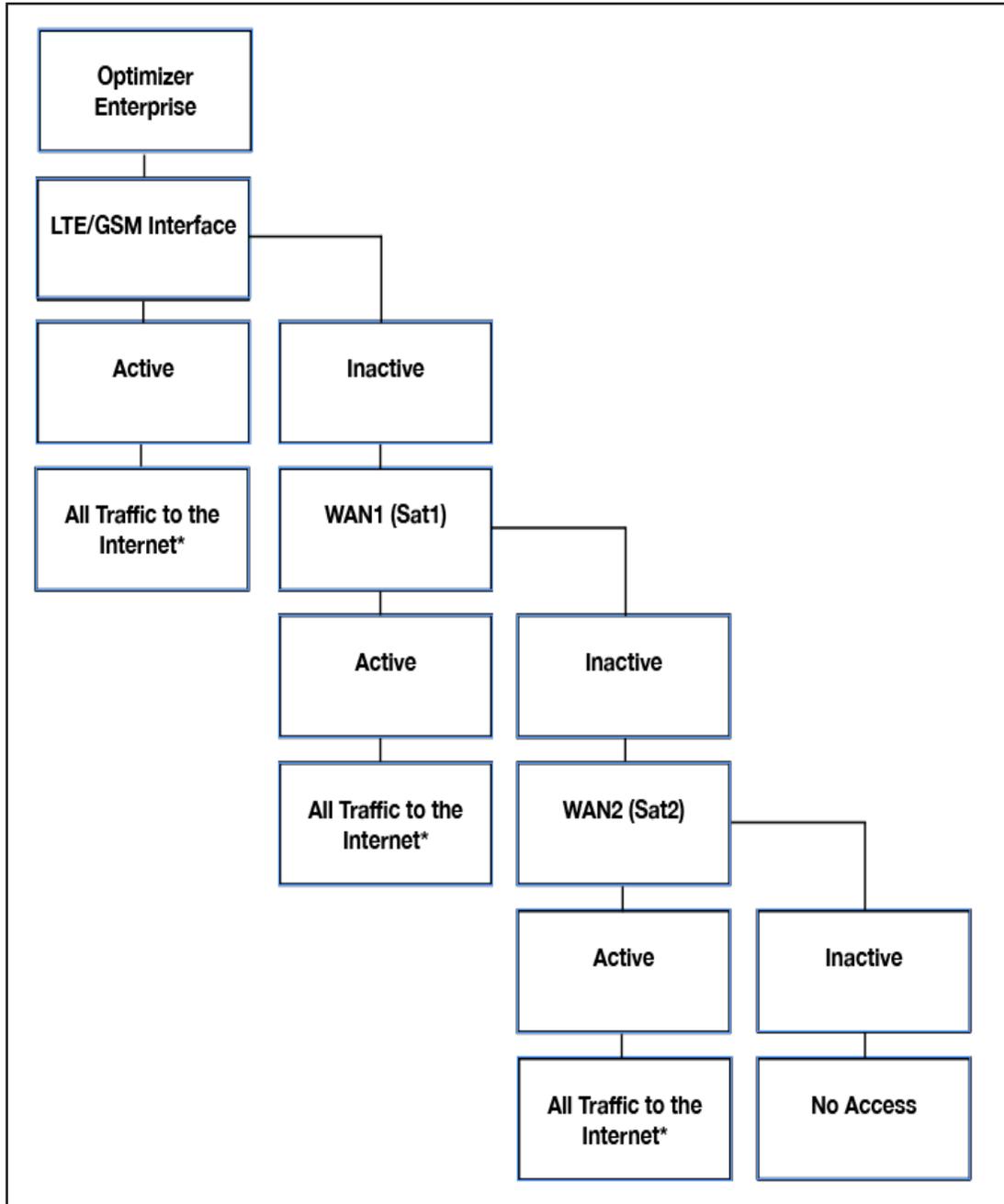
Blacklisted Hosts or URLs have no Internet access, regardless of compression status. **See Chapter 5.2.2.**

*The default Failover /Load Balancing configuration is as follows:

Setup is required for the LTE/GSM Interface.

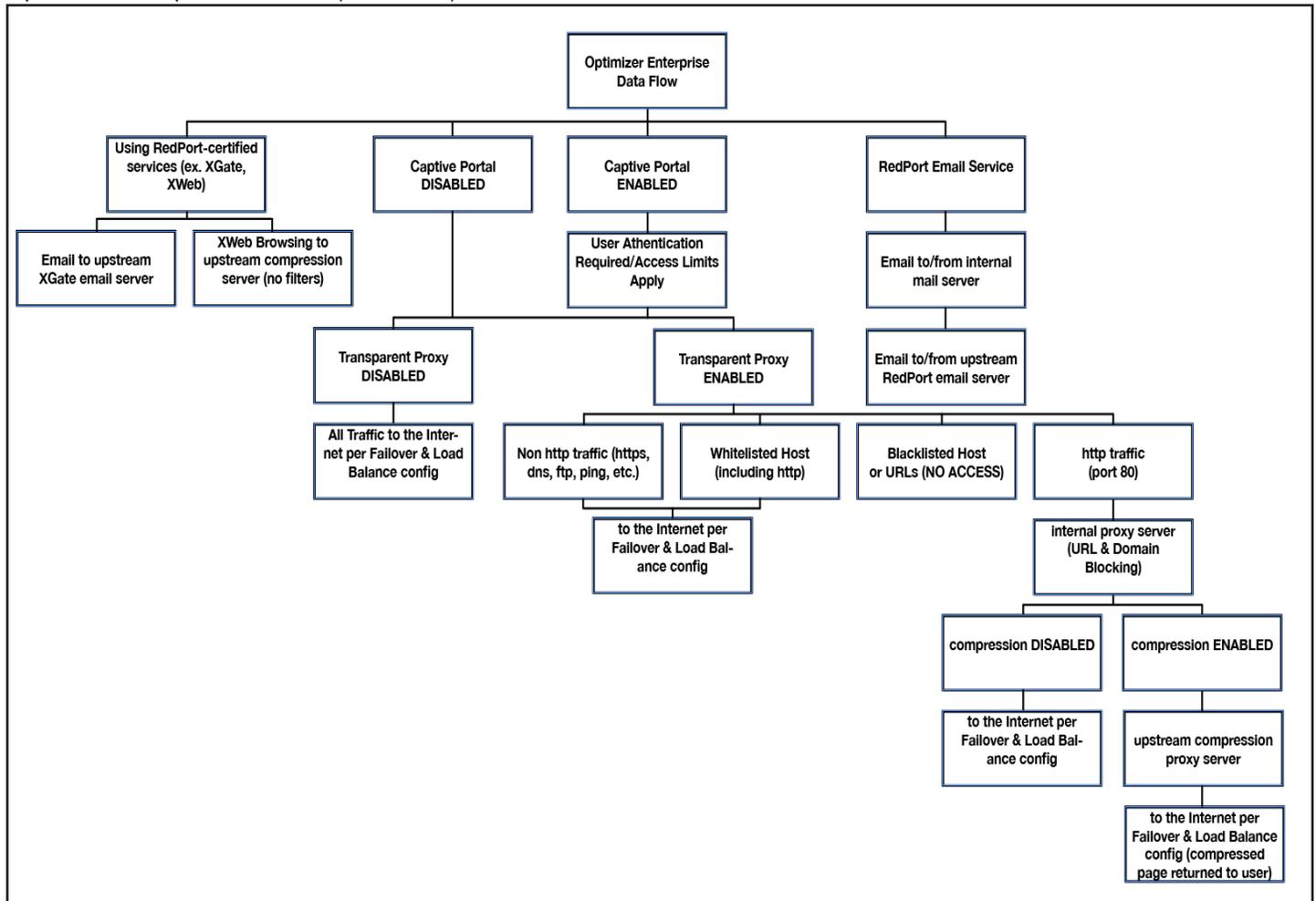
NOTE: All traffic to the Internet is subject to the firewall and load balance configuration. You can change the Failover configuration and you can Load Balance between and among the interfaces. For example, you can create rules to send all http traffic through the LTE/GSM Interface but never through the WAN ports. **See Chapter 9.13.**

Optimizer Enterprise **Default** Failover/Load Balancing Configuration (Data Flow)



3.4.2. Data Flow - All Paths

Optimizer Enterprise All Paths (Data Flow)



3.5. Navigating the User Interface

Access to the user interface depends upon how you log in 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 many pages in the user interface you will see three buttons in the bottom corners:



- **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.

4. Getting Started - User Interface Access

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

- Captive Portal (Crew Internet Access).
- Internal Transparent Proxy for Web Filtering (Including optional Pay service for QL dialadele.com).
- SMS Messaging using smartphones (for compatible devices).
- GPS/NMEA Repeater Voice Capability using smartphones (for compatible devices).
- Automatic Failover from LTE/GSM to WAN1 to WAN2

NOTE: LTE/GSM must be configured.

There are also services available that are disabled:

- 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 log in 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-524-XXXX-2.4GHz' or 'wxa-524-XXXX-5GHz' where 'XXXX' is the last four digits of the Optimizer Enterprise's Mac address. Select this wireless network.

For alternative Home Page access methods, see the Optimizer Enterprise Quickstart Guide.

2. Open any web browser on the computer and enter one of the following:

- http://192.168.10.1 or http://10.1.5.1.

3. The Optimizer Enterprise ships with two existing administrative accounts:

- Admin - for normal day-to-day operation by the onsite administrator.
- Superadmin - for configuration and maintenance by the installer/technician, etc.

4.1.1. Onsite Administrator Login (Admin)

Onsite Administrator: username=admin, password=webxaccess.

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

- Generate PIN-Codes (for captive portal use).
- Send/receive email (if email is enabled).
- Manage crew email accounts (if email is enabled).
- Monitor the system status.
- Manage the local WiFi setup (change the network name, password, etc.).
- Modify traffic routing if configured for Manual mode.
- Enable remote support for diagnostics and/or maintenance.

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

See the Optimizer Enterprise Onsite Administrator Guide for information in administering the most-used features.

4.1.2. Installer/Network Administrator Login (Superadmin)

Technician: username=superadmin, password=webxaccess.

This login opens to the Home page and 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.

The screenshot displays the RedPort router's Home page. At the top, there is a navigation bar with tabs for Home, Services, Status, System, VPN, Network, Users, Statistics, and Logout. Below this is a 'Tasks' bar with links for Traffic Routing and MWAN Overview. The main content area is titled 'Welcome' and is divided into several sections:

- Crew Internet Services:** Includes Captive Portal URLs (Login, Status, Logout) and buttons for Generate pincodes, Create users, Generate pincode usage reports (CDRs), and View/Manage pincodes.
- Email Access:** Shows email access settings and parameters (WEB, POP, SMTP) and a button to Go to webmail.
- Email Management:** Contains buttons for Create and manage crew email accounts, Retrieve, delete, or drop large emails (BigMail) quarantined on the server, Perform common email tasks, and View email logs.
- System Status:** Features buttons for System status overview, Realtime bandwidth usage over satellite link, Historic bandwidth usage over satellite link, and System message log.
- Local WiFi setup:** Includes SSID and Security settings and buttons for WiFi setup and Change hotspot name and/or add security and set password.
- System:** Contains buttons for Router password and Reboot router.

This Home Page is the onsite administrator's gateway to the most used features. See the Optimizer Enterprise

Onsite Administrator Guide for Home Page details and use.

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 Enterprise router.

VPN: Virtual Private Network permits a continuous shared private network across a public network.



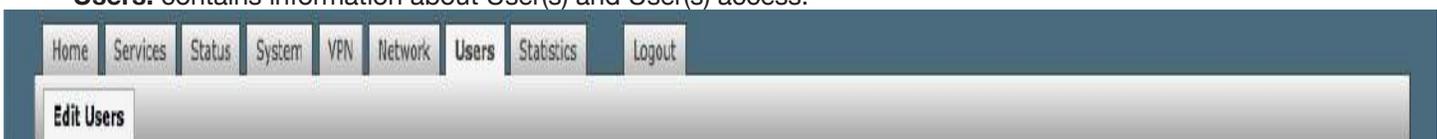
Use this section to set up a VPN through PPTP, IPSec, OpenConnect VPN, or OpenVPN options to configure a private network that transcends through a public network.

Network: contains access to the network Interfaces, the Firewall, and Failover and Load Balancing setup.



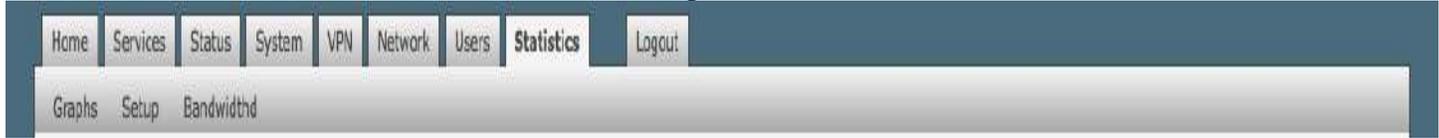
Use this section to configure network interfaces, run diagnostics, or modify the firewall. You can also change the Failover sequence and configure the load balance.

Users: contains information about User(s) and User(s) access.



Use this section to edit both User accounts as well as allow/limit access for each User.

Statistics: contains information about resource usage.



Use this section to review system statistical data related to the router's Interfaces, Wireless, System Load, Memory, Processes, and Uptime.

4.2. How to Use with Default Setup

We ship the router ready for use as follows:

- Anyone with an existing Primary Account with a RedPort-certified compression email service (such as XGate) and/or web browsing account (such as XWeb) is able to immediately use the router to send/receive email or browse the web. There are no Internet access restrictions when using these services. Users simply connect a computer, iOS, or Android device to the Optimizer Enterprise's wireless network, set the email "Connection Type" to "Optimizer xxxx" where xxxx represents the satellite connection. See the XGate Help file for more information.
- Captive Portal and Transparent Proxy are enabled to control access to the Internet so anyone opening a web browser (outside of XGate/XWeb) and entering a URL will be re-directed to the Captive Portal. They will not be able to access the Internet until they are setup as a user. Users that are given access via the Captive Portal can go anywhere on the Internet unless the installer has configured the proxy server to restrict access. Individual user access can be restricted by time; by data; by time of day; by speed. **See Chapter 5.1.**
- Voice is enabled for use with compatible satellite devices using standard satellite airtime. **See Chapter 5.8.**
- SMS is enabled for use with compatible satellite devices using standard satellite airtime. **See Chapter 5.5.**
- Failover sequence is set to Automatic - LTE/GSM > WAN1 > WAN2. LTE/GSM must be configured for use. **See Chapter 9.13.**
- Load Balance is set to ALL traffic through the one Active interface. **See Chapter 9.13.**
- Firewall is Open allowing all traffic to pass. **See Chapter 9.18.**

This out-of-the-box configuration works well for single broadband users with an XGate and/or XWeb primary account and can be suitable for the multi-interface, multi-user environment where each person has a separate primary XGate email and/or XWeb browsing account.

If in a multi-user environment we recommend the optional RedPort Email service for easy access and management of crew accounts. **See Chapter 5.3.** Additional fees may apply. Contact your service provider for current pricing.

Enabling Web Compression Service will direct all http traffic to the upstream compression proxy server and return a compressed page to the user. Ads are stripped out, text is compressed, images are re-sampled and more. On average, you will experience 3-5x compression on http traffic, thereby increasing the speed of your connection and the effective per Mb cost of your connection. **See Chapter 5.2.** Additional fees may apply. Contact your service provider for current pricing.

Transform your satellite device into a multi-user voice unit with the optional RedPort VoIP Service. 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 5.8.** Additional fees may apply. Contact your service provider for current pricing.

CAUTION: This router is shipped to you with all WAN ports open, POP and SMTP are open to the WAN if you

enable Email, if you enable the 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**.

4.3. Router Security

By default, your router is open to the Internet:

- WAN ports are open.
- Voice PBX, if enabled, is listening on all ports.
- POP and SMTP are open to the WAN, if Email is enabled.

This setup 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

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 Services > Crew Internet Access > Tools and change the Admin password for the Captive Portal admin access. **See Chapter 5.1.4.1**.

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 9.8**. 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 Captive Portal or LAN) in Services > Voice PBX > Settings (**See Chapter 5.8**). OR, you can leave it to listen on all interfaces and use a firewall rule to restrict traffic (**See Chapter 9.8**).

CAUTION: Blocking 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.

CAUTION: 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.

5. Services

5.1. Crew Internet Services (Captive Portal)

The Optimizer Enterprise is shipped with Captive Portal enabled. This allows controlled access to the Internet by requiring authentication by users. It blocks access to the Internet without authentication. Authentication can be via username and password or PIN-Code or Mac address of a specific PC. **See Chapter 5.1.2.**

PIN-Codes to restrict access can be created by the Onsite Administrator. In addition, the speed of access can be limited by the PIN-Code as can the duration/or time of the session. **See Chapter 5.1.2.3.**

User sessions are logged in Call Data Records (CDR) for tracking the amount of time on the service and the amount of data transferred. **See Chapter 5.8.3.**

The screenshot displays the 'Captive Portal Settings for Crew Internet Access' configuration page. At the top, there is a navigation bar with 'Home', 'Services', 'Status', 'System', 'VPN', 'Network', 'Users', 'Statistics', and 'Logout'. Below this is a secondary menu with 'Crew Internet Access' selected, and sub-items like 'Web Compression and Filtering', 'RedPort Email', 'Remote Access', 'SMS', 'GPS Tracking', 'Dynamic DNS', 'GPS/NMEA Repeater', 'Voice PBX', 'SNMP', and 'Network Shares'. The 'Settings' section includes 'Users', 'Pass-through MAC', 'Pincodes', 'CDRs', and 'Tools'. The main heading is 'Captive Portal Settings for Crew Internet Access'. Below the heading is a descriptive paragraph: 'Share and control access to the Internet by requiring users to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. User sessions are logged by Call Data Records (CDR) tracking time and amount of data transferred.' A note states: 'Note: Router will **reboot** on Save & Apply.' The configuration area has four tabs: 'General Settings' (selected), 'Advanced Settings', 'Allowed Hosts', and 'WPAD'. There are four main settings: 1. 'Enable' with a checked checkbox and a blue information icon; the text says 'Enable/Disable captive portal.' and includes a 'Caution' about high traffic usage. 2. 'Enable Fleetwide Pincodes' with an unchecked checkbox and a blue information icon; the text says 'Allow the use of pincodes that can float between vessels.' and includes a 'Caution' about administrative overhead and a note that floating pincodes cannot be generated on the router. 3. 'Enable Transparent Proxy' with a checked checkbox and a blue information icon; the text says 'Enable/Disable transparent routing to upstream HTTP proxy for compression and filtering.' 4. 'HotSpot Name' with a text input field containing 'RedPort HotSpot' and a blue information icon; the text says 'Name of hotspot as displayed on login and status screens.' At the bottom left is a 'Reset' button, and at the bottom right are 'Save' and 'Save & Apply' buttons.

The image above is the default state of the Captive Portal Settings as the router is shipped to you. See the Optimizer Enterprise Onsite Administrator Guide for information on how the onsite administrator manages Captive Portal use.

5.1.1. Captive Portal Settings

5.1.1.1. General Settings



Requires 'superadmin' login.

With the Captive Portal enabled, all users trying to use the Internet will be redirected to a screen where they will be required to enter a PIN-Code or a username and password before they will be allowed to browse the Internet.

CAUTION: With Captive Portal enabled, the firewall is wide open to all traffic; so, it is important to configure a firewall and/or have internal Transparent Proxy enabled WITH filtering configured, to control usage.

Internal Transparent Proxy is enabled which means that all http traffic that is not whitelisted or blacklisted is redirected to the router's internal proxy server. This internal proxy server can be configured for URL blocking and domain blocking.

CAUTION: If you Disable Transparent Proxy then all http traffic goes straight to the Internet without any filtering.

HotSpot Name is the name on the page that is presented to the user when they log in. RedPort HotSpot is the default name. Customize the HotSpot Name by entering the text you prefer.

5.1.1.2. Advanced Settings

Requires 'superadmin' login.

In general, there are only two items on this page that may require modification, Idle Timeout and Session Timeout.

Captive Portal Settings for Crew Internet Access

Share and control access to the Internet by requiring users to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. User sessions are logged by Call Data Records (CDR) tracking time and amount of data transferred.

Note: Router will **reboot** on **Save & Apply**.

General Settings | **Advanced Settings** | Allowed Hosts | WPAD

Idle Timeout	300	Default idle timeout in seconds. User will be logged out if no traffic is detected for this period. Set to '0' for unlimited.
Session Timeout	3600	Default session timeout in seconds. User will be logged out at the expiration of this timer. Set to '0' for unlimited.
DNS Domain	local	
Primary DNS Server	10.15.1	
Secondary DNS Server	192.168.10.1	
Update Interval	60	Captive portal accounting update interval in seconds. Smaller intervals result in more accurate accounting at the cost of higher CPU loads.
TCP Ports	80 443 25 110 22 53 5454 89 5080 5062	White space separated list of white listed ports on the router. These are ports on the router itself that are allowed access through the captive portal. Port 80 allows access to the web admin, port 110 and 25 to the mail server, etc.
IP Address	10.15.1	IP address of captive portal. Must be in the same subnet as the captive portal network.
Redirect URL	http://10.15.1:4090/www/status.chi	Force user to this URL after login. Leave blank string for default URL.
Network Address	10.15.0	Network address of captive portal. Must be in the same subnet as the captive portal IP address.
Netmask	255.255.255.0	Network address mask.

Reset | Save | Save & Apply

Idle Timeout - The default is set to 300 seconds (5 minutes). If no traffic is detected for the idle timeout period, the user will be automatically logged out. They must log in again to continue.

Session Timeout - The default is set to 3600 seconds (60 minutes). The user will be automatically logged out at the end of the session timeout period. They must log in again to continue.

Both of these timers can be set to '0' for unlimited time period; however, that is NOT recommended. Using Idle Timeout and Session Timeout minimizes the consumption of data without the user's knowledge. For instance, using the default settings as an example, if a user is logged in and has Skype open, and then walks away from the computer, because Skype is running in the background, the Idle Timeout period will never be reached because traffic is detected. However, after 60 minutes, the Session Timeout period will expire. The user must log back in to use the Internet when they return to the computer regardless of the length of time they've been gone, 61 minutes or two days. By having a Session Timeout period, background data is stopped. If there is no background data running the user is logged out at the end of the Idle Timeout period.

5.1.1.3. Allowed Hosts

Requires 'superadmin' login.

This is the whitelist for the Captive Portal. These are the hosts that can be accessed without having to log in

through the captive portal.

The screenshot shows the RedPort web interface. The top navigation bar includes 'Home', 'Services', 'Status', 'System', 'VPN', 'Network', 'Users', 'Statistics', and 'Logout'. Below this, there are sub-menus for 'Crew Internet Access' (Web Compression and Filtering, RedPort Email, Remote Access, SMS, GPS Tracking, Dynamic DNS, GPS/NMEA Repeater, Voice PBX, SNMP, Network Shares) and 'Settings' (Users, Pass-through MAC, Pincodes, CDRs, Tools). The main heading is 'Captive Portal Settings for Crew Internet Access'. A note states: 'Note: Router will reboot on Save & Apply.' Below this are tabs for 'General Settings', 'Advanced Settings', 'Allowed Hosts', and 'WPAD'. The 'Allowed Hosts' tab is active, showing a list of 15 entries with delete icons. The entries are: 209.170.128.0/19, 208.79.80.0/22, 208.86.224.0/22, 204.109.56.0/21, 199.48.128.0/21, 199.102.76.0/22, 69.64.64.48, 68.168.97.37, 64.150.188.243, 209.160.77.225, 209.160.78.93, 208.85.241.104, 74.115.212.64/29, 69.64.67.148/29, and 192.168.90.0/24. A legend below the list explains the format: 'Hosts, IP Addresses, and Networks that are allowed without authentication. Valid entries include fully qualified hostname, IP address, or network address in CIDR format. e.g. www.google.com, 8.8.8.8, 208.45.23.0/24.' At the bottom, there are 'Reset', 'Save', and 'Save & Apply' buttons.

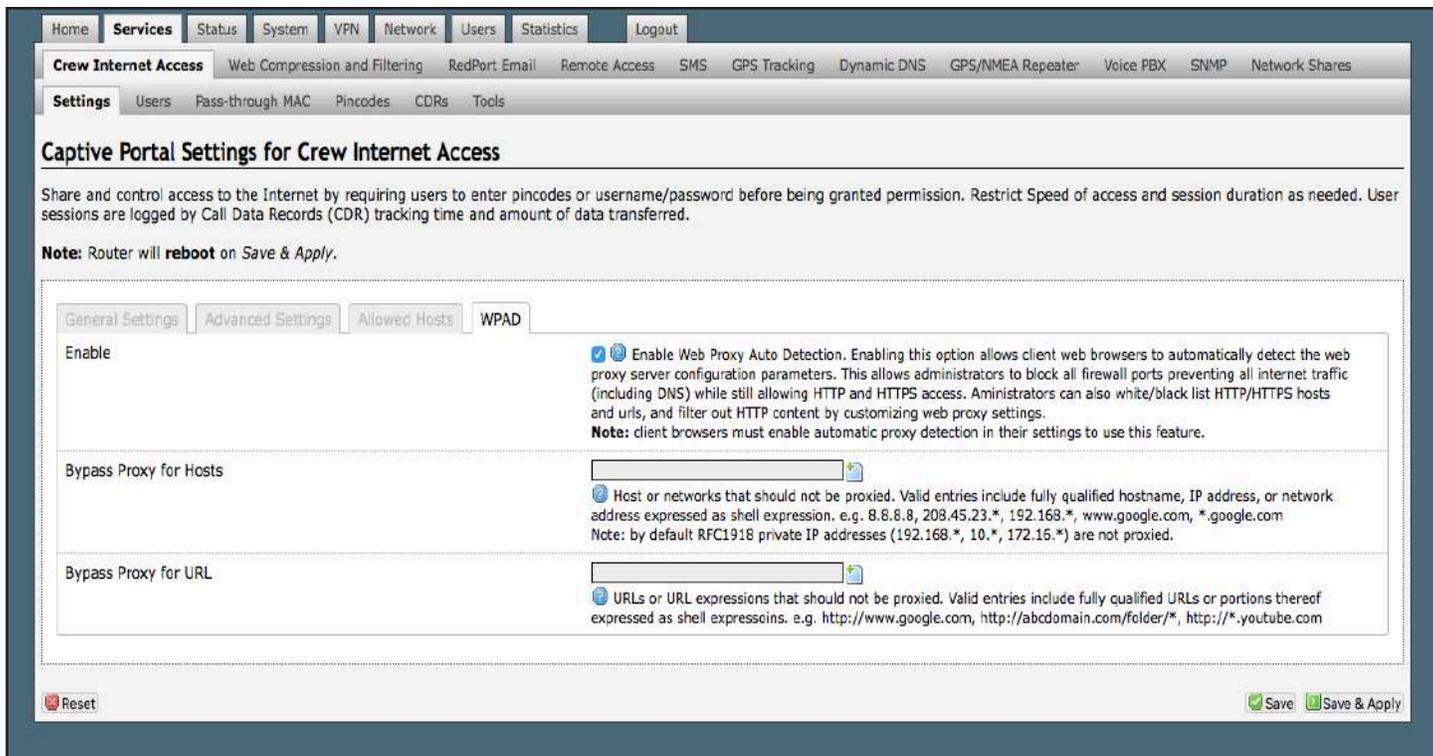
By default, there are a number of hosts there. They are all GMN hosts for our services (email, VOIP, etc.) If you don't want them, you can delete them.

NOTE: If you are using an email service that is not RedPort or XGate, this is where you would add the email servers of your chosen service.

5.1.1.4. WPAD

Requires 'superadmin' login.

WPAD is a special feature for auto configuring the proxy settings on the client's web browser for tighter control over access to the Internet.



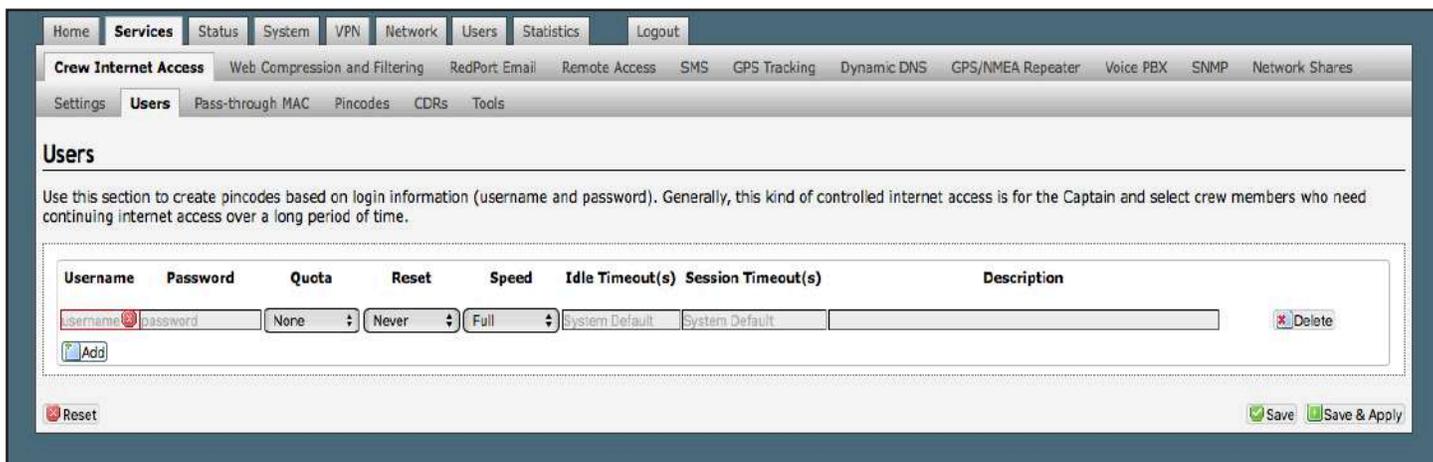
5.1.2. Allowing Individuals Access to the Internet

There are three ways to manage access to the Internet via the Captive Portal:

5.1.2.1. Users with Username and Password

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

Create Users with a username and password with the Users Tab. Use this section to restrict access in lieu of using PIN-Codes. Typically reserved for the onsite administrator and select crew who need continuing access over a long period of time.



NOTE: By default, there is one Captive Portal user that is not visible in the UI. It is username=admin, password=webxaccess. It is recommended that you change the password for this admin user. See **Chapter 5.1.4.1.**

- **Username:** A unique character string that this user will enter at log in.
- **Password:** A character string that the user will enter at log in. The Password must be different from the username.
- **Quota:** You can restrict the username to a specific amount of data transferred. The default is no restriction. To set a maximum, use the drop-down menu. When you set a maximum, the user has Internet access until the maximum is reached. When the maximum is reached the user will be disconnected from the Internet.
- **Reset:** The Quota assigned to a Username can be configured to reset periodically (daily, weekly, monthly) using the drop-down menu. When a reset period is selected, the Quota will renew automatically at the start of the new reset period.
- **Speed:** Set the maximum bandwidth allowed for this user.

NOTE: Maximum speed is dependent upon the speed of the satellite device/service.

- **Idle Timeout(s):** Expressed in seconds, enter the idle timeout period to change it from the default. At the end of the idle period, the user will be logged out if no traffic has been detected during the period. The default period is configured at installation and can be found in Services > Crew Internet Access > Settings > Advanced Settings.
- **Session Timeout(s):** Expressed in seconds, enter the session timeout period to change it from the default. At the end of the timeout period the user will be logged out of the session. The default period is configured at installation and can be found in Services > Crew Internet Access > Settings > Advanced Settings.
- **Description:** Optional - Enter a short description of the account.

Click <Save> to enter more users or click <Save & Apply> when all users are entered. Wait for the message "Configuration Applied".

5.1.2.2. Pass-Through MAC

Requires 'superadmin' login.

Allow specific devices on the local network to immediately access the Captive Portal without having to log in, by adding the MAC address of the device. (Not Recommended)

The screenshot shows the RedPort web interface. The top navigation bar includes: Home, Services, Status, System, VPN, Network, Users, Statistics, Logout. Below this is a sub-menu for 'Crew Internet Access' with options: Web Compression and Filtering, RedPort Email, Remote Access, SMS, GPS Tracking, Dynamic DNS, GPS/NMEA Repeater, Voice PBX, SNMP, Network Shares. The current page is 'Pass-through MAC' under the 'Users' sub-menu. The page title is 'Pass-through MAC'. Below the title is a descriptive paragraph: 'Adding MAC addresses to the pass-through list allows them access through the captive portal automatically without authentication. The device may need to be repowered or have its DHCP lease renewed after assigning it a static IP address. Note that pass through MAC address will be disconnected after the captive portal timeout period and become inoperable. Best practice has setting long timeouts for these devices.' Below this is a section titled 'Connected Devices' containing a table with two columns: 'MAC' and 'IP Address'. The table lists two entries: 'F4-90-EA-10-10-92' with IP '10.15.3' and '10-DD-B1-A2-AD-6C' with IP '10.15.2'. Below this is a section titled 'White Listed Devices' with a note: 'Note: It takes a few seconds to reassign a static IP address. Refresh the page to see updated values.' Below the note is a table with headers: 'MAC', 'IP Address', 'Quota', 'Reset', 'Speed', 'Idle Timeout(s)', 'Session Timeout(s)', and 'Description'. The table is currently empty, with the text 'This section contains no values yet' centered below it. At the bottom left is a 'Reset' button, and at the bottom right are 'Save' and 'Save & Apply' buttons.

See **Chapter 5.1.2.3** for Quota, Reset, Speed and Timeout descriptions.

5.1.2.3. PIN-Codes

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

Generate PIN-Codes to limit Internet access. Sell them or give them to transient crew, passengers, or visitors.

Home **Services** Status System VPN Network Users Statistics Logout

Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PEX SNMP Network Shares

Settings Users Pass-through MAC **Pincodes** CDRs Tools

Pincodes

Generate captive portal pincodes.

Number of Pincodes	<input type="text" value="10"/>
Prefix	<input type="text" value="1234"/> <small>number to be prepended to pincodes.</small>
Quota	<input type="text" value="None"/> <small>Pincodes will allow users on the internet until their quota is exhausted.</small>
Reset	<input type="text" value="Never"/>
Expire	<input type="text" value="Never"/> <small>Pincodes will unconditionally expire this time period after creation (i.e. drop dead date). This setting takes precedence over the "Reset" period.</small>
Speed	<input type="text" value="Full"/>
Start Time	<input type="text" value="Unrestricted"/> <small>Limit a data session from start through end time. Times are in the router's local timezone.</small>
Stop Time	<input type="text" value="Unrestricted"/> <small>Limit a data session from start through end time. Times are in the router's local timezone.</small>
Pincodes	<input type="button" value="Create"/> <small>Create Pincodes.</small>
Enter Filename	<input type="text" value="pincodes-2018-02-25.csv"/>
Download	<input type="button" value="Download"/> <small>Download a CSV file containing pincodes.</small>

To create pincodes for controlled internet access:

- Select pincodes parameters (quota, reset interval, and speed).
- Push 'Create' to create pincodes.
- Push 'Download' to download CSV formatted spreadsheet.

Description of Parameters:

- Number of Pincodes : Specifies the number of unique pincodes to generate with the same Quota, Reset period, and Speed.
- Prefix : An arbitrary text to add to the pincodes number. This might be helpful for tracking pincodes inventory.
- Quota : size in Mb of the pincodes. The user will be able to use their pincodes for internet or email access until the total number of Mb sent/received exceeds this value. Once that threshold is met, the user will be logged out and no longer able to access internet/email. If there is a reset period on the pincodes, the user will be able to log back in using the same pincodes once the reset period is reached.
- Reset : Reset period for pincodes. This allows for a specified renewal time for the pincodes to become active again. If a pincodes as a reset period of 'None' the pincodes will not renew when it expires (this would be a one-time pincodes).
- Expire : Drop dead date for pincodes. Pincodes will unconditionally expire the selected period after creation. The drop dead date takes precedence over the "Reset" period.
- Speed : Maximum bandwidth consumed by the user.
- Start/Stop Time : Specifies time slot for which a pincodes user is allowed access to the Internet.

- **Number of Pincodes:** Enter the quantity of pincodes that will have the same configuration/restrictions, up to the maximum of 100 pincodes can be created in a batch.

- **Prefix:** This can be useful for tracking pincode inventory. Enter up to a five-digit number that will be added to the pincode.
- **Quota:** You can restrict a pincode to a specific amount of data transferred. The default is no restriction. To set a maximum, use the drop-down menu. When you set a maximum, the user has Internet access until the maximum is reached. When the maximum is reached the pincode will stop working.
- **Reset:** The pincode can be configured to reset periodically (daily, weekly, monthly) using the drop-down menu. When a reset period is selected, the pincode configuration will renew automatically at the start of the new reset period. For example, if a pincode has a quota of 10Mb of data and the reset period is set to daily, that user will be allowed to transfer a maximum of 10Mb of data each day. Once the maximum data transfer of 10Mb is achieved the pincode will temporarily stop working until the start of the next period. If the Reset period is set to Never, once the maximum quota is achieved the pincode expires and it cannot be renewed.
- **Speed:** Set the maximum bandwidth allowed for this pincode.

NOTE: maximum speed is dependent upon the speed of the satellite device/service.

- **Start Time:** Use Start Time in conjunction with Stop Time to limit the time of day a pincode can be used. Select a Start Time from the drop-down menu.

NOTE: A Stop Time must also be selected.

- **Stop Time:** Use Stop Time in conjunction with Start Time to limit the time of day a pincode can be used. Select a Stop Time from the drop-down menu.

NOTE: A Start Time must also be selected.

- **Pincodes:** When all the parameters of the pincode are selected in the fields above, click <Create> to generate the pincodes. The list of pincodes will display in the text window.

```
Number of pincodes: 10
Quota: none bytes
Reset interval: Never
Expire: never
Speed: Full

4086789-0184
8966715-8954
1968416-0520
4031340-7609
3197847-4155
1510602-2117
```

- **Enter Filename:** Use in conjunction with Download to create a .csv file as the new pincodes are generated. Enter a name for the .csv file.
- **Download:** Use in conjunction with Enter Filename to create a .csv file as the new pincodes are generated. Click <Download> and Save the file to the computer. Open the .csv file to see the pincodes.

5.1.3. CDRs (Call Data Records)

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

Call Data Records (CDRs) are usage logs. They are the accounting for the Captive Portal system. Usage quotas, time restrictions and resets all use the CDRs. Anyone that logs into the Captive Portal will have a CDR. They can

be generated for any PIN-Code or any username or any MAC address.

CDRs

Generate CDRs (Call Data Records, or the reports for internet usage) for users and pincodes.

Username or Pincode

Enter "All" to for a complete list of all CDRs. Note this could take some time to complete on systems with many pincodes.

Reporting Period

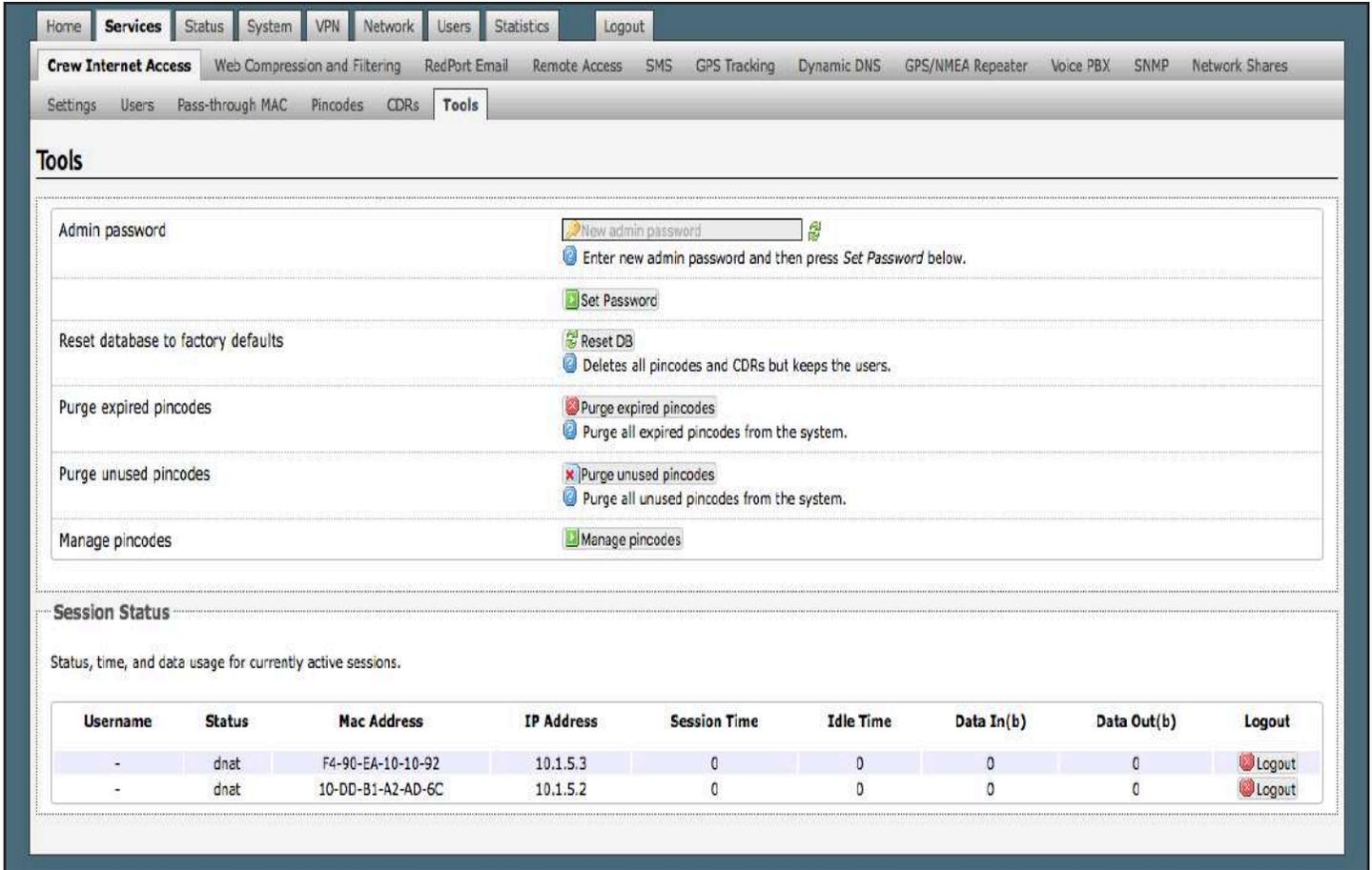
Submit

- **Username or Pincode:** Enter the username or pincode for the CDR you want to view, download or remove.
- **Reporting Period:** Select the period from the drop-down menu.
- **Submit:** Select this to view the log for the username or pincode entered above.
- **Enter Filename:** Use in conjunction with Download to create a .csv file of the CDR. Enter a name for the .csv file.
- **Download CSV:** Use in conjunction with Enter Filename to create a .csv file of the CDR. Click <Download> and Save the file to the computer. Open the .csv file to see the CDR.
- **Remove CDRs:** Click <Remove> to delete the CDRs for the username or pincode.

5.1.4. Tools

Requires 'superadmin' login.

This section can be used to change the Admin password for the Captive Portal and for Captive Portal clean up.



5.1.4.1. Admin password

This can be used to change the admin password for the Captive Portal. This is NOT the admin password to the router itself. By default, the Captive Portal login is: username=admin, password=webxaccess. You will notice that it happens to be the same as the admin password for the router. Best Practice: Create a new password here for the Captive Portal 'admin' login.

To change the password, enter the new password in the text box and click <Set Password>.

5.1.4.2. Reset Database to Factory Defaults

This wipes out the entire pincode database including CDRs.

CAUTION: This action CANNOT be undone.

5.1.4.3. Purge Expired PIN-Codes

Over time, as the database builds, you may want to purge expired PIN-Codes to free up space.

5.1.4.4. Purge Unused PIN-Codes

Use this to purge unused PIN-Codes from the system.

5.1.4.5. Manage PIN-Codes

This will show a summary of all the PIN-Codes, all the usernames, and all the MAC addresses that are active in the

Captive Portal. Each one appears as a separate line item in the PIN- Codes table.

The screenshot shows the RedPort web interface. At the top, there is a navigation menu with tabs for Home, Services, Status, System, YFN, Network, Users, Statistics, and Logout. Below this is a sub-menu for 'Crew Internet Access' with various service options like Web Compression and Filtering, RedPort Email, Remote Access, SMS, GPS Tracking, Dynamic DNS, GPS/NMEA Repeater, Voice PBX, SNMP, and Network Shares. A secondary menu includes Settings, Users, Pass-through MAC, Pincodes, CDRs, and Tools.

The main content area is titled 'Tools' and contains a 'Manage Pincodes' section. This section includes several actions: 'Select All Pincodes' (with a green 'Select' button), 'Un-Select All Pincodes' (with a green 'Un-Select' button), 'Remove CDRs' (with a red 'Reset' button and a blue 'Delete CDRs for selected pincodes' button), 'Delete All Selected' (with a red 'Delete' button), and 'Download CSV' (with a green 'Download' button). There is also a text input field for 'Enter Filename' containing 'pins-2018-02-25.csv'.

Below the 'Manage Pincodes' section is a table titled 'Pincodes'. The table has the following columns: Pincode, Speed, Quota, Reset, Expire, Time Range, Usage(b), Time(s), Select, Reset, Delete, and Edit. The table contains 20 rows of data, each representing a different PIN-Code configuration.

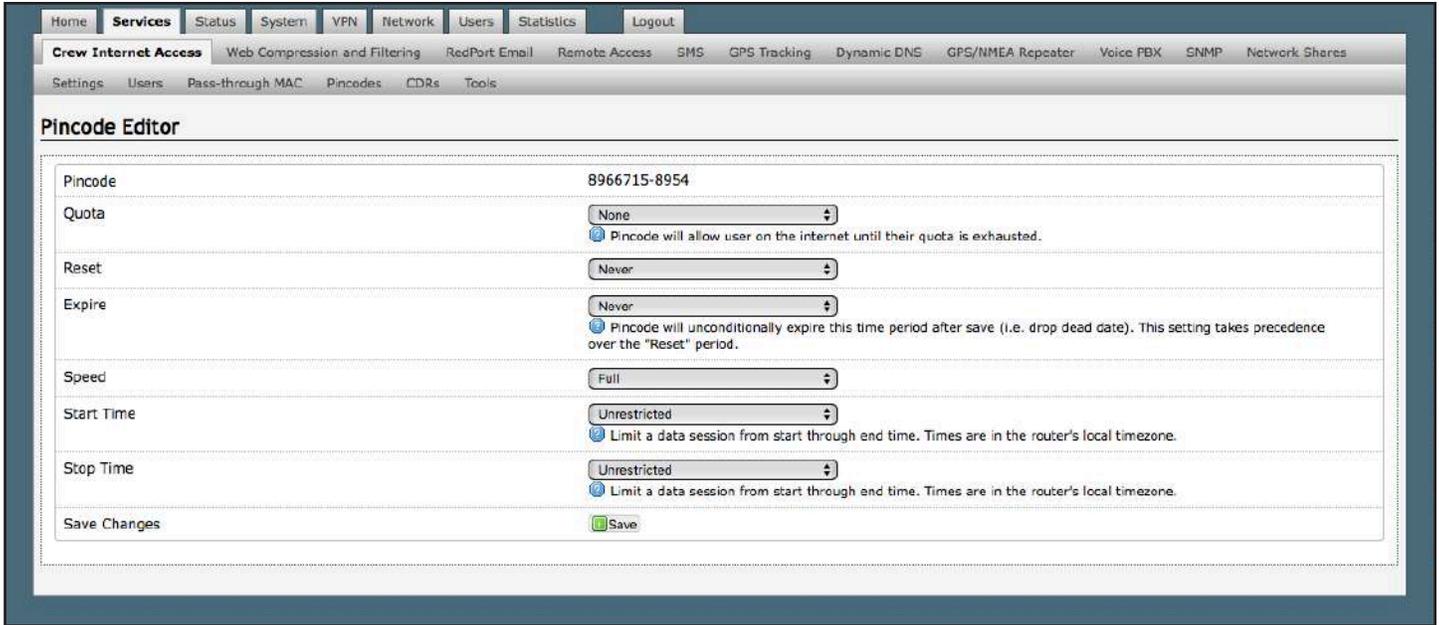
Pincode	Speed	Quota	Reset	Expire	Time Range	Usage(b)	Time(s)	Select	Reset	Delete	Edit
test	128 kbps	10485760	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
jason	open	none	never	never	unrestricted	235267821	4806	<input type="checkbox"/>			
C8-E0-EB-53-98-9E	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
C8-E0-EB-53-98-9D	open	none	never	never	unrestricted	17384617	17071	<input type="checkbox"/>			
C8-E0-EB-53-98-1A	16 kbps	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
9295491-7428	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
8966715-8954	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
6632431-1485	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
5849211-0527	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4860980-5534	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4798984-8891	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4472760-7312	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4461521-7673	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4298399-8349	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4139695-3303	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4086789-0184	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
4031340-7609	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
3475663-4940	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
3235248-4060	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
3197847-4155	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
3156068-7854	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
2788226-4302	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
2567907-4697	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
1968416-0520	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			
1510502-2117	open	none	never	never	unrestricted	nil	nil	<input type="checkbox"/>			

Using the top section of this screen you can:

- Remove CDRs for one or more 'PIN-Codes'.
- Delete one or more 'PIN-Codes'.
- Download the table to a .csv file.

In addition, using the buttons in the PIN-Codes table, you can:

- Reset the Quota of an individual PIN-Code.
- Delete the PIN-Code from the system, including the CDRs.
- Edit the parameters of the PIN-Code.



In the example above, we have elected to edit the PIN-Code 8966715-8954. See [Chapter 5.1.2.3](#) for information on PIN-Code parameters.

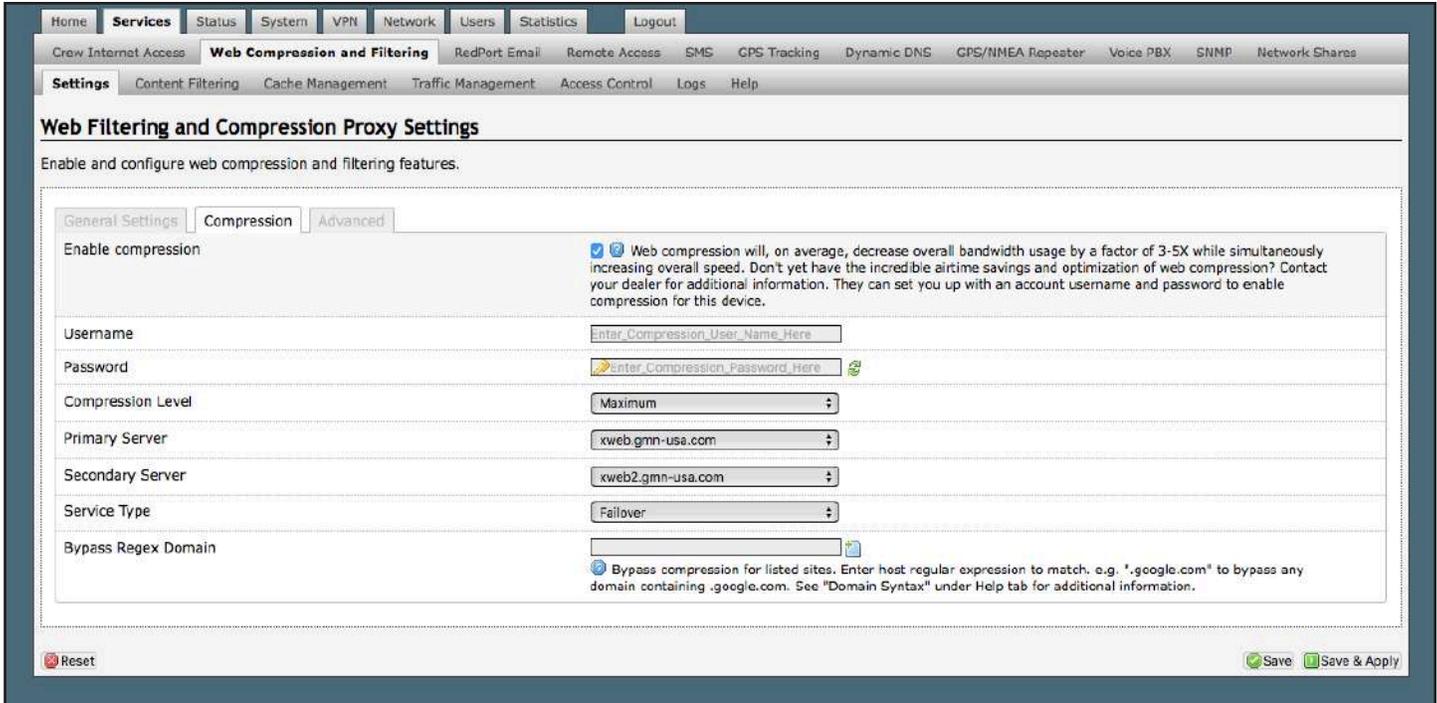
5.2. Web Compression and Filtering

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.

5.2.1. Settings

Requires 'superadmin' login.



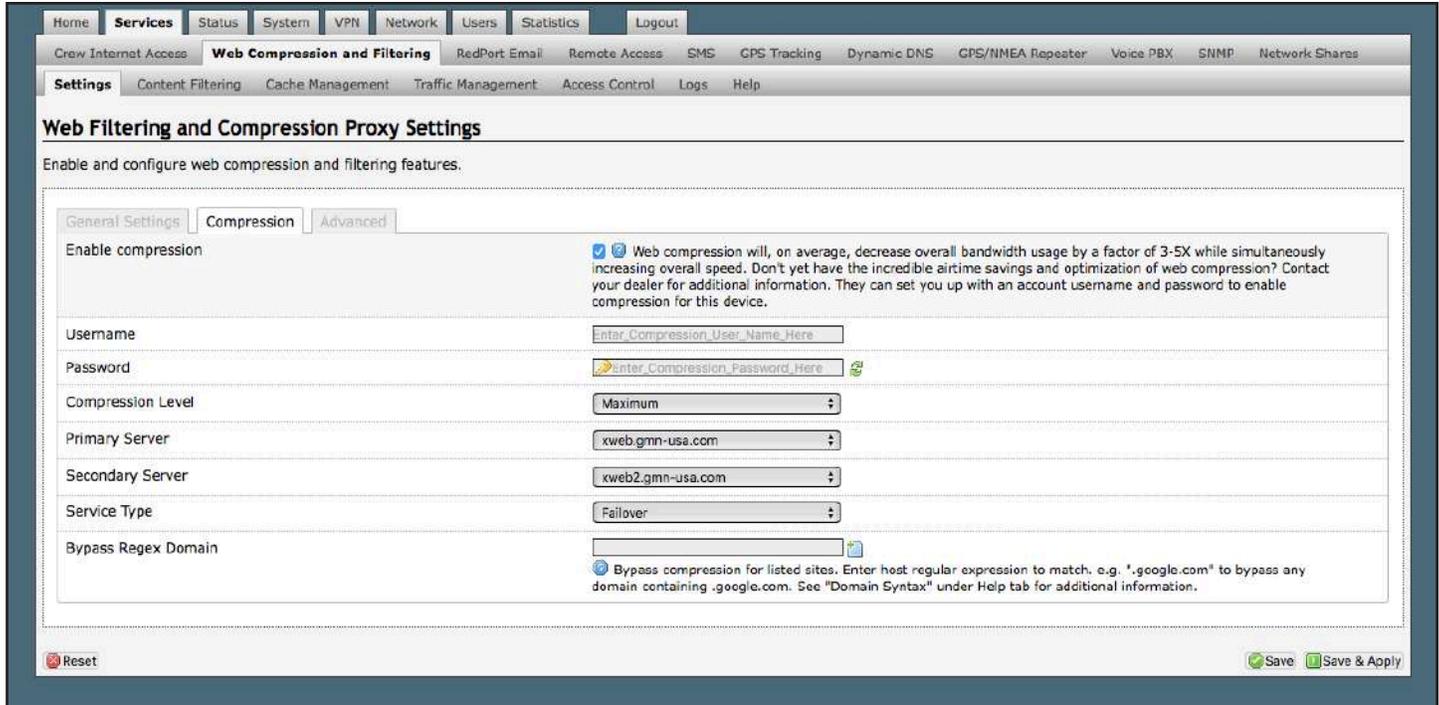
5.2.1.1. Compression

Requires 'superadmin' login.

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 Shared Web Compression service, click the checkbox to Enable compression. The page will expand, see With Compression Enabled below.
- **Username:** Enter the Username given to you by your service provider. This username is specific to the compression service.
- **Password:** Enter the Password given to you by your service provider. This password is specific to the compression service.
- **Bypass Regex Domain:** This is the 'whitelist' of sites that should not be compressed. To add a site, 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.

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



- **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 log in on your behalf. If this is checked, then the authentication happens at the user end, which means that when a user goes to any website 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 airtime plans should select “Maximum”. Those on high data plans may prefer “Standard” or “Minimum”.

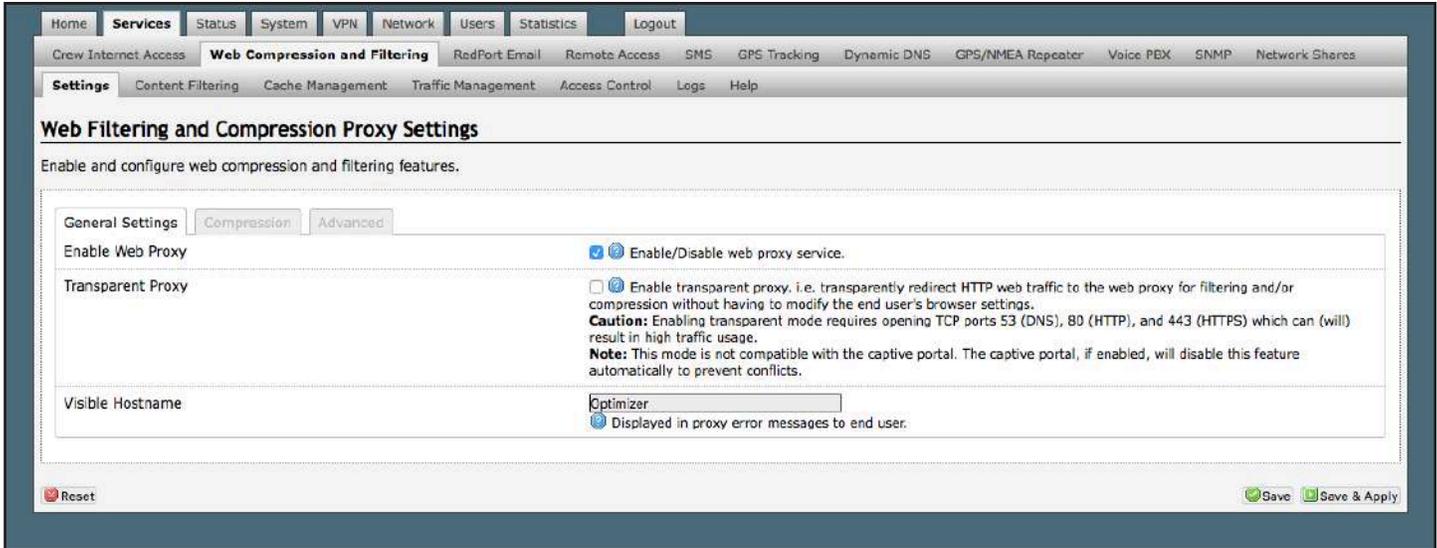
5.2.1.2. General Settings

Requires ‘superadmin’ login.

These are the general settings for the internal proxy service when the Captive Portal is Disabled.

Since the Captive Portal is enabled by default, there is no need to change anything on this page. In fact, if the Captive Portal is enabled, the features on this page will automatically be disabled to prevent conflicts.

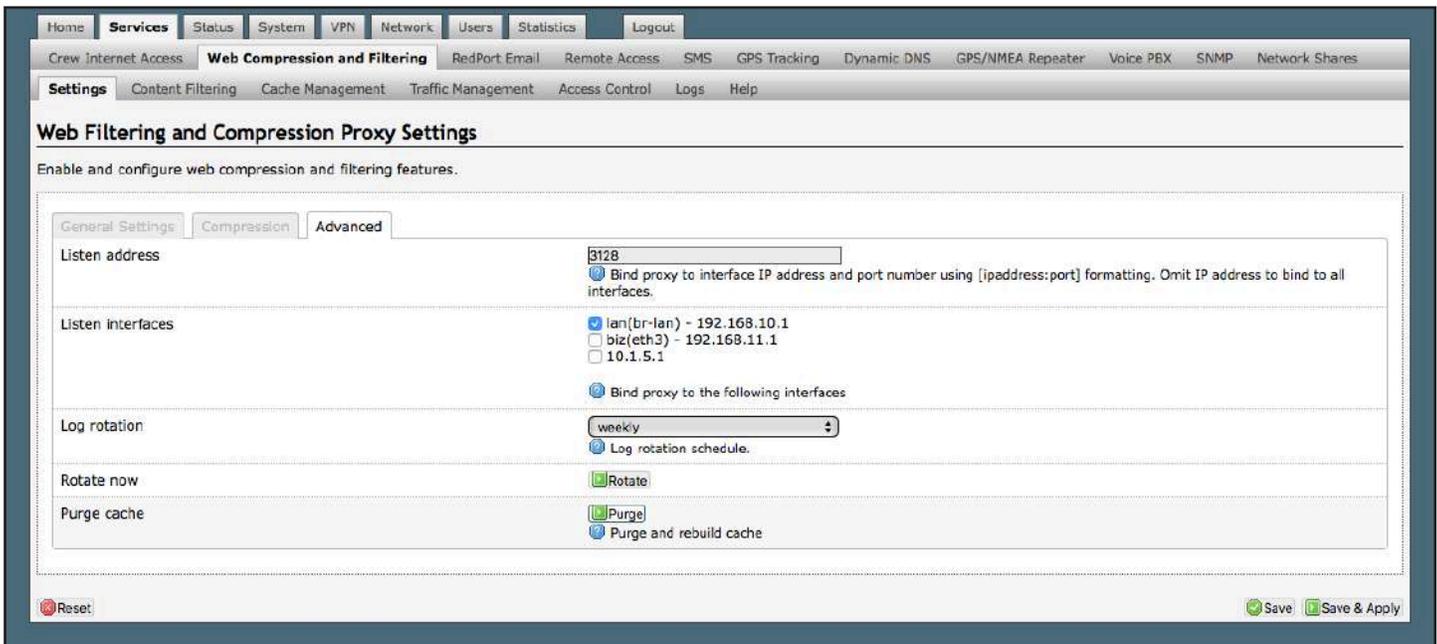
You can still use the internal proxy server and enable transparent proxy to redirect all http traffic for filtering.



5.2.1.3. Advanced Settings

Requires 'superadmin' login.

Under normal operating conditions there is little to change here. See the next page for possible exceptions.



Some items of interest include:

- **Default Filtering Scheme:** This setting affects the amount of content filtering that is applied to a website 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 airtime plans. "Aggressive" has the most impact and is suggested for the best bandwidth utilization. The Aggressive setting blocks YouTube, flash, etc.
- **Debug Level:** The settings here 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 may

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.

5.2.2. Filters (Content Filtering through Diladele)

Requires 'superadmin' login.

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 compression enabled. See next page for details.

Increased Content Filtering is available through a Third-party company, Diladele. This robust pay service provides:

- Web filtering for HTTP and HTTPS traffic.
- Prevention of access to various categories of sites.
- Blockage of explicit content.
- Removal of advertisements.
- Control of downloads.
- Monitoring of traffic.
- Creation of activity reports.

Navigate to <Services> tab, then to <Web Compression and Filtering> tab, then to <Content Filtering>.

Home Services Status System VPN Network Users Statistics Logout

Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares

Settings Content Filtering Cache Management Traffic Management Access Control Logs Help

Web Content Filtering and Logging

Block illegal and potentially malicious file downloads, remove annoying advertisements, prevent access to various categories of web sites and block resources with explicit content.

Features:

- Filter SSL Encrypted HTTPS Web Traffic
- Filter Groups of Users Based on Microsoft Active Directory
- Block Pornography and Explicit (Adult) Contents
- Block File Downloads
- Control Web Usage by Categories
- Remove Annoying Web Ads
- Protect Online Privacy

Enable Enable content filtering

Configure [Configure Content Filtering](#)
[Setup blocking by category, usage reporting, and much more.](#)

Update [Download Now](#)
[Update categories, malware, and ad site database. Note that the update requires connectivity to the Internet.](#)

Caution: Download size is approximately 80MB which may impact your airtime billing.

Automatic Update [Automatically schedule category, malware, and ad site database. Note that the update requires connectivity to the Internet.](#)

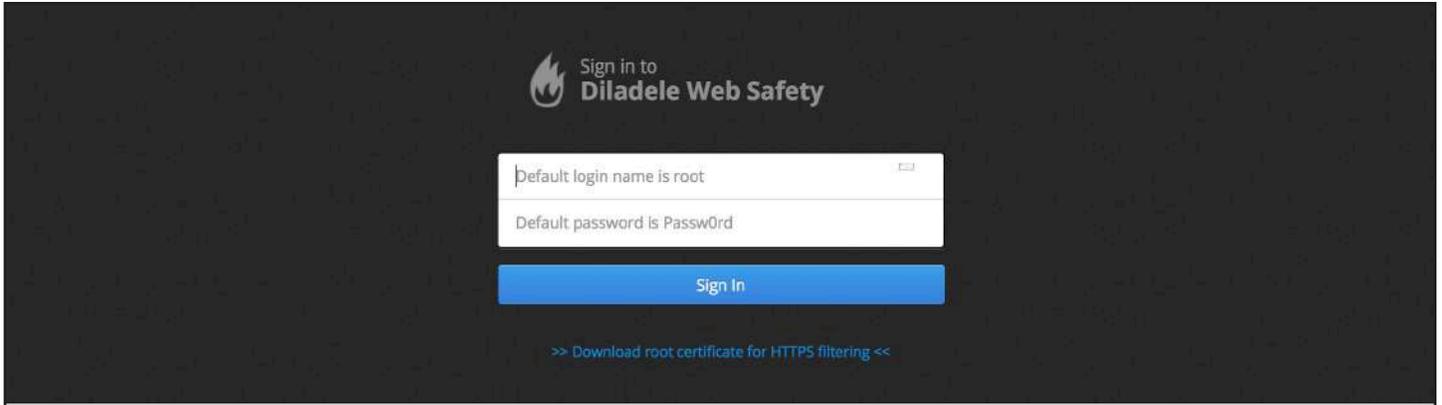
Caution: Download size is approximately 80MB which may impact your airtime billing.

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

Obtain license from RedPort authorized dealers.

Click "Enable content filtering".

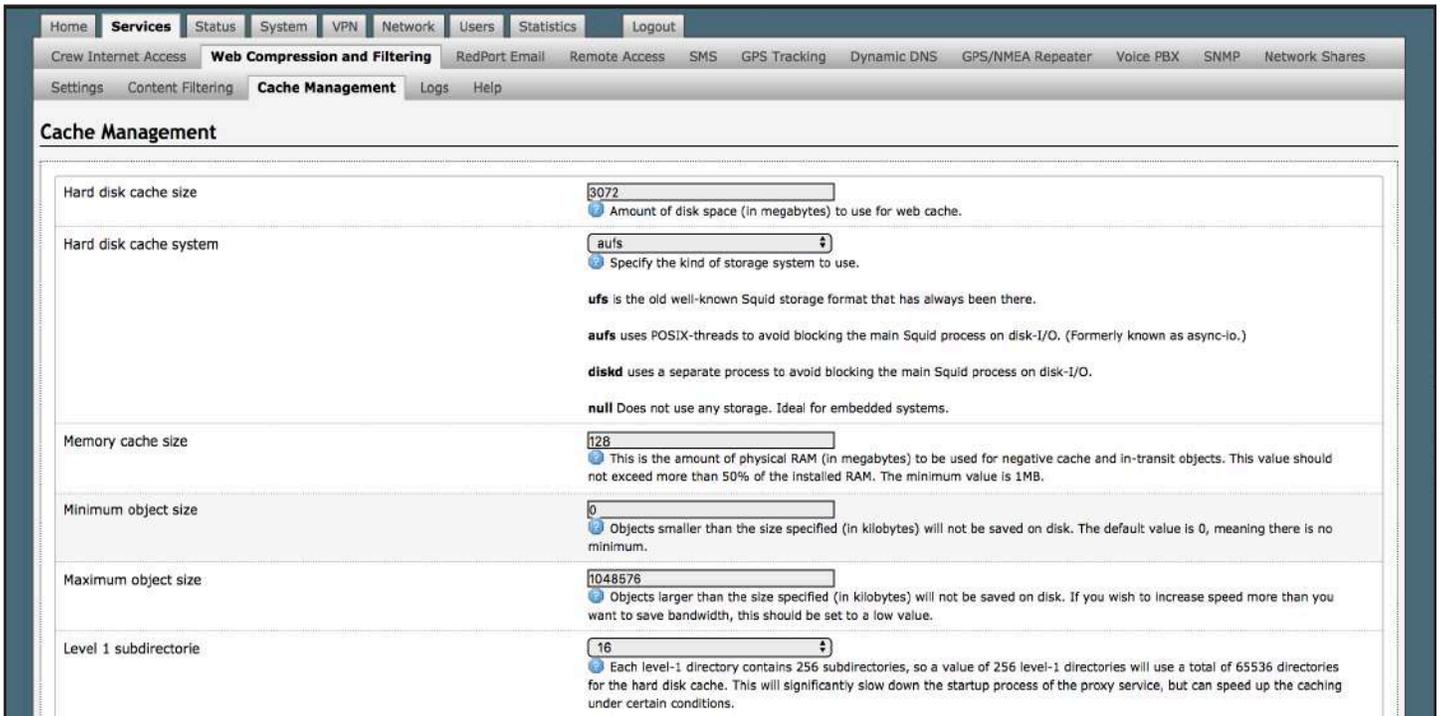
Click "Configure Content Filtering".



Enter Diladele login and password supplied by RedPort authorized dealer.

5.2.3. Cache Management

Requires 'superadmin' login.



Memory replacement policy	<input type="text" value="Heap GDSF"/> <p><input checked="" type="checkbox"/> The memory replacement policy determines which objects are purged from memory when space is needed. The default policy for memory replacement is GDSF.</p> <p>LRU: Last Recently Used Policy - The LRU policies keep recently referenced objects. I.e., it replaces the object that has not been accessed for the longest time.</p> <p>Heap GDSF: Greedy-Dual Size Frequency - The Heap GDSF policy optimizes object-hit rate by keeping smaller, popular objects in cache. It achieves a lower byte hit rate than LFUDA though, since it evicts larger (possibly popular) objects.</p> <p>Heap LFUDA: Least Frequently Used with Dynamic Aging - The Heap LFUDA policy keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate since one large, popular object will prevent many smaller, slightly less popular objects from being cached.</p> <p>Heap LRU: Last Recently Used - Works like LRU, but uses a heap instead.</p> <p>Note: If using the LFUDA replacement policy, the value of Maximum Object Size should be increased above its default of 12KB to maximize the potential byte hit rate improvement of LFUDA.</p>
Cache replacement policy	<input type="text" value="Heap LFUDA"/> <p><input checked="" type="checkbox"/> The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. The default policy for cache replacement is LFUDA. Please see the type descriptions specified in the memory replacement policy for additional detail.</p>
Low-water-mark in %	<input type="text" value="90"/> <p><input checked="" type="checkbox"/> Cache replacement begins when the swap usage is above the low-low-water mark and attempts to maintain utilisation near the low-water-mark.</p>
High-water-mark in %	<input type="text" value="95"/> <p><input checked="" type="checkbox"/> As swap utilisation gets close to the high-water-mark object eviction becomes more aggressive.</p>
Enable offline mode	<input type="checkbox"/> <input checked="" type="checkbox"/> Use off-line content and don't try to validate cached objects. The offline mode gives access to more cached information than the proposed feature would allow (stale cached versions, where the origin server should have been contacted).
Do not cache	<input type="text"/> <p><input checked="" type="checkbox"/> Enter each domain or IP address on a new line that should never be cached.</p>

Reset Save Save & Apply

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

5.2.4. Traffic Management

Requires 'superadmin' login.

The <Traffic Management> tab is available when "Content Filtering" is not enabled.

Home Services Status System VPN Network Users Statistics Logout	
Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares	
Settings Content Filtering Cache Management Traffic Management Access Control Logs Help	
Traffic Management	
Maximum download size	<input type="text" value="0"/> <p><input checked="" type="checkbox"/> Limit the maximum total download size to the size specified here (in kilobytes). Set to 0 to disable.</p>
Maximum upload size	<input type="text" value="0"/> <p><input checked="" type="checkbox"/> Limit the maximum total upload size to the size specified here (in kilobytes). Set to 0 to disable.</p>
Overall bandwidth throttling	<input type="text" value="0"/> <p><input checked="" type="checkbox"/> This value specifies (in kilobytes per second) the bandwidth throttle for downloads. Users will gradually have their download speed increased according to this value. Set to 0 to disable bandwidth throttling.</p>
Per-host throttling	<input type="text" value="0"/> <p><input checked="" type="checkbox"/> This value specifies (in kilobytes per second) the download throttling per host. Set to 0 to disable this.</p>
Throttle only specific extensions	<input type="checkbox"/> <input checked="" type="checkbox"/> Check this to enable throttling by extension type. Leave unchecked to throttle all downloads/uploads by host or network.
Finish transfer if less than X KB remaining	<input type="text" value="0"/> <p><input checked="" type="checkbox"/> Retrieval will be completed if the browser connection is closed and the transfer has less than X kilobytes remaining. Set to 0 to abort the transfer immediately.</p>
Abort transfer if more than X KB remaining	<input type="text" value="0"/> <p><input checked="" type="checkbox"/> Retrieval will be aborted if browser connection is closed and the transfer has more than X kilobytes remaining. Set to 0 to abort the transfer immediately.</p>
Finish transfer if more than X % finished	<input type="text" value="0"/> <p><input checked="" type="checkbox"/> Retrieval will be completed if browser connection is closed and the transfer has less than X % remaining. Set to 0 to abort the transfer immediately.</p>

Reset Save Save & Apply

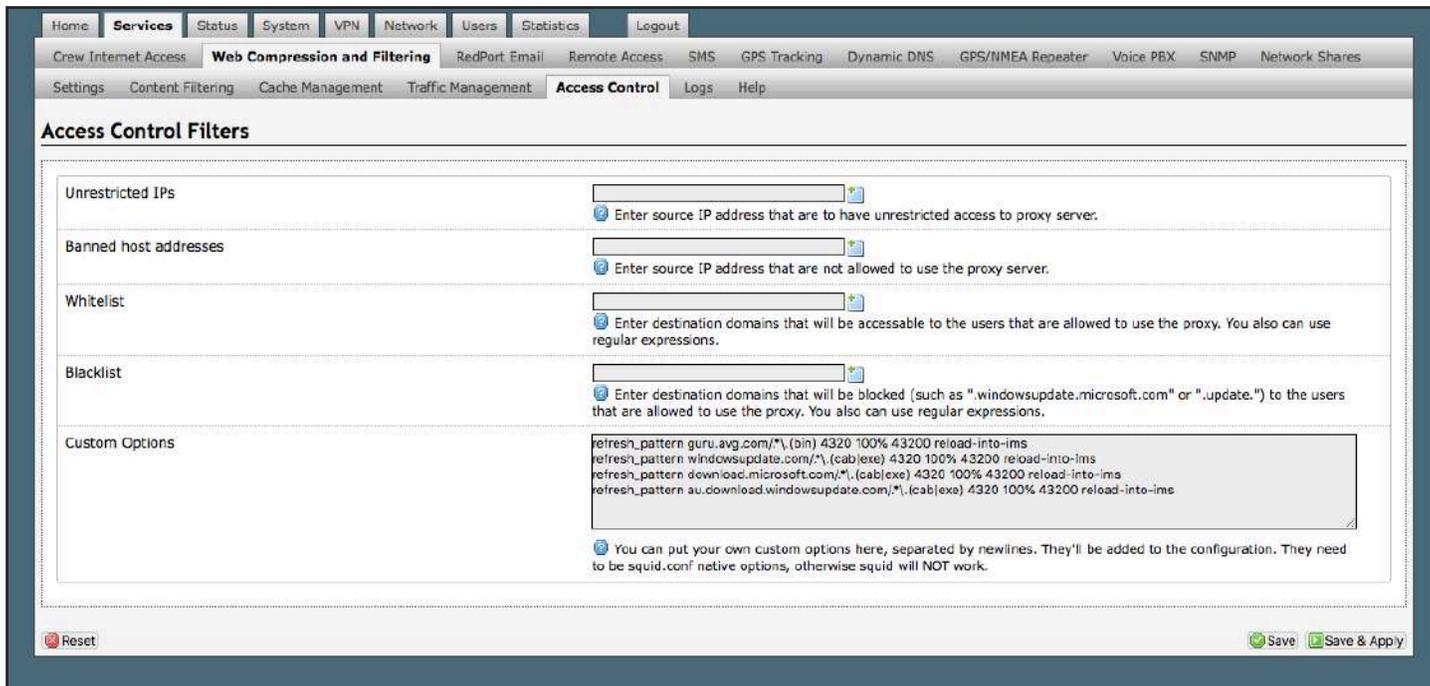
Traffic Management allows you to oversee:

- Maximum download and upload sizes.
- Throttling parameters.
- Transfer restrictions.

5.2.5. Access Control

Requires 'superadmin' login.

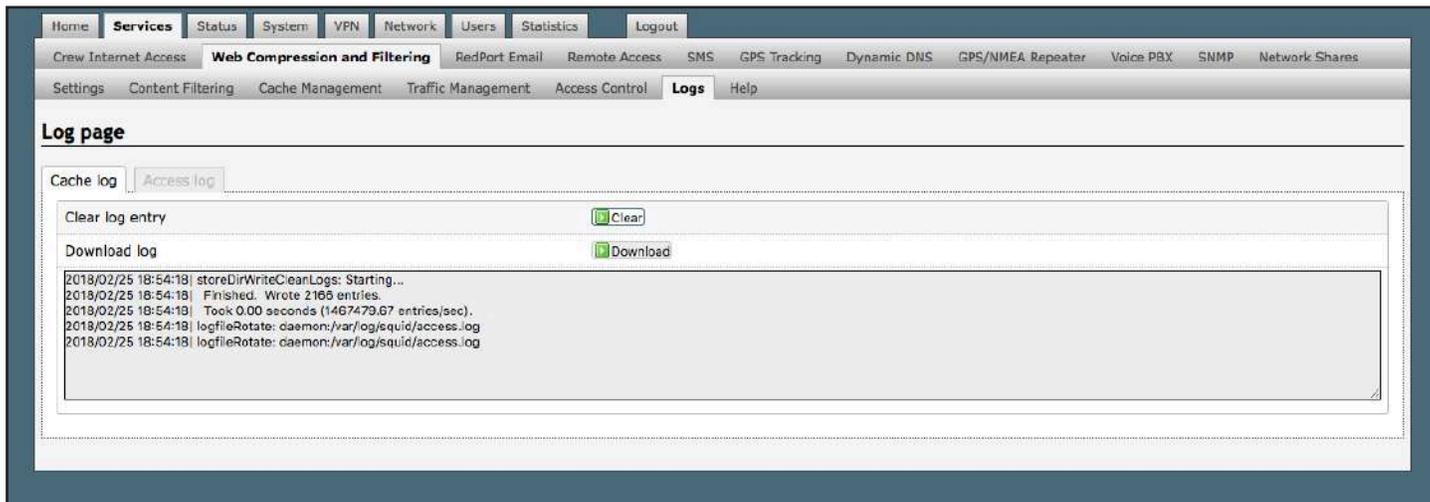
The <Access Control> tab is available when "Content Filtering" is not enabled.



5.2.6. Logs

Requires 'superadmin' login.

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 [Chapter 5.2.7](#)).



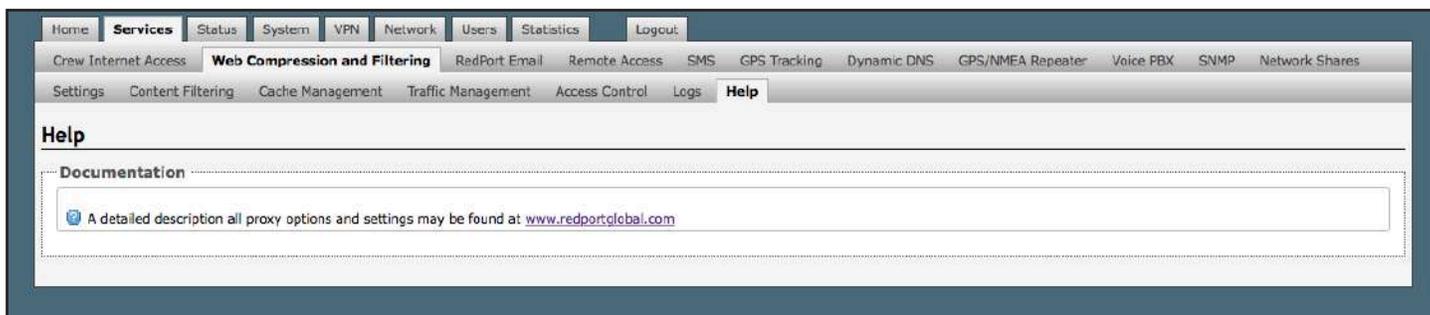
Log files are kept in RAM and are rotated weekly, by default. You can change the Log Rotation schedule in Web Compression and Filtering > Settings > Advanced > Log Rotation.

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

5.2.7. Help

Requires 'superadmin' login.

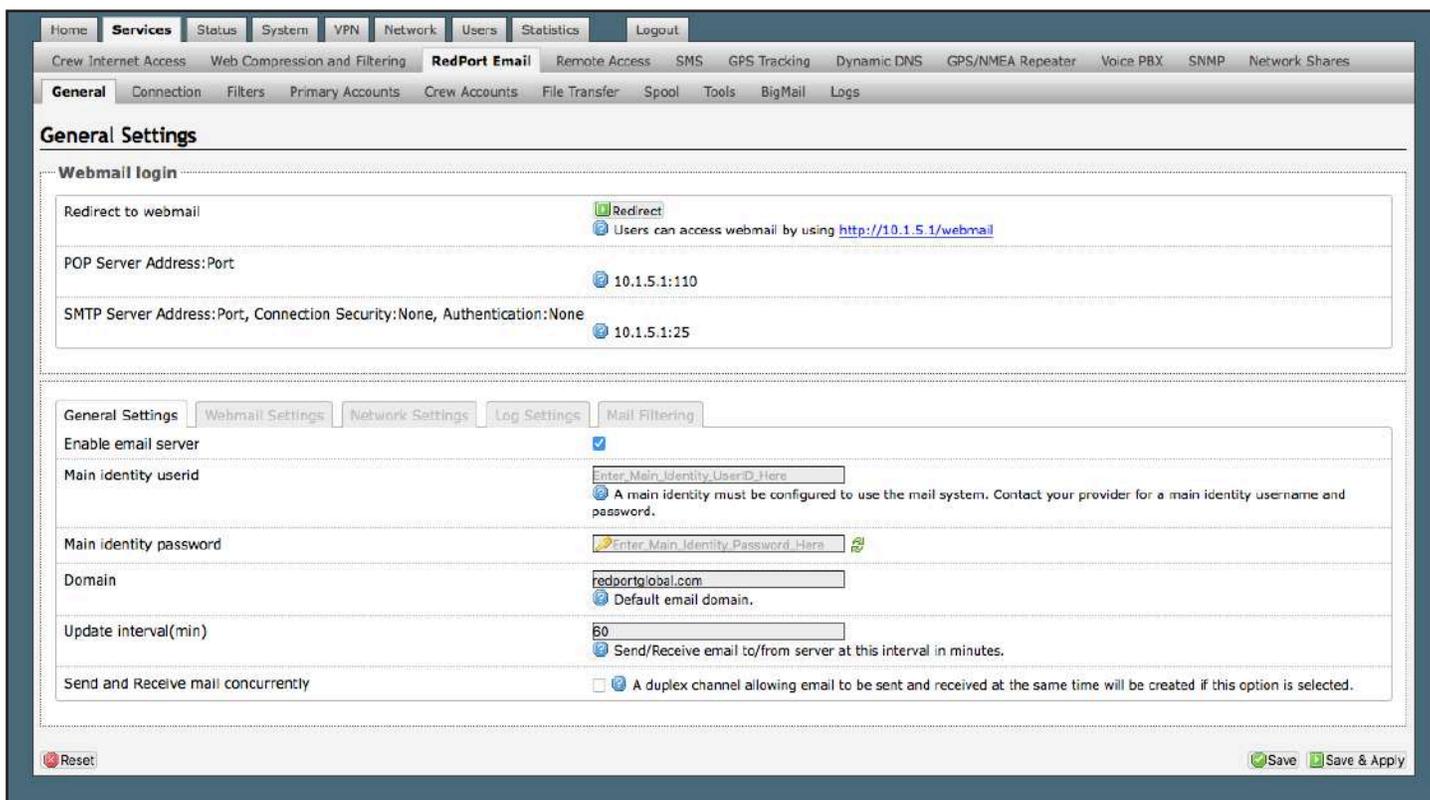
For your convenience the Help page includes a link to the RedPort Global website.



5.3. RedPort Email

Requires 'superadmin' login.

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.



Once enabled, the onsite administrator can manage email for the entire crew. The users can log in to a webmail program to view their email, so they do not need special software on their computer or device. The Optimizer Enterprise 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.

5.3.1. Enable and Configure RedPort Email

Requires 'superadmin' login.

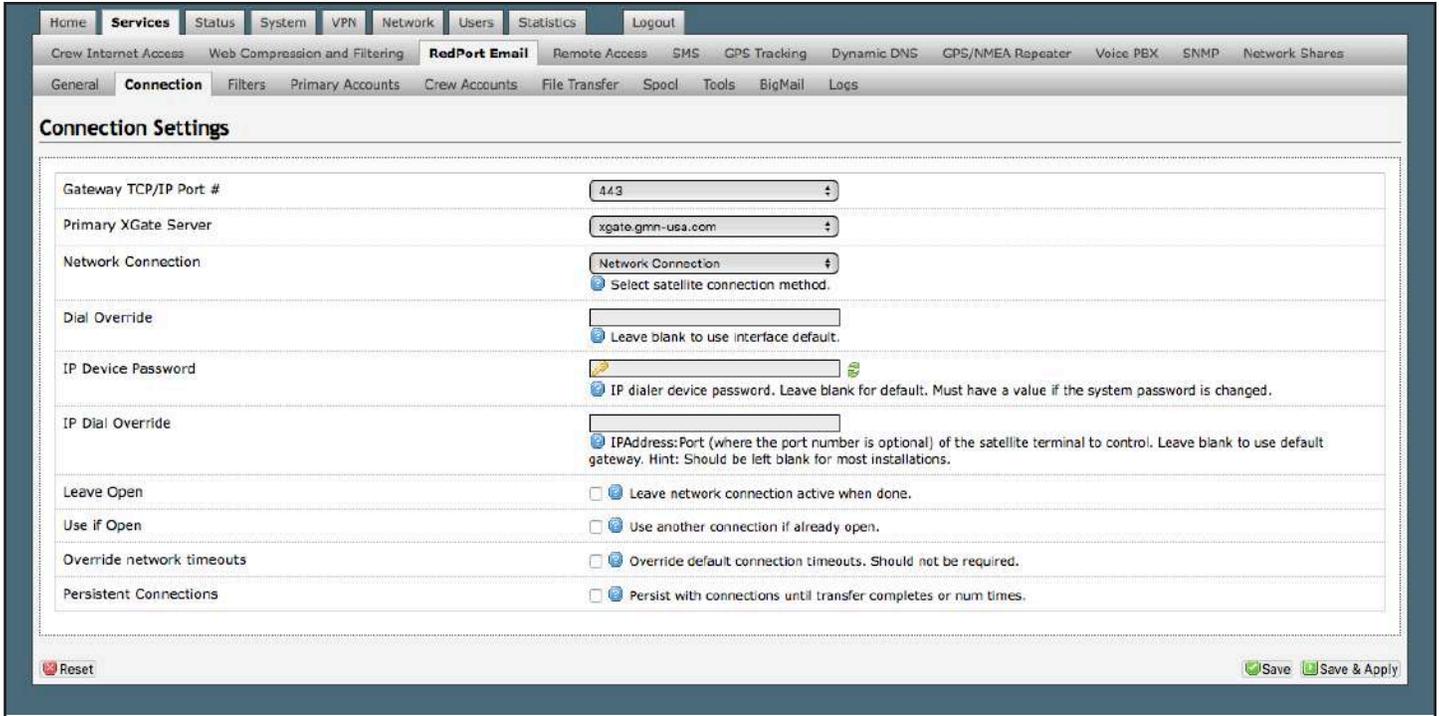
In the RedPort Email General Settings:

The screenshot shows the 'General Settings' tab for RedPort Email. The 'Enable email server' checkbox is checked. The 'Main identity userid' field contains a placeholder 'Enter Main Identity UserID Here' with a help icon and a note: 'A main identity must be configured to use the mail system. Contact your provider for a main identity username and password.' The 'Main identity password' field contains a placeholder 'Enter Main Identity Password Here' with a help icon and a green checkmark. The 'Domain' field contains 'redportglobal.com' with a help icon and a note: 'Default email domain.' The 'Update interval(min)' field contains '60' with a help icon and a note: 'Send/Receive email to/from server at this interval in minutes.' The 'Send and Receive mail concurrently' checkbox is unchecked with a help icon and a note: 'A duplex channel allowing email to be sent and received at the same time will be created if this option is selected.'

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 log in 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 Appendix A of the RedPort Email Guide for information on email block compression and its impact on Update intervals).
5. Click <Save>.

NOTE: Typically, 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 **Chapter 5.3.2** for more information regarding primary accounts.

6. Go to the Connection tab:



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. Click <Save & Apply> to apply the change.

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

5.3.2. Primary Accounts

Requires 'superadmin' login.

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/RedPort 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 Optimizer RedPort Email Guide for details).
- Inbound Mail Filter (See **Chapter 7.0** of the Optimizer RedPort Email Guide for details).
- Outbound Mail Filter (See **Chapter 7.0** of the Optimizer 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.

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

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

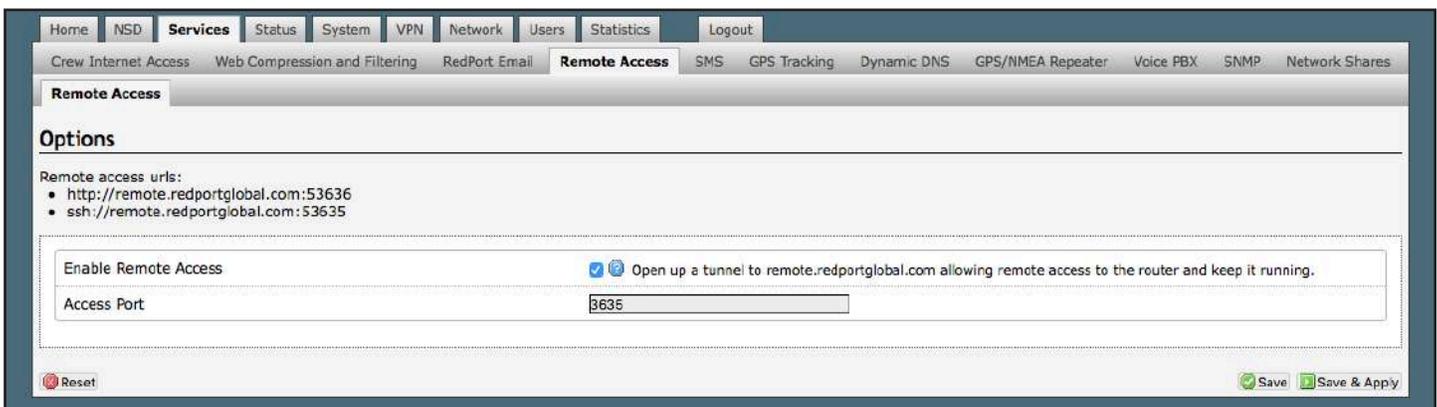
Please see the Optimizer RedPort Email Guide for comprehensive information on the use of RedPort Email service.

5.4. Remote Access

Requires 'superadmin' login.

Used to permit Remote Access to the router UI. Access permits technical support members the ability to log into the router from the Internet.

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



Remote login from the <Services> tab sets up a persistent access that will remain available until disabled.

Click “Enable Remote Access”. Remote access URLs will be presented. The URLs can be utilized by the customer or passed to technical support members to allow access to the router.

The screenshot displays the RedPort web interface with a navigation menu at the top containing: Home, NSD, Services, Status, System, VPN, Network, Users, Statistics, and Logout. Below the menu, there are sub-tabs for Tasks, Traffic Routing, and MWAN Overview. The main content area is divided into several sections:

- Welcome**: A section with a heading "Crew Internet Services - DISABLED" and a button labeled "Enable Crew Internet".
- Email Access**: A section titled "Email Access" with sub-heading "Email access settings and parameters:" and a list of settings: WEB - <http://127.0.0.1/webmail>, POP - 127.0.0.1:110, and SMTP - 127.0.0.1:25 with no connection or authentication security. A button labeled "Go to webmail" is present.
- Email Management**: A section with four buttons: "Create and manage crew email accounts", "Retrieve, delete, or drop large emails (BigMail) quarantined on the server", "Perform common email tasks", and "View email logs".
- System Status**: A section with four buttons: "System status overview", "Realtime bandwidth usage over satellite link", "Historic bandwidth usage over satellite link", and "System message log".
- Local WiFi setup**: A section with sub-heading "SSID and Security" and two buttons: "WiFi setup" and "Change hotspot name and/or add security and set password".
- Remote Support**: A section with sub-heading "Remote access uris:" and a list of URIs: <http://remote.redportglobal.com:53636> and <ssh://remote.redportglobal.com:53635>. Two buttons are present: "Disable Remote Support" and "Terminate remote support".
- System**: A section with two buttons: "Router password" and "Reboot router".

Optionally, temporary Remote Access can also be given through the <Home> tab.

This access will automatically be disabled when the router is rebooted. The access can also be disabled by clicking <Disable Remote Support>.

5.5. SMS Messaging

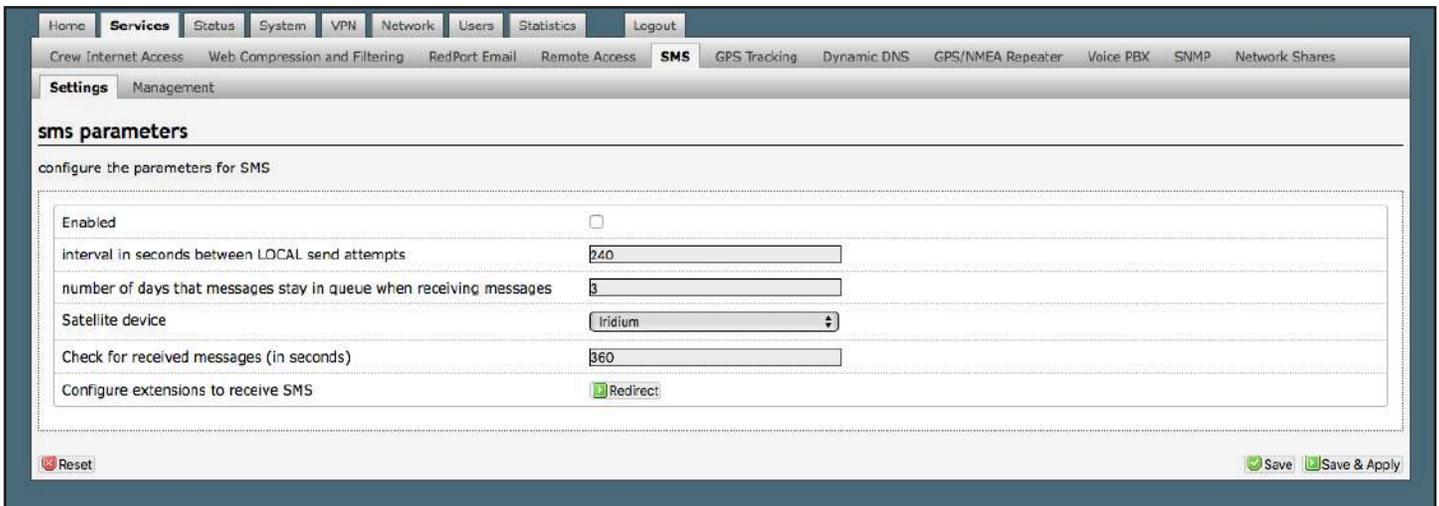
Requires 'superadmin' login.

If using a compatible satellite device, it is possible to send and receive SMS messages directly from the Optimizer Enterprise router and to route incoming SMS messages to one or more smartphones connected to the local wireless network.

5.5.1. SMS Settings

Requires 'superadmin' login.

Use Settings to enable and configure the SMS parameters.



1. Click the checkbox to enable SMS.
2. Click the appropriate Satellite device from the drop-down menu.

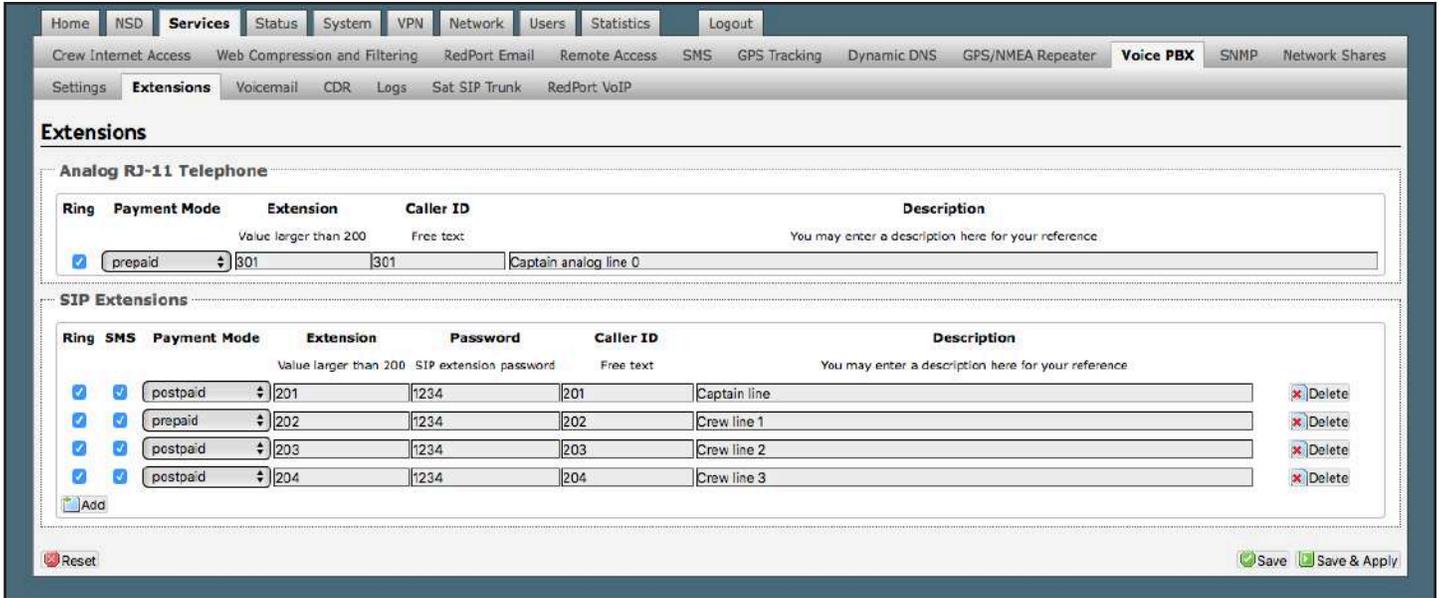


3. Click <Save & Apply>.

5.5.2. Configure SIP Extensions to Receive SMS Messages

Requires 'superadmin' login.

With SMS enabled, click <Redirect> (see SMS Settings screen above) to configure which extensions are to receive incoming SMS messages.



To enable an extension to receive SMS messages, use the checkbox in the SMS column. For more information on configuring SIP Extensions **See Chapter 5.5.**

5.5.3. 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 Play store for Android devices.

Using the smartphone or tablet Settings, connect to the Optimizer Enterprise wireless network 'wxa-524-xxxx'.



Open the XGate Phone App. Click <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.

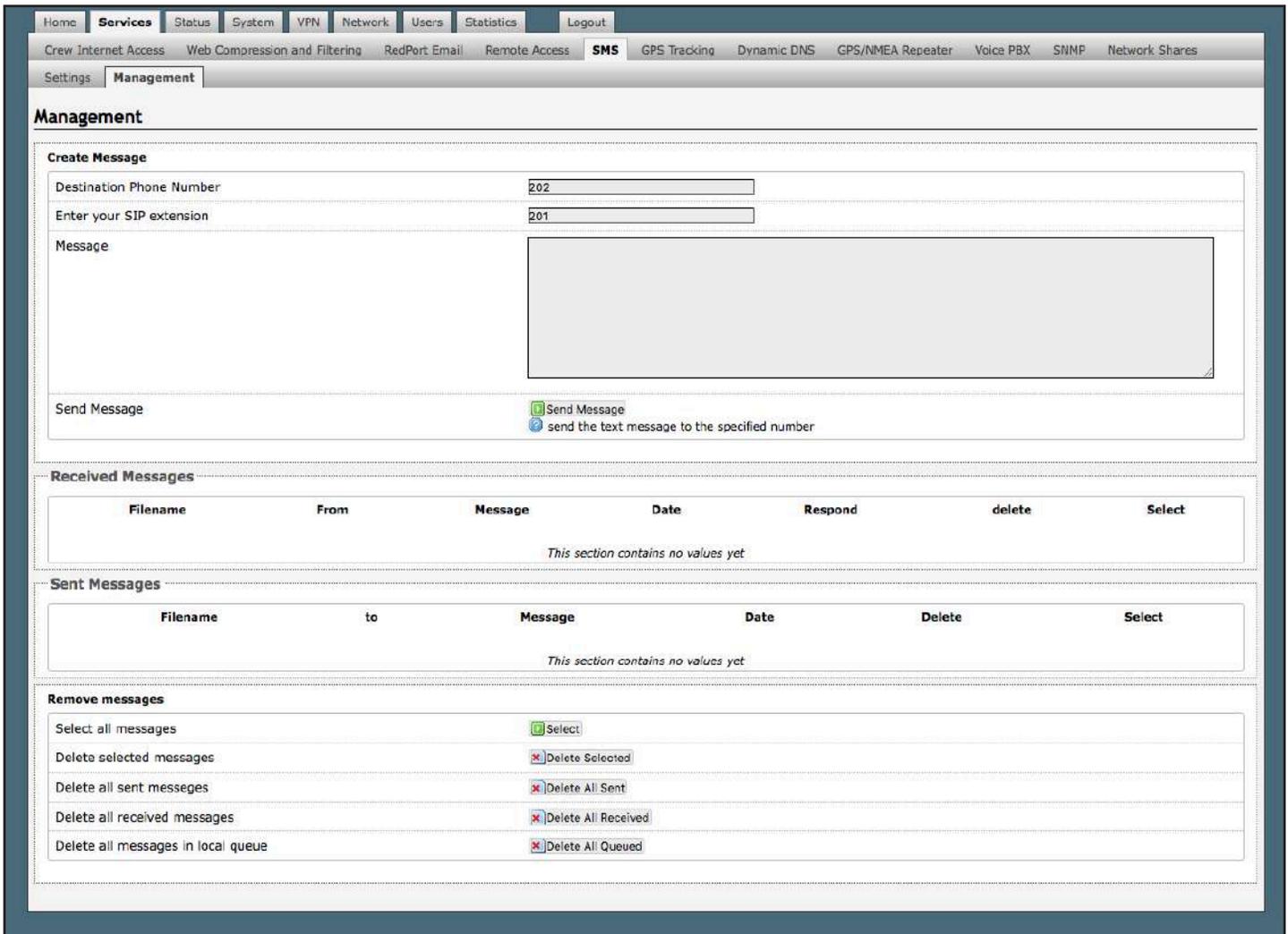
Multi-user Voice and SMS is possible with the optional RedPort VoIP service. Contact your service provider for

details.

5.5.4. SMS Management

Requires 'superadmin' login.

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



Home Services Status System VPN Network Users Statistics Logout

Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares

Settings Management

Management

Create Message

Destination Phone Number

Enter your SIP extension

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

Delete selected messages

Delete all sent messages

Delete all received messages

Delete all messages in local queue

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

5.6. GPS Tracking

Requires 'superadmin' login.

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.

5.6.1. Tracking powered by RedPort with GSatTrack

Requires 'superadmin' login.

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.

Home Services Status System VPN Network Users Statistics Logout

Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS **GPS Tracking** Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares

Tracking

Tracking Parameters

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

General Tracking Parameters

Enable Tracking

Tracking Interval 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: 2891346999902.

Globalstar phone A valid NMEA/GPS feed is required. Tracking IMEI: 2891346999902.

Iridium terminal/Aurora/MCG-101 A valid NMEA/GPS feed is required.

Tracking via SMS

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

INMARSAT Isatphone

Iridium terminal/Aurora/MCG-101 A valid NMEA/GPS feed is required.

Recipient Email Address Enter a valid email address. Also used for SOS messages.

Vessel name Enter optional vessel name and/or other free text.

Reset Save Save & Apply

1. Enable Tracking by clicking the checkbox.
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 position report. Adjust the Tracking Interval to meet your needs.
3. Go to Tracking powered by RedPort and select the satellite terminal you are using.

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

Tracking powered by RedPort

Please visit www.RedPortGlobal.com for registration information

INMARSAT FleetBroadband	<input type="checkbox"/>
Iridium OpenPort/Pilot	<input type="checkbox"/>
INMARSAT Isatphone	<input type="checkbox"/>
VSAT or broadband satellite	<input type="checkbox"/> A valid NMEA/GPS feed is required. Tracking IMEI: 626083925968886.
Globalstar phone	<input type="checkbox"/> A valid NMEA/GPS feed is required. Tracking IMEI: 626083925968886.
Iridium terminal/Aurora/MCG-101	<input type="checkbox"/> A valid NMEA/GPS feed is required.

4. Click <Save & Apply>.

5.6.2. Tracking via SMS

Requires 'superadmin' login.

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	<input type="checkbox"/>
Tracking Interval	<input type="text" value="60"/> Specify the tracking interval in minutes.

-- / --

Tracking via SMS

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

INMARSAT Isatphone	<input type="checkbox"/>
Iridium terminal/Aurora/MCG-101	<input type="checkbox"/> A valid NMEA/GPS feed is required.
Recipient Email Address	<input type="text" value="user@domain.com"/> Enter a valid email address. Also used for SOS messages.
Vessel name	<input type="text"/> Enter optional vessel name and/or other free text.

1. Enable Tracking by clicking the checkbox.

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 position report. Adjust the Tracking Interval to meet your needs.

3. Go to Tracking via SMS and 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 1.

5. Click <Save & Apply>.

5.7. GPS/NMEA Repeater

Requires 'superadmin' login.

The Optimizer Enterprise 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 Enterprise 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.

5.7.1. Equipment Setup

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

5.7.1.1. 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 Optimizer Enterprise with an appropriate USB to NMEA device cable as indicated by the NMEA device manufacturer.

CAUTION: It is not recommended to have a USB Satphone and LTE/GSM modem connected at the same time via a USB Hub. It may create conflicts.



The Optimizer Enterprise 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.

5.7.1.2. 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 a PL- 2302HX or a FTDI Chip USB to serial adapter as noted above.



5.7.1.3. 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.



5.7.2. Dynamic DNS

Requires 'superadmin' login.

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Hints

[Show more](#) Follow this link
You will find more hints to optimize your system to run DDNS scripts with all options

Overview

Below is a list of configured DDNS configurations and their current state.
If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'
[To change global settings click here](#)

Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
myddns_ipv4	yourhost.example.com No data	<input type="checkbox"/>	Never Disabled	<input type="button" value="Start"/>	Edit Delete
myddns_ipv6	yourhost.example.com No data	<input type="checkbox"/>	Never Disabled	<input type="button" value="Start"/>	Edit Delete

5.7.3. 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 Enterprise User Interface.

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

Repeater Parameters

Enable Enable GPS monitoring and repeating.

Binary Mode Pass raw binary data through without parsing for NMEA-183 sentences.

GPS/NMEA feed from USB Use USB connected GPS or NMEA feed as a source.
Note: Not compatible with RS-232 based satellite phones.

UDP Listener Port
 Listen on UDP port number and rebroadcast.

UDP Port
 Broadcast to UDP port number.

TCP Port
 Broadcast to TCP port number.

1. Enable - Click this checkbox to Enable GPS monitoring and repeating.
2. GPS/NMEA feed from USB - Select this when connecting a GPS or NMEA device via USB cable.
3. NMEA Baud Rate - 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.
4. UDP Listener Port - Enter the UDP port number that the GPS is connected to. The default is set to the standard UDP Listener Port for NMEA 183 devices of 10101.

5. UDP Port - Enter the UDP port number to broadcast the GPS data to. The default is set to the standard UDP Port for NMEA 183 devices of 11101.

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

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

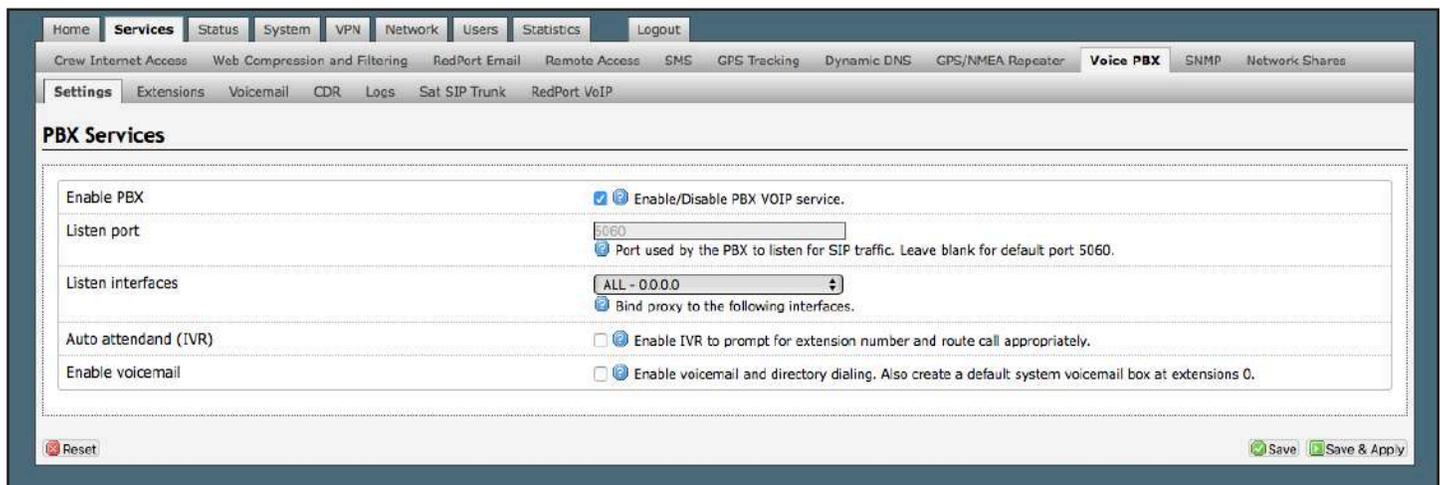
Configure the destination software to match this port number; or, change this entry to match the requirements of the destination software.

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.

To use the GPS Repeater feature, your computer must be connected to the Optimizer's WiFi network or directly connected to one of the Optimizer's Ethernet ports (i.e. the BIZ port and the WAN ports, by default, are open). Any port that is configured to go through the Captive Portal will not work with the GPS/NMEA Repeater feature.

5.8. VOICE PBX

Requires 'superadmin' login.



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

- Sailor FBB terminal - requires XGate Phone app*. (See **Chapter 5.8.5**).
- IsatHub iSavi - requires IsatHub Control app and either IsatHub Voice app or XGate Phone app*. (See Optimizer Voice iSavi Addendum for information on how to pair the iSavi with the Optimizer Enterprise).
- Any satellite terminal with a RJ-11 port - requires XGate Phone app* AND an ATA adapter. (We support the Grandstream HT701 and the Cisco SPA 112).

This configuration allows one voice call or 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 5.8.6**.

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

- FBB.
- BGAN.

- VSAT.
- RedPort Aurora.
- Iridium Pilot.
- Thuraya IP.
- IsatHub iSavi.

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

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

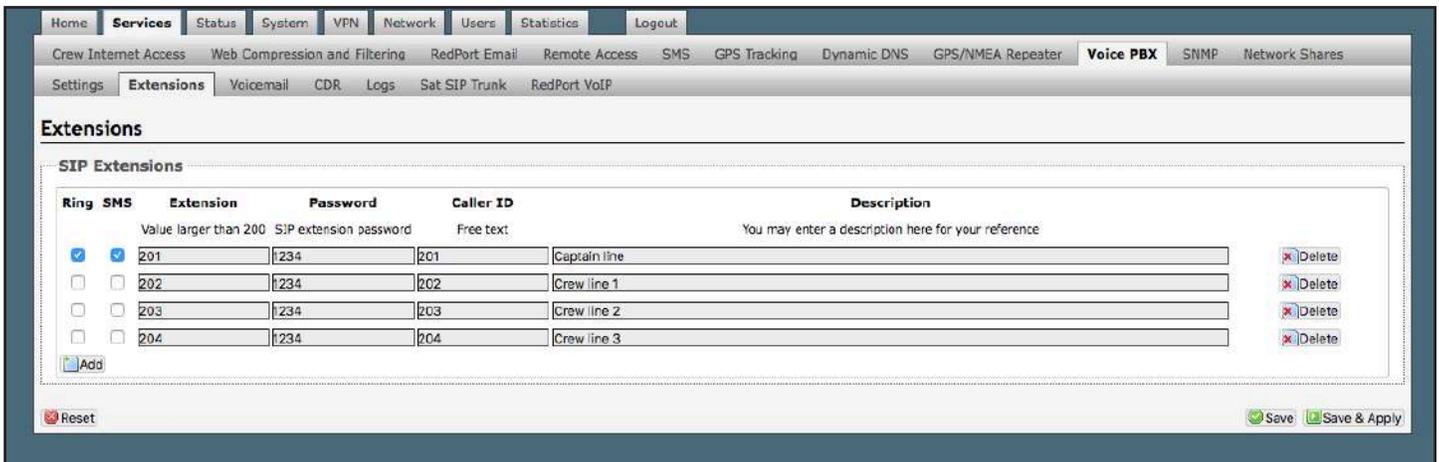
5.8.1. Setup Extensions

Requires 'superadmin' login.

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 on those extensions with Ring enabled.

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



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 Play store 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.

5.8.1.1. How to Make/Receive Voice Calls

Using the smartphone or tablet Settings, connect to the Optimizer wireless network 'wxa-524- xxxx'.

Open the XGate Phone App to make and receive calls.

NOTE: Standard voice calling rates apply.

Only one phone call can be active at a time. (Multi-user Voice and SMS is possible -- up to four consecutive sessions -- with the optional RedPort VoIP service. Contact your service provider for details. **See Chapter 5.8)**

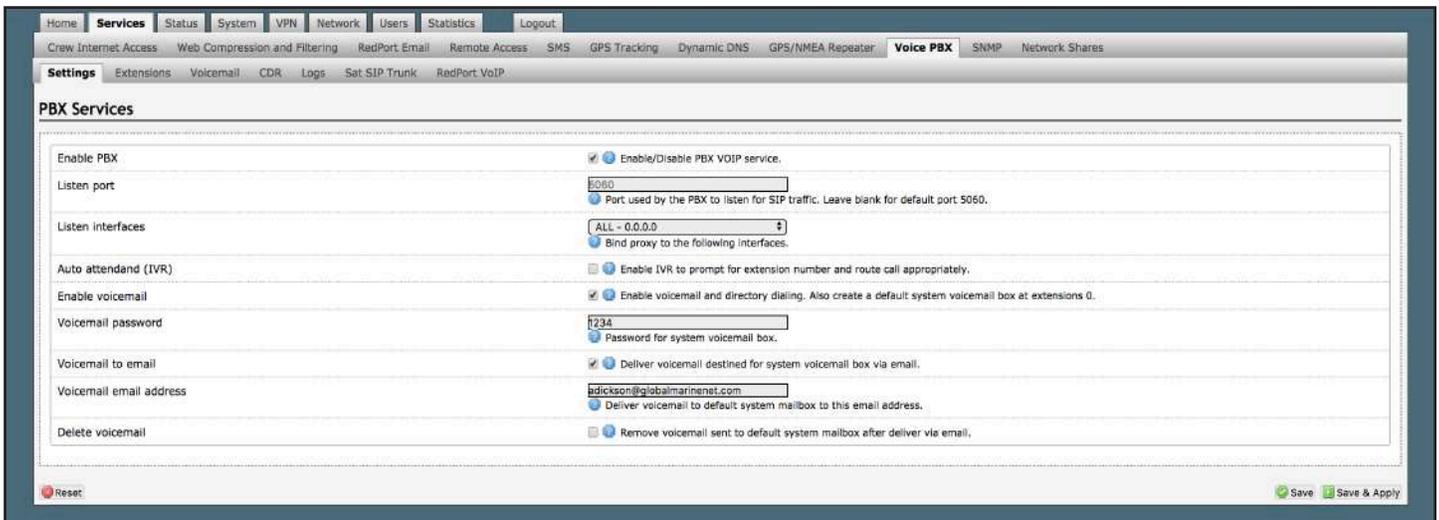


NOTE: Inmarsat IsatHub (iSavi) users. Please see redportglobal.com for the iSavi Quick Start Guide containing information and instructions for setup and use of the Optimizer with the iSavi terminal for voice calls and SMS messaging.

5.8.2. Voicemail

Requires 'superadmin' login.

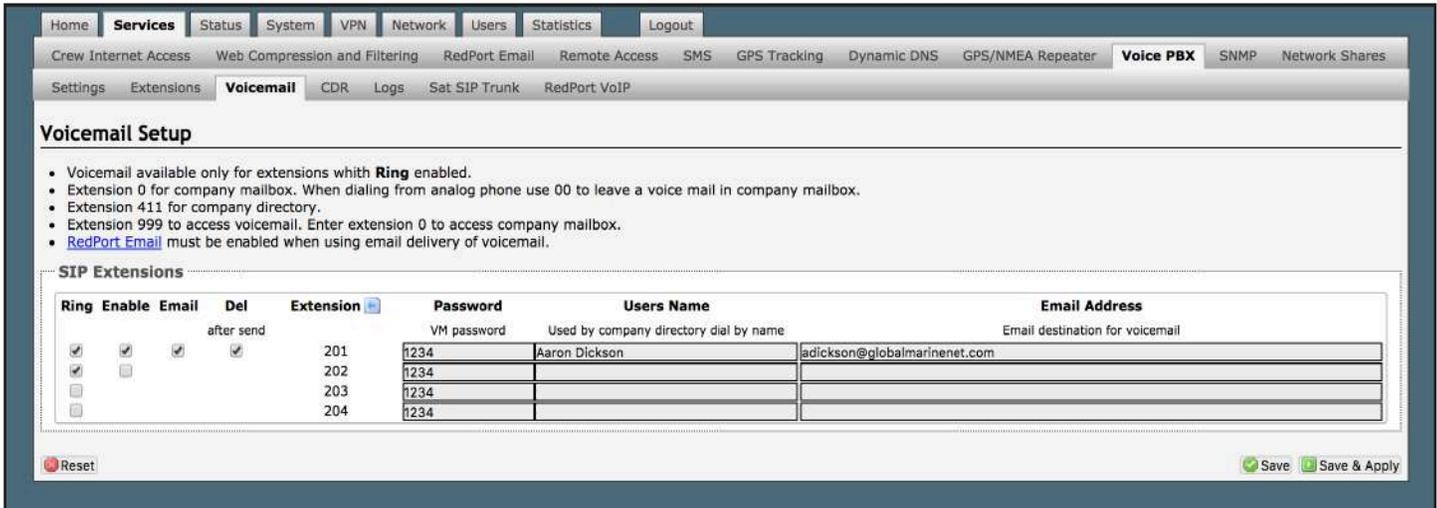
Voicemail options will only be available if Voicemail is enabled on <Services> tab, then <Voice PBX>, and then <Settings> tab:



- Click "Enable voicemail and directory dialing".

- Modify Voicemail password if desired.
- If desired, click “Deliver voicemail destined for system voicemail box via email”.
- Enter desired email address for voicemail message forwarding.
- If desired, click “Delete voicemail sent to default system mailbox after deliver via email”.
- Click <Save & Apply>.

Navigate to <Services> tab, then to <Voice PBX> tab, and then to <Voicemail> tab:



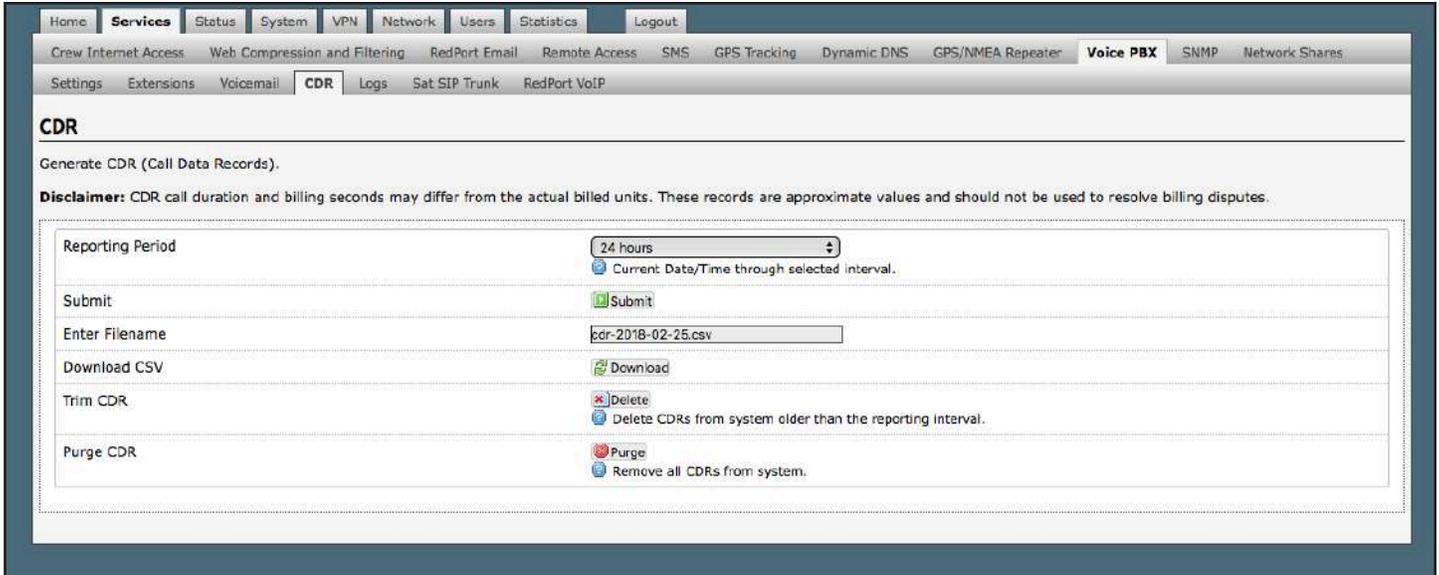
To set up Voicemail:

- Click Ring.
- Click Enable.
- Click Email if desired - to enable delivery of voicemail to email.
- Click Del (delete) if desired - to delete the voicemail from the system after being sent to email.
- Fill in desired Password - will be entered when retrieving voicemails via phone.
- Fill in desired Users Name - will allow user name system search via phone system.
- Fill in desired Email Address - required to permit system to email voicemails.
- Click <Save & Apply>.

5.8.3. 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.



On active systems, the call data records can quickly use up memory. It is recommended that you periodically Trim CDR or Purge CDR records from the system.

5.8.4. Logs

Requires 'superadmin' login.

This screen provides PBX status information and some management.

Logs and Status

Active Calls

Hangup all calls

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

Vobal Decoder

Decoder is disabled. Please contact your provider for an activation code should you wish to enable the service.

PBX Status

Restart PBX

SIP Status

Name/Username	Host	Dyn	Forcerport	Comedia	ACL Port	Status	Description
100	(Unspecified)	D	Auto (No)	No	0	UNKNOWN	
101	(Unspecified)	D	Auto (No)	No	0	UNKNOWN	
201	(Unspecified)	D	Auto (No)	No	0	UNKNOWN	
202	(Unspecified)	D	Auto (No)	No	0	UNKNOWN	
203	(Unspecified)	D	Auto (No)	No	0	UNKNOWN	
204	(Unspecified)	D	Auto (No)	No	0	UNKNOWN	

6 sip peers [Monitored: 0 online, 6 offline Unmonitored: 0 online, 0 offline]

Log

Clear log entry

Download log

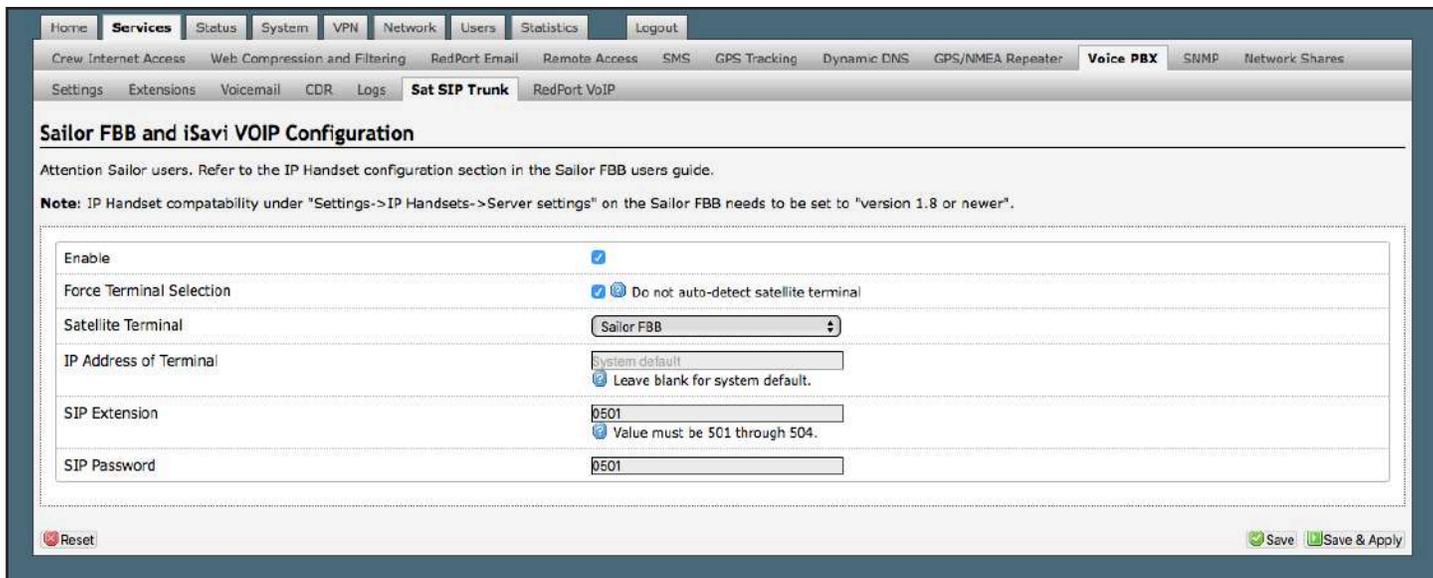
```
[Apr 16 14:14:02] Asterisk 11.12.0 built by lsoltero @ ubuntu on a x86_64 running Linux on 2018-04-10 18:46:46 UTC
[Apr 16 14:14:02] NOTICE[14012] cdr.c: CDR simple logging enabled.
[Apr 16 14:14:02] WARNING[14012] cel.c: Could not load cel.conf
[Apr 16 14:14:02] NOTICE[14012] loader.c: 48 modules will be loaded.
[Apr 16 14:14:02] WARNING[14012] loader.c: Error loading module 'res_musiconhold.so': File not found
[Apr 16 14:14:02] NOTICE[14012] res_smdi.c: Unable to load config smdi.conf: SMDI disabled
[Apr 16 14:14:02] NOTICE[14012] res_smdi.c: No SMDI interfaces are available to listen on, not starting SMDI listener.
[Apr 16 14:14:02] WARNING[14012] loader.c: Error loading module 'res_musiconhold.so': File not found
```

- **Active Calls:** Displays all active channels in use. Click <Hangup> to immediately hang up all active calls.
- **Vobal Decoder:** Displays the VoIP Activation Key when RedPort VoIP service is enabled. **See Chapter 5.8.6.**
- **PBX Status:** Displays the current status of all SIP extensions. Click <Restart> to reboot the PBX service.
- **Log:** Displays the current Log of PBX usage. Click <Clear> to remove the log content. Click <Download> to Open or Save the PBX Log.

5.8.5. 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.



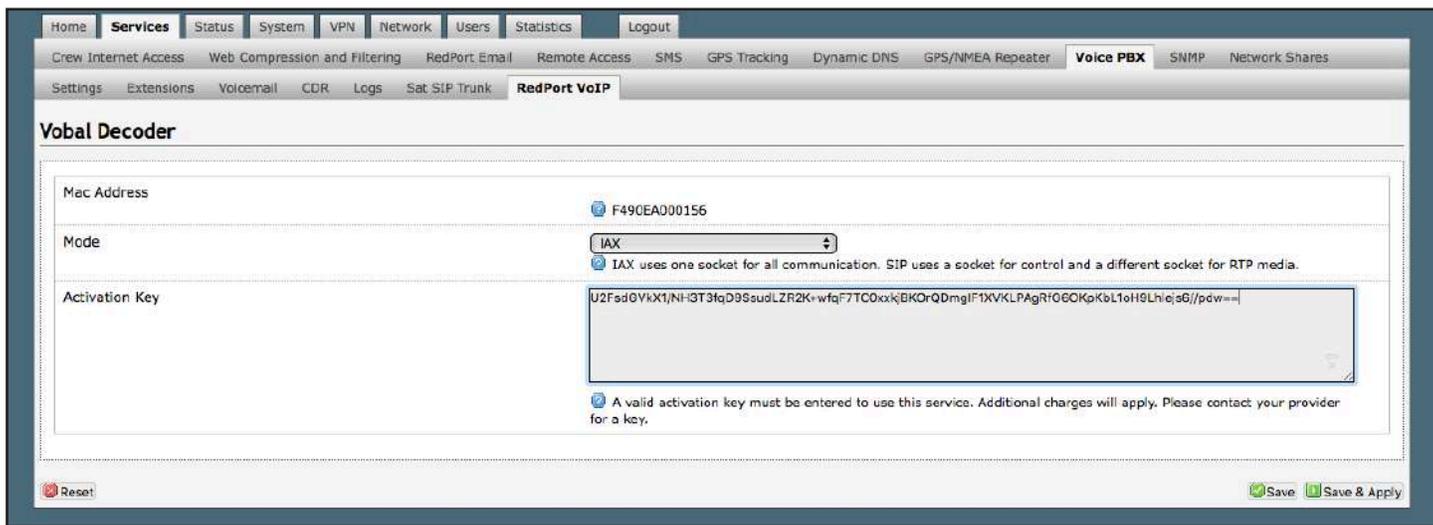
NOTE: You may need to edit the IP Handset configuration in the Sailor FBB user interface. Settings > IP Handsets > Server Settings on the Sailor FBB must be set to version 1.8 or newer. (Refer to the Sailor FBB users guide for how to access the Sailor FBB Settings).

5.8.6. RedPort VoIP Activation

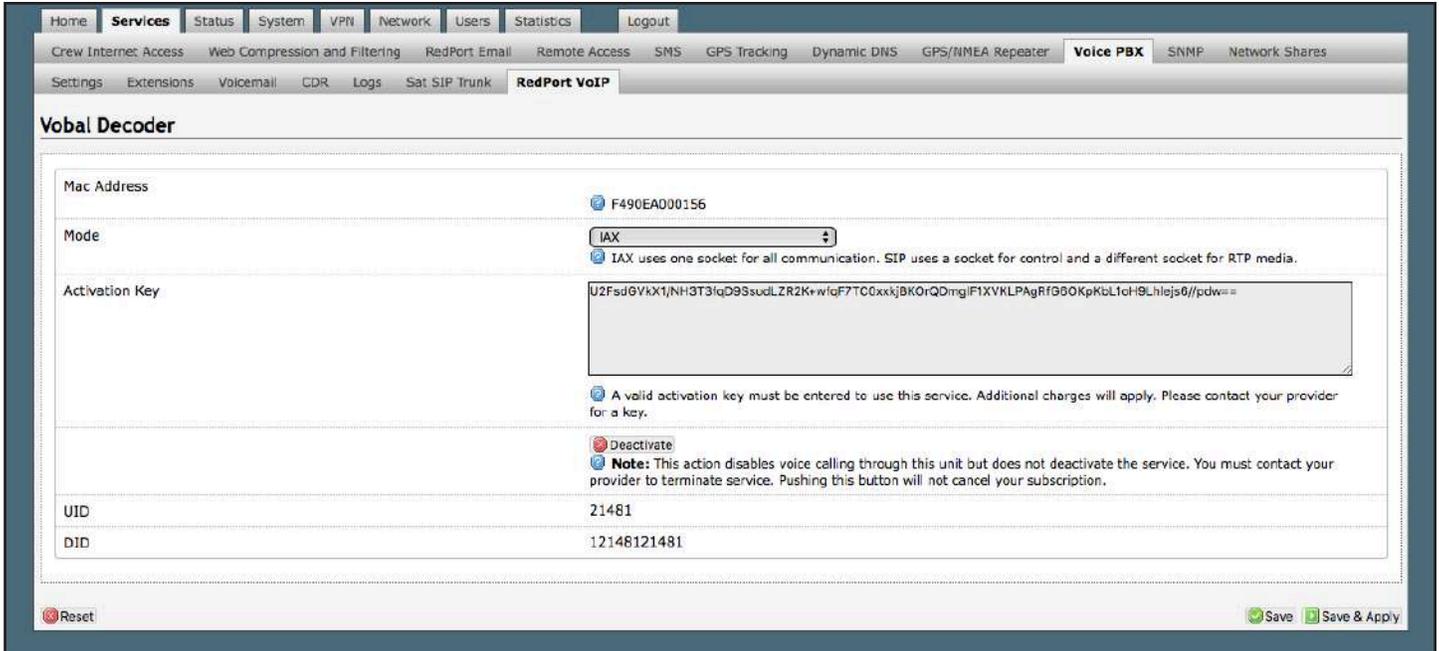
Requires 'superadmin' login.

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 regular 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 user interface.

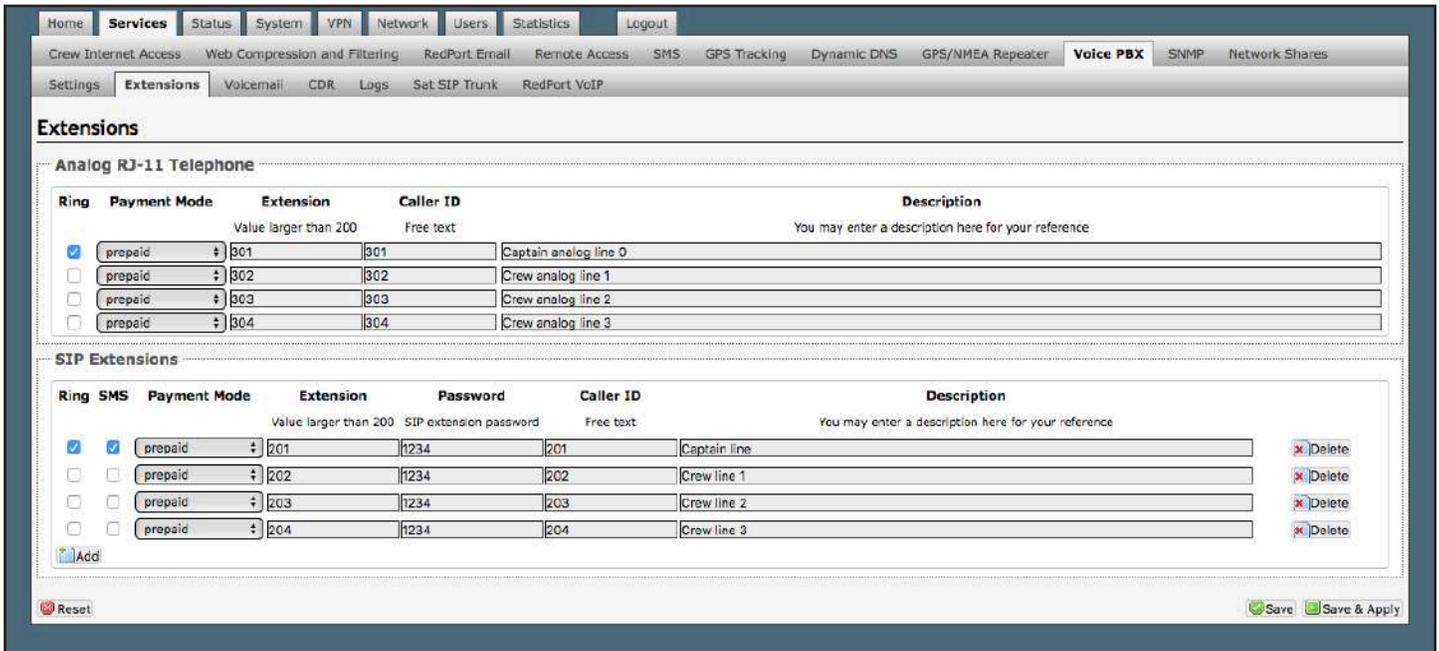


Enter the Key and click <Save & Apply>.



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

Configure the SIP extensions for Ring and/or SMS by clicking the checkbox next to the SIP extension. See **Chapter 5.8.1**.



Select the payment method of each Analog or 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 extension password.
- Change the outgoing CallerID display.
- Enter a description for your reference.

When the configuration of the Analog/SIP extensions is complete, click <Save & Apply>.

5.9. SNMP

SNMP - Simple Network Management Protocol.

Requires 'superadmin' login.

Home Services Status System VPN Network Users Statistics Logout

Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX **SNMP** Network Shares

General Community Com2Sec Group View Access Log

SNMP Settings

Execute "Save & Apply" to apply settings and restart SNMP daemon.

General

Enable	<input checked="" type="checkbox"/> Enable SNMP server.
Port	UDP:161 SNMP UDP port to monitor. Transport can be changed to something other than UDP by specifying [udp tcp][:IPV4-address][:port]. See Net-SNMPD(8) for address specification format.
sysLocation	office The physical location of this node (e.g., telephone closet, 3rd floor).
sysContact	user@example.com The textual identification of the contact person for this managed node, together with information on how to contact this person.
sysName	RedPort Optimizer An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.
sysServices	72 A value which indicates the set of services that this entity primarily offers. A node which is a host offering application services would have a value of 72. See SNMP docs for details.
sysDescr	RedPort Optimizer A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
sysObjectID	1.2.3.4 The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining "what kind of box" is being managed.

Reset Save Save & Apply

5.10. 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: File Transfer for details).

5.10.1. Create a Shared Directory

Network Shares

Samba

General Settings [Edit Template](#)

Hostname:

Description:

Workgroup:

Listen interfaces:

- LAN - 192.168.10.1
- WAN - 192.168.0.79
- 192.168.11.1
- 10.1.5.1

Bind shares to the following interfaces

Shared Directories

Name Share name	Path Relative directory path	Allowed users A comma separated list	Read-only	Allow guests	
<input type="text" value="transferin"/>	<input type="text" value="transferin"/>	<input type="text" value="adtest"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>
<input type="text" value="transferout"/>	<input type="text" value="transferout"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>

Users

Username	Password	
<input type="text" value="adtest"/>	<input type="text" value="1234"/>	<input type="button" value="Delete"/>

Click <Add> to create a new Shared Directory:

Shared Directories

Name Share name	Path Relative directory path	Allowed users A comma separated list	Read-only	Allow guests	
<input type="text" value="transferin"/>	<input type="text" value="transferin"/>	<input type="text" value="adtest"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>
<input type="text" value="transferout"/>	<input type="text" value="transferout"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="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. Click <Save & Apply>.

5.10.2. Add Users

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

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

Username	Password	
adtest	1234	Delete
Add		

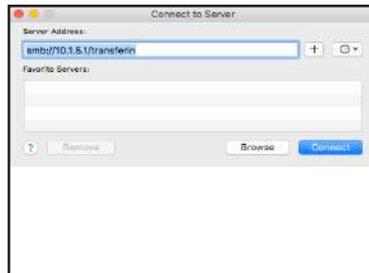
Click <Save & Apply>.

5.10.3. How to Access the Shared Directory and Path Folders:

5.10.3.1. From a Mac PC

Go to Finder > Go > Connect to Server.

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



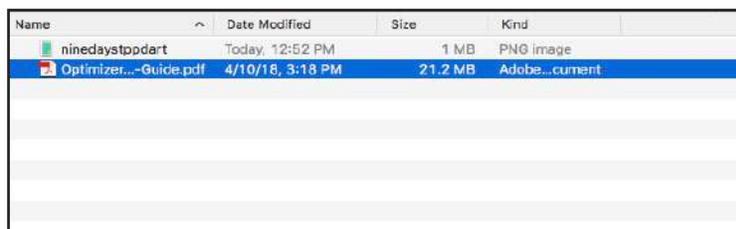
Click <Connect>.

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.

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

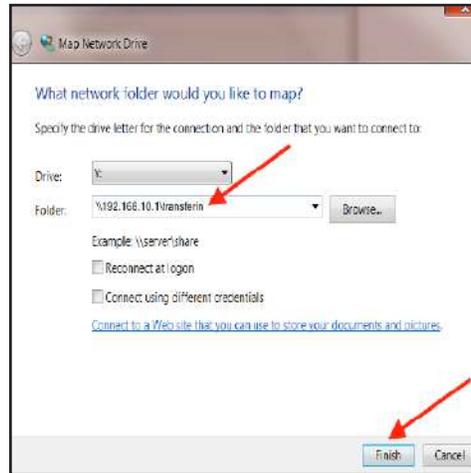


5.10.3.2. From a Windows PC

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 CrewComm\the Path Folder.



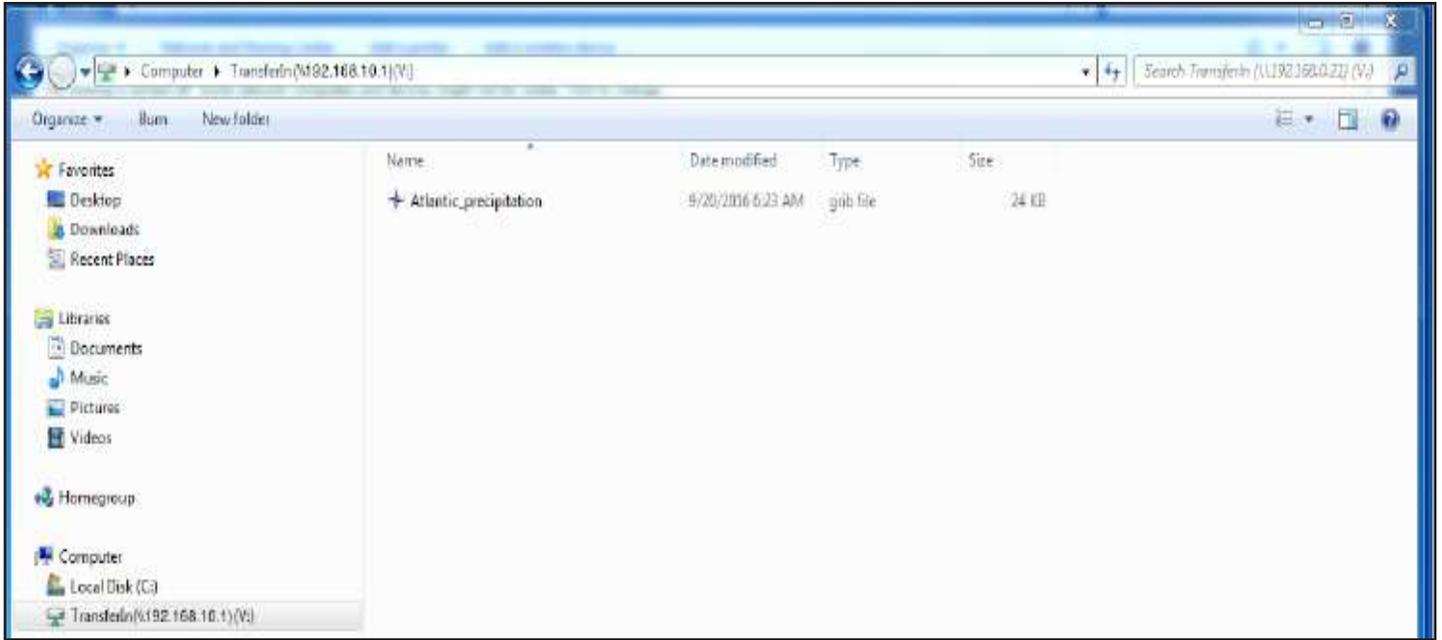
Click <Finish>.



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).



6. Status

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

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



The information provided here includes:

Overview tab - general status.

- System.
- Memory.
- Swap.
- Network.
- DHCP Leases.
- DHCPv6 Leases.
- Wireless.
- Associated Stations.
- Dynamic DNS.
- MWAN.
- Active OpenConnect Users.

Firewall tab - Firewall Status.

- IPv4 Firewall details.
- IPv6 Firewall details.

Routes tab.

- ARP details.
- Active IPv4-Routes.
- Active IPv6-Routes.
- IPv6 Neighbours.

System Log tab.

- Detailed System log.

Kernel Log tab.

- Detailed Kernel log.

Realtime Graphs tab.

- Load graph.
- Traffic graph.
- Wireless graph.
- Connections graph.

All Status information is READ ONLY.

7. 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 time zone).

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 log in 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 log in. 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. Administration

The default password to access the Optimizer Enterprise 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.

The screenshot shows the 'Router Password' configuration page. It has a navigation bar with 'System' selected, and sub-menus for 'Administration', 'Profiles', 'Backup / Flash Firmware', and 'Reboot'. The page is divided into two sections. The top section is titled 'Change Password' and instructs the user to change the password for the 'superadmin' user. It contains two password input fields: 'Password' and 'Confirmation', both with eye icons for visibility. The bottom section is also titled 'Change Password' and instructs the user to change the password for the 'admin' user, noting that this password does not apply to the superadmin account. It also contains 'Password' and 'Confirmation' input fields with eye icons. At the bottom of the page, there are buttons for 'Reset', 'Save', and 'Save & Apply'.

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

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

This procedure changes the password for the Superadmin or the Admin login ONLY. When connecting 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 Enterprise User Interface.

7.3. Profiles

Requires 'superadmin' login.

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

The screenshot shows the 'Profile Manager' configuration page. It has a navigation bar with 'System' selected, and sub-menus for 'Administration', 'Profiles', 'Backup / Flash Firmware', and 'Reboot'. The page title is 'Profile Manager'. Below the title, there is a paragraph explaining that to create predefined router configurations, the user should 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. Below this text is a table titled 'Manage Profiles' with two columns: 'Profile' and 'Description'. The table contains two rows: one for 'WifExtenderProfile' with the description 'Removes the BIZ port and converts it to a wifi extender port for use with the Halo Wifi extender', and one for 'Factory' with the description 'Factory default settings'. Each row has 'Install' and 'Delete' buttons. Below the table is an 'Add' button. At the bottom of the page, there are buttons for 'Reset', 'Save', and 'Save & Apply'.

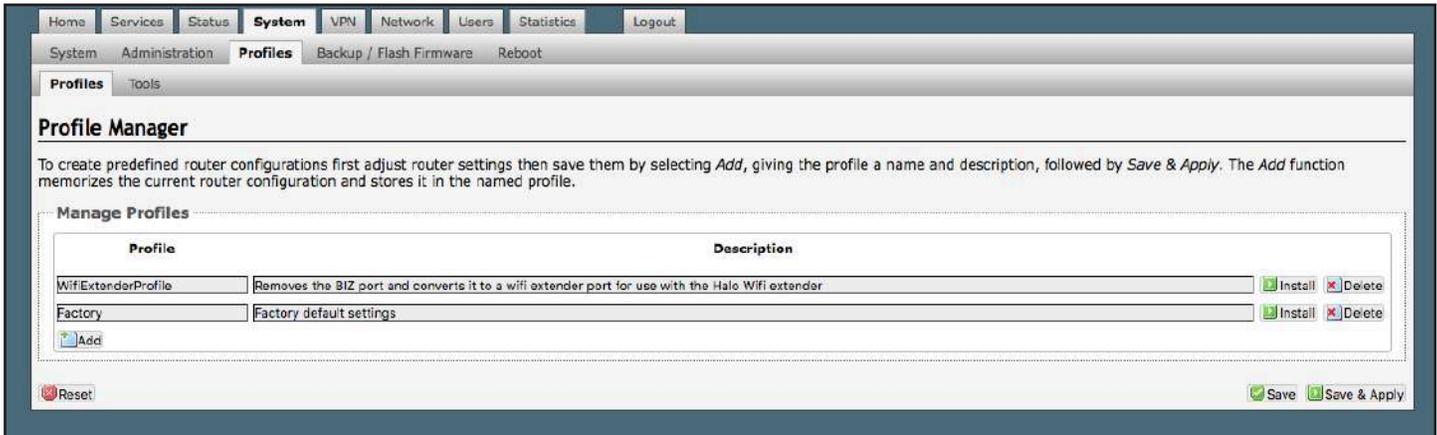
You can configure the Optimizer Enterprise for a specific satellite device and save the profile. This is good for failover situations when using multiple devices. An extreme example would be that you might have the firewall wide open on a VSAT device but in an emergency must use an Iridium handheld device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

Once a profile is saved it can be exported for use in another Optimizer Enterprise 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:



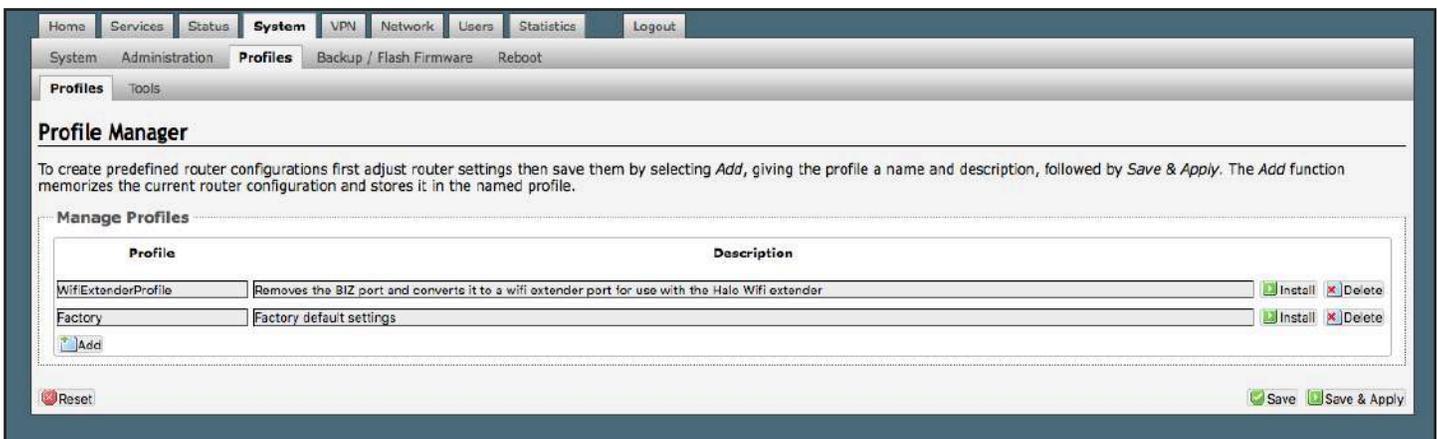
1. Click <Add>.
2. Enter a Name of the new profile and a description.
3. Click <Save & Apply>.

The Add function memorized the current router configuration and stores it in the named profile.

7.3.2. Change to Another Saved Profile

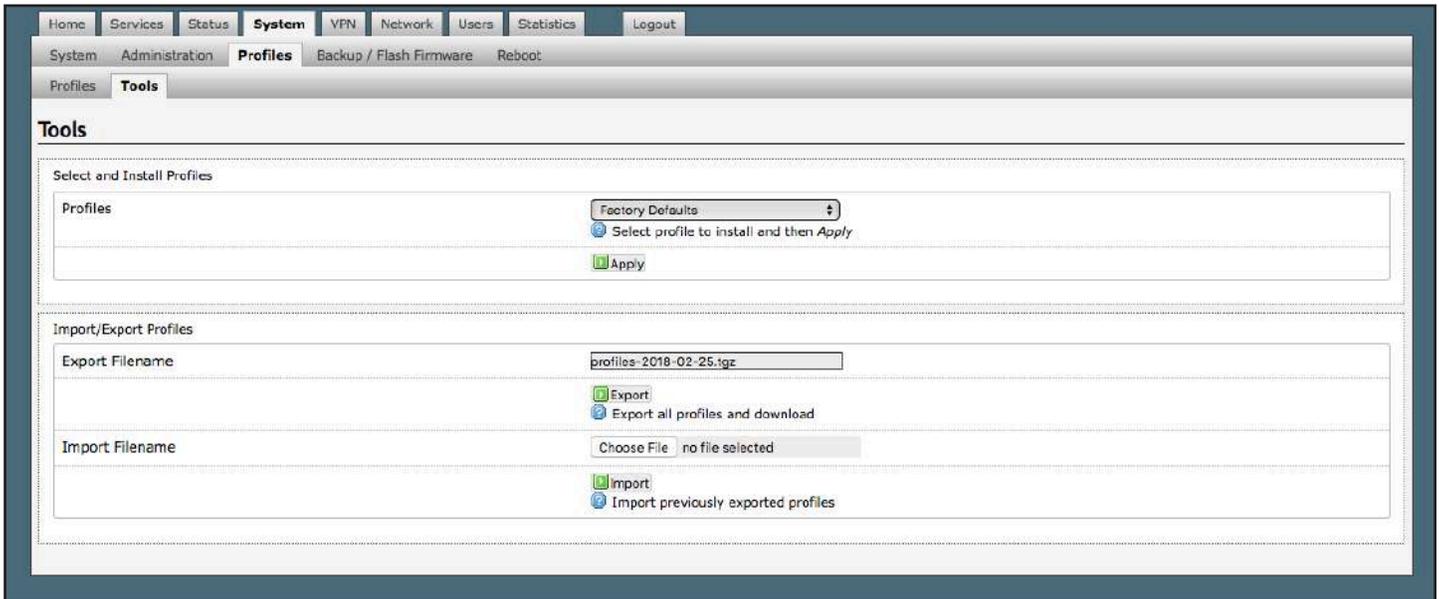
NOTE: Changing profiles will cause the router to reboot.

There are two ways under the Profile tab to change to a different saved profile. To change from one profile to different profile from the Profiles > Profiles tab:



1. Click <Install> next to the new profile of choice.
2. New profile will be installed and the router will reboot.

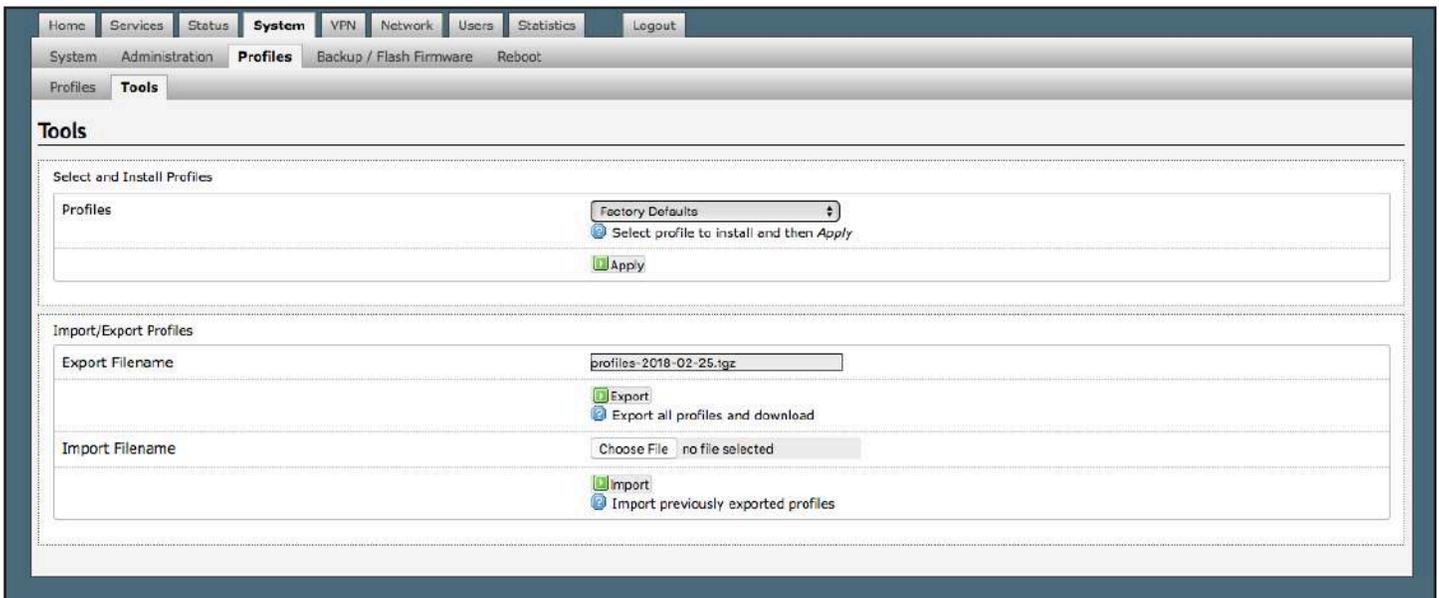
To change to a new profile from the Profiles > Tools tab:



1. Click <"Profile Name"> from the drop-down arrow in the "Profiles" section.
2. Click <Apply>.
3. New profile will be installed, and the router will reboot.

7.3.3. Tools - Export a Profile

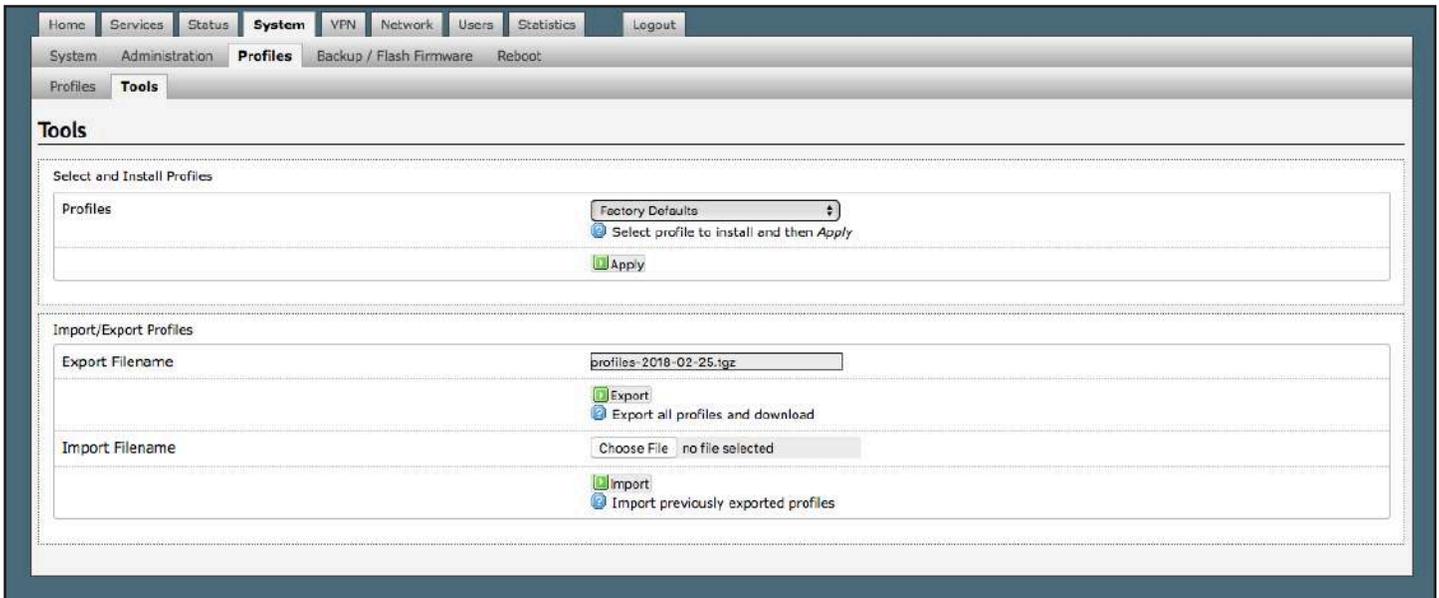
You can export the profiles from the router and use the exported file to 'clone' another Optimizer Enterprise router in System > Profiles > Tools.



1. Enter a filename or use the default name.
2. Click <Export> and save the file.

7.3.4. Import a Profile

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

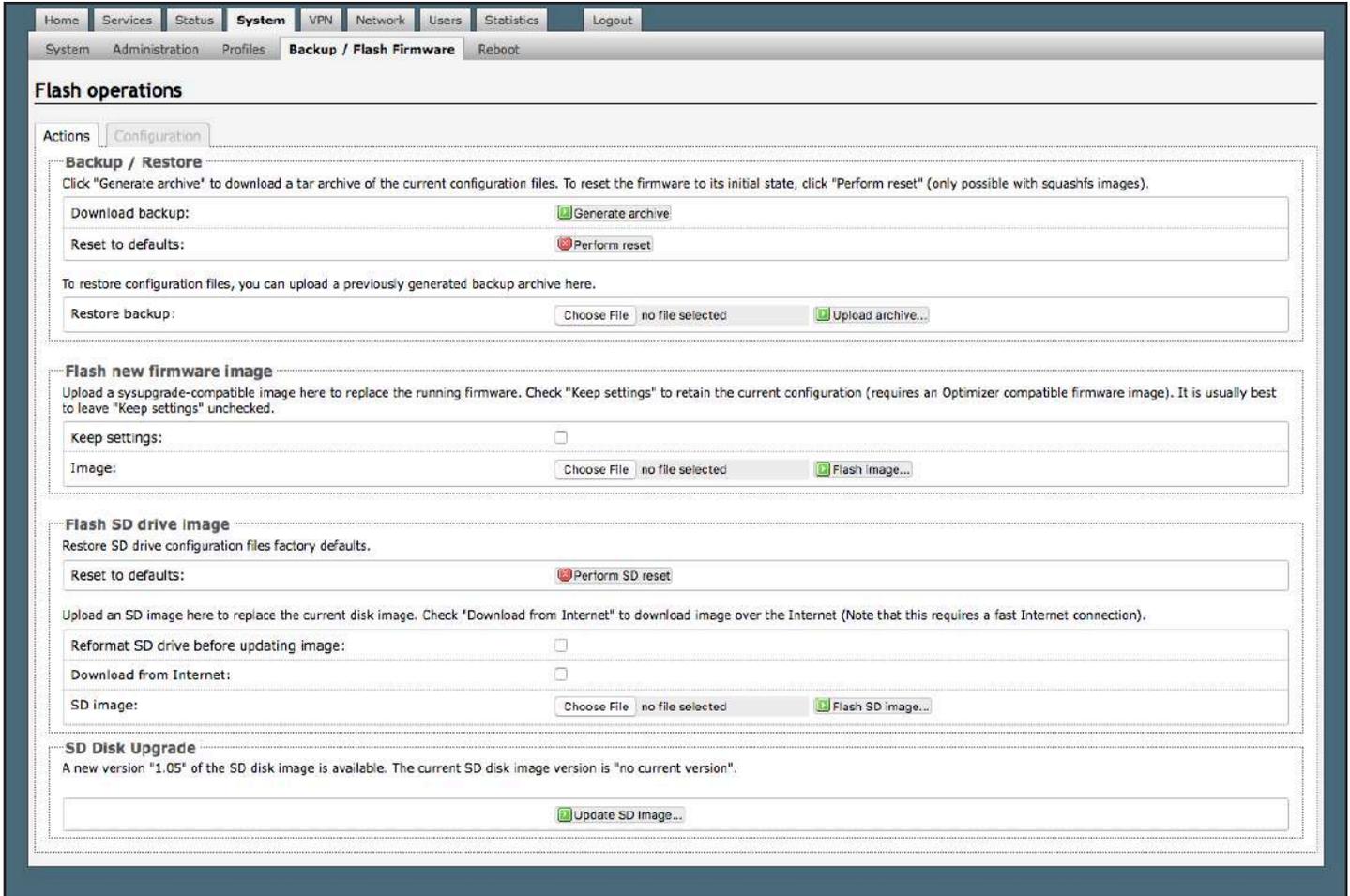


1. Click <Choose File> to locate the saved profiles .tgz file.
2. Click <Import>.

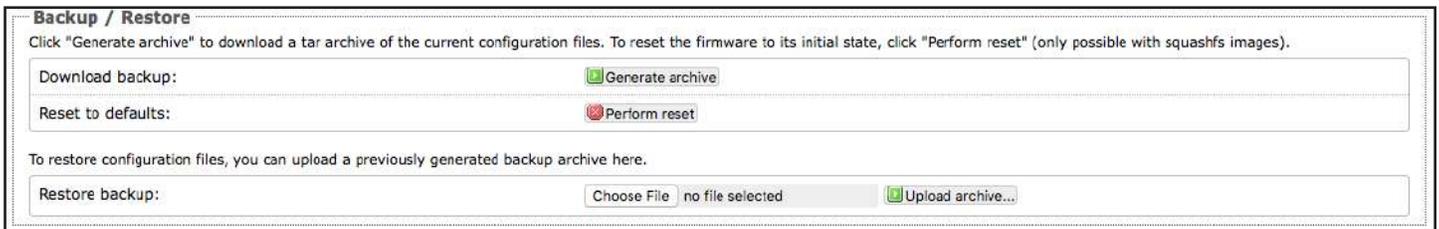
7.4. Backup/Flash Firmware

Requires 'superadmin' login.

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



7.4.1. Backup/Restore



- **Download backup <Generate archive>**: Create and save a Backup archive of the current configuration.
- **Reset to defaults <Perform reset>**: Reset the router to the default configuration.
- **Restore backup <Choose File>, then <Upload archive>**: Restore the router to a previously saved configuration.

To apply the same configuration among several Optimizer Enterprise routers (for example in a fleet situation) create and save a Profile of the configuration that can be applied to other Optimizer Enterprise routers. **See Chapter 7.4.**

7.4.2. Flash New Firmware Image

NOTE: Changing the firmware will cause the router to reboot.

Get the latest Optimizer firmware version from here: 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: no file selected

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

2. Click <Choose File> to where you saved the .bin file and select that file.

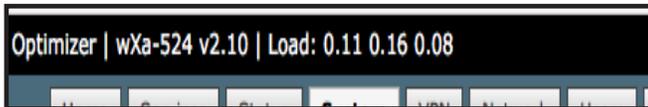
CAUTION: Loading incorrect firmware on your device could render it useless. Be sure to select the appropriate firmware for your device.

3. Click <Flash Image>.

4. The router will reboot.

5. Wait for the lights on the front of the Optimizer Enterprise to begin flashing. When the flashing lights stop, the firmware update is complete. This typically takes several minutes.

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



7.4.3. Flash SD Drive Image

NOTE: Changing the SD Drive Image will cause the router to reboot.

NOTE: If there is an SD Disk Upgrade message informing you of a new version, it is recommended that you update the Image to the most current version.

Flash SD drive image
Restore SD drive configuration files factory defaults.

Reset to defaults:

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: no file selected

SD Disk Upgrade
A new version "1.05" of the SD disk image is available. The current SD disk image version is "1.04".

Reset to defaults <Perform SD reset> : 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:

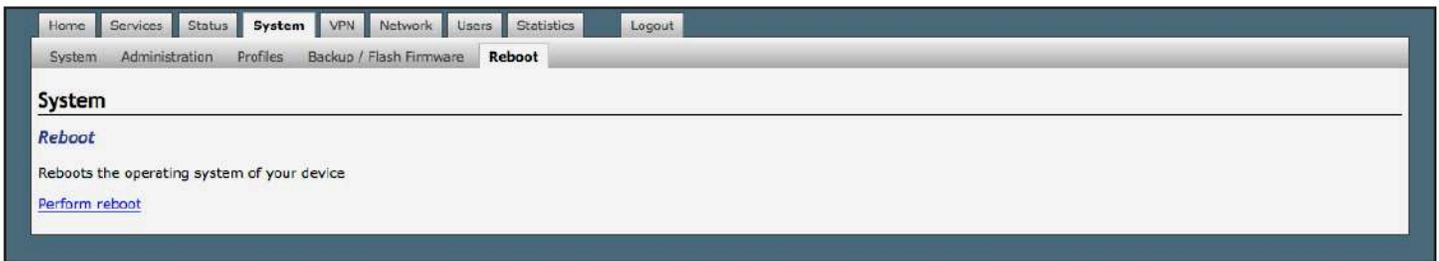
redportglobal.com/support/technical-downloads/.

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

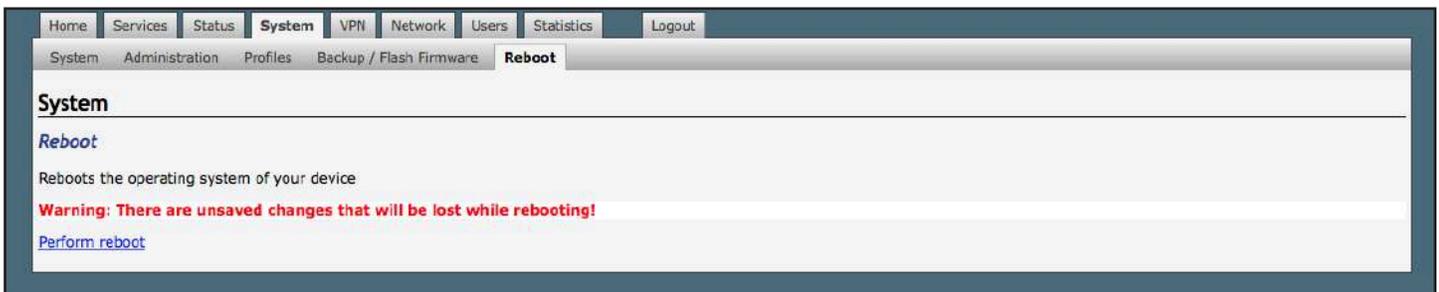
SD Disk Upgrade (only displayed if there is a known new version) <Update SD Image>.

7.5. Reboot

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



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



8. Virtual Private Network (VPN)

Requires 'superadmin' login.

A Virtual Private Network permits a continuous shared private network across a public network.

Use this section to set up a VPN through PPTP, IPSec, OpenConnect VPN, or OpenVPN options to configure a private network that transcends through a public network.

8.1. Point-to-Point Tunneling Protocol PPTP

The screenshot shows the 'PPTP VPN' settings page. The navigation bar includes 'Home', 'Services', 'Status', 'System', 'VPN', 'Network', 'Users', 'Statistics', and 'Logout'. The 'VPN' menu is expanded to show 'PPTP', 'IPSec', 'OpenConnect VPN', and 'OpenVPN'. The 'Settings' tab is selected. The page title is 'PPTP VPN'. The 'Settings' section contains the following fields:

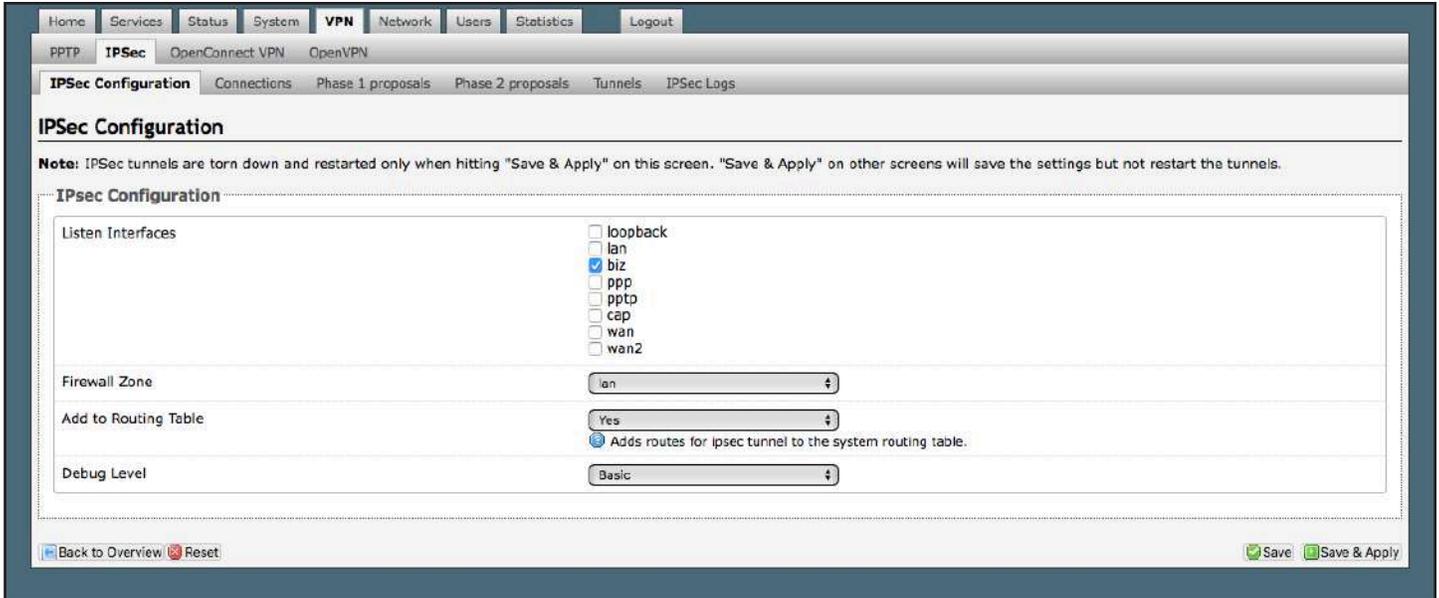
- Enable:** A checkbox that is currently unchecked.
- Local IP:** A text input field containing '192.168.20.1'. Below it is a radio button selected with the text 'Usually an IP on a unique subnet (ie, not LAN)'.
- Remote IP Range:** A text input field containing '20-30'. Below it is a radio button selected with the text 'Remote host IP range in the same network as the local IP. i.e. 20-30 for 192.168.20.20-50'.

At the bottom left is a 'Reset' button. At the bottom right are 'Save' and 'Save & Apply' buttons.

The screenshot shows the 'PPTP VPN Users' page. The navigation bar and menu are the same as in the previous screenshot. The 'Users' tab is selected. The page title is 'PPTP VPN'. The 'VPN users' section contains a table with the following headers: 'Name', 'Password', and 'Comment'. The table is currently empty, with the text 'This section contains no values yet' centered below the headers. There is an 'Add' button at the bottom left of the table area. At the bottom left of the page is a 'Reset' button. At the bottom right are 'Save' and 'Save & Apply' buttons.

8.2. IPSec

IPSec - Internet Protocol Security



8.3. OpenConnect VPN

Home Services Status System **VPN** Network Users Statistics Logout

PPTP IPSec **OpenConnect VPN** OpenVPN

Server Settings User Settings

OpenConnect VPN

OpenConnect

General Settings CA certificate Edit Template

Enable server

Server's certificate SHA1 hash F9A4BDEEC5B471661657FE303D2D8F97C4A8F670
That value should be communicated to the client to verify the server's certificate

Server's Public Key ID sha1:CE097B2A92599658D9D102A1C29814D3CAB61BD3
An alternative value to be communicated to the client to verify the server's certificate; this value only depends on the public key

User Authentication plain
The authentication method for the users. The simplest is plain with a single username-password pair. Use PAM modules to authenticate using another server (e.g., LDAP, Radius).

Firewall Zone
 cap: cap:
 lan: lan: biz:
 ppp: ppp:
 vpn: ppto:
 wan: wan: wan2:
The firewall zone that the VPN clients will be set to

Port 4443
The same UDP and TCP ports will be used

Max clients 8

Max same clients 2

Dead peer detection time (secs) 180

Predictable IPs The assigned IPs will be selected deterministically

Enable compression Enable compression

Enable UDP Enable UDP channel support; this must be enabled unless you know what you are doing

AnyConnect client compatibility Enable support for CISCO AnyConnect clients

VPN IPv4-Network-Address 192.168.100.1

VPN IPv4-Netmask 255.255.255.0

VPN IPv6-Network-Address
CIDR-Notation: address/prefix

DNS servers

The DNS servers to be provided to clients; can be either IPv6 or IPv4

IP Address	Delete
8.8.8.8	
Add	

Routing table

The routing table to be provided to clients; you can mix IPv4 and IPv6 routes, the server will send only the appropriate. Leave empty to set a default route

IP Address	Netmask (or IPv6-prefix)	Delete
192.168.10.0	255.255.255.0	
Add		

Reset Save Save & Apply

8.4. OpenVPN

Home Services Status System **VPN** Network Users Statistics Logout

PPTP IPSec OpenConnect VPN **OpenVPN**

OpenVPN

OpenVPN instances
Below is a list of configured OpenVPN instances and their current state

	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	<input type="checkbox"/>	no	start	1194	udp	Edit Delete
sample_server	<input type="checkbox"/>	no	start	1194	udp	Edit Delete
sample_client	<input type="checkbox"/>	no	start	1194	udp	Edit Delete

Client configuration for an ethernet Add

Reset Save Save & Apply

9. Network

Requires 'superadmin' login.

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

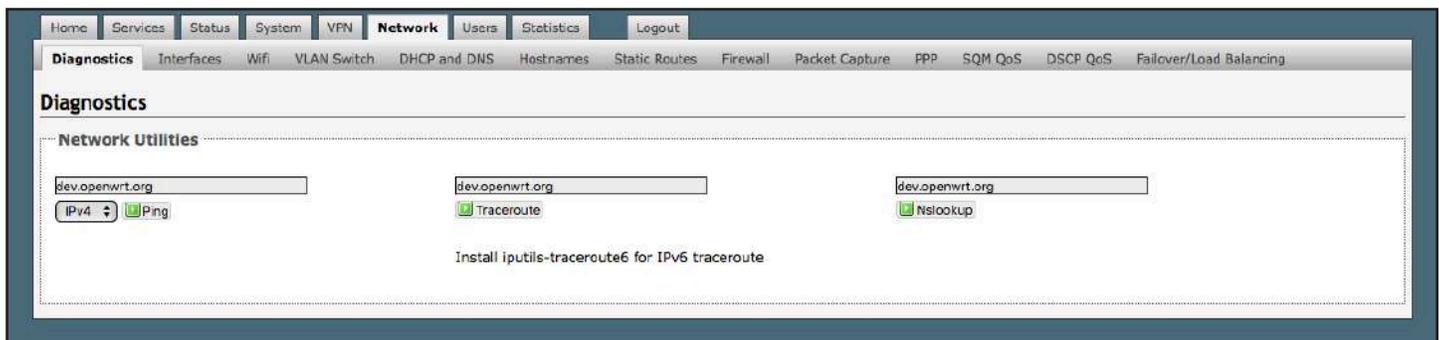
CAUTION: This gives you complete control over the router behavior.

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.

9.1. Diagnostics

This screen provides diagnostic network utilities:

- **Ping:** Click <Ping> to send a set of packet data to a designated website to determine whether the website is reachable as well as the time required for the action.
- **Traceroute:** Click <Traceroute> to send a packet of data to a designated website and return the pathway along the transmission to provide diagnostic data.
- **Nslookup:** Click <Nslookup> to determine information about Internet servers.



9.2. Interfaces Overview

This screen is an at-a-glance view of the current status of each network interface and provides easy access to edit the interface. Each interface can have its own firewall rules (**See Chapter 9.8**).

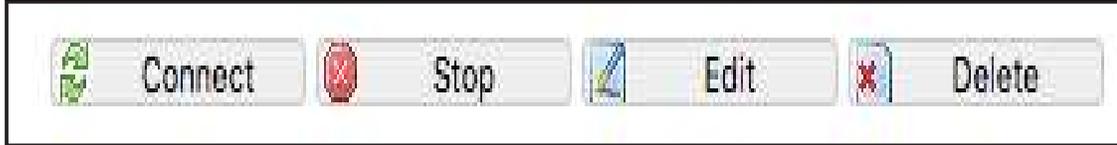
The screenshot shows the 'Interfaces' configuration page in the RedPort web interface. The page is titled 'Interface Overview' and lists several network interfaces. Each interface entry includes a network icon, a name, a status bar, and a set of actions (Connect, Stop, Edit, Delete). The interfaces listed are:

- WAN6**: Status: Up. Uptime: 0h 0m 0s. MAC-Address: [redacted]. RX: 8.32 MB (90902 Pkts.). TX: 929.69 KB (7386 Pkts.).
- CAP**: Status: Up. Uptime: 14h 18m 33s. MAC-Address: 00:00:00:00:00:00. RX: 81.55 KB (884 Pkts.). TX: 365.31 KB (1016 Pkts.). IPv4: 10.1.5.1/24.
- BIZ**: Status: Up. Uptime: 14h 19m 6s. MAC-Address: F4:90:EA:00:01:57. RX: 0.00 B (0 Pkts.). TX: 0.00 B (0 Pkts.). IPv4: 192.168.11.1/24.
- LAN**: Status: Up. Uptime: 14h 19m 6s. MAC-Address: F4:90:EA:00:01:56. RX: 156.73 KB (1105 Pkts.). TX: 391.21 KB (1092 Pkts.). IPv4: 192.168.10.254/24. IPv6: fd49:4e9d:af71::1/60.
- PPP**: Status: Up. Uptime: 14h 12m 28s. RX: 40.19 KB (615 Pkts.). TX: 49.72 KB (881 Pkts.). IPv4: 10.247.113.122/32.
- PPTP**: Status: Up. MAC-Address: [redacted]. RX: 0.00 B (0 Pkts.). TX: 0.00 B (0 Pkts.).
- WAN**: Status: Up. Uptime: 14h 18m 56s. MAC-Address: F4:90:EA:00:01:54. RX: 8.32 MB (90902 Pkts.). TX: 929.69 KB (7386 Pkts.). IPv4: 192.168.0.79/24.
- WAN2**: Status: Up. Uptime: 0h 0m 0s. MAC-Address: F4:90:EA:00:01:55. RX: 0.00 B (0 Pkts.). TX: 0.00 B (0 Pkts.).

Below the interface list, there is a 'Global network options' section with a text input for 'IPv6 ULA-Prefix' containing the value 'fd49:4e9d:af71::4B'. At the bottom, there are 'Reset', 'Save', and 'Save & Apply' buttons.

- **CAP:** This is reserved for the Captive Portal. If the Captive Portal is enabled, all traffic that comes through the Captive Portal will be subject to this interface configuration. This allows you to create rules that apply to the Captive Portal only.
- **BIZ:** This is the business port. By default, it is wide open; any computer directly connected to the BIZ port on the router has full access to the Internet without restrictions.
- **BEST PRACTICE:** Restrict access to this port, protect the router under lock and key OR disable the BIZ interface.
- **LAN:** This is reserved for the local area network. All traffic not routing through the Captive Portal will be subject to this interface configuration.
- **PPP:** This is reserved for USB connected satellite phones and LTE/GSM modems.
- **WAN:** This is typically used for the primary satellite system.
- **WAN2:** This is typically used for the secondary satellite system.

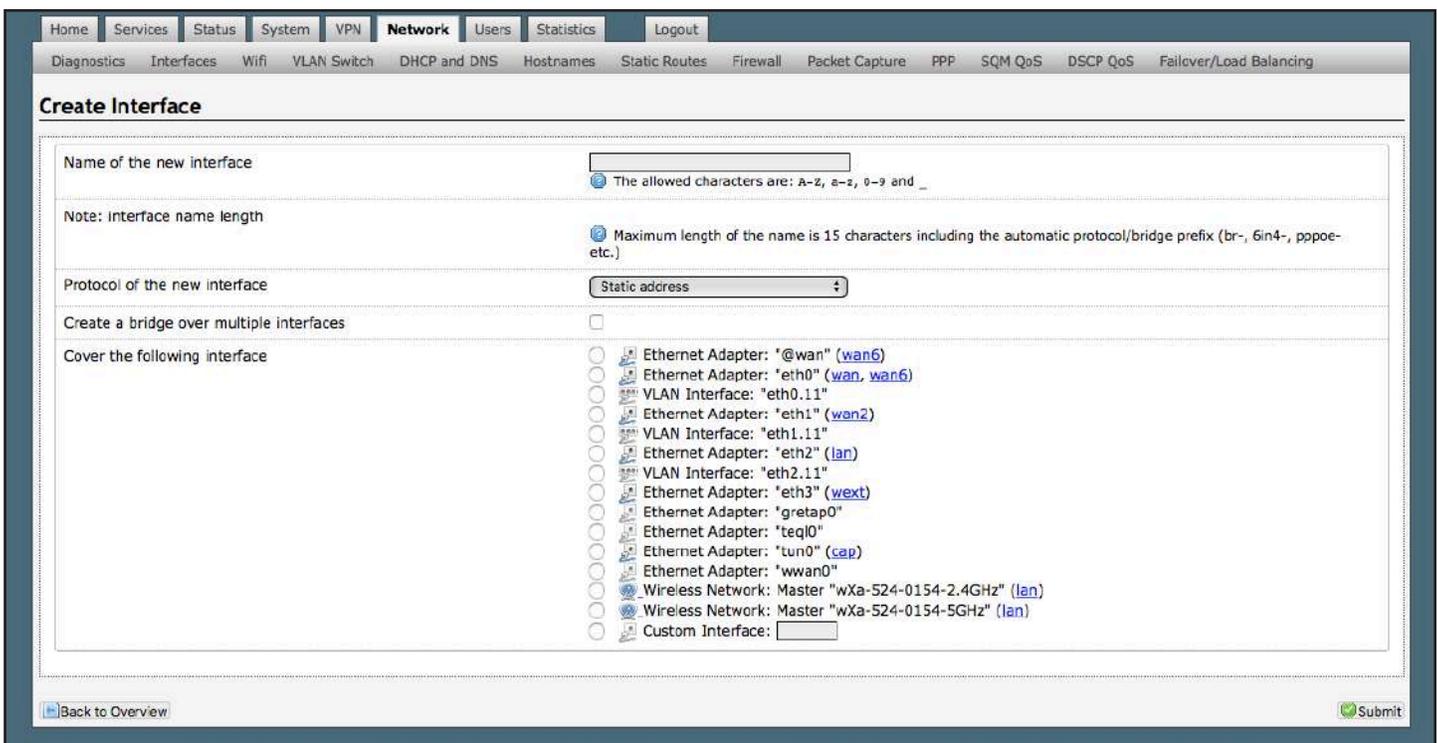
9.2.1. Interface Actions



- **Connect** - Enable an interface.
- **Stop** - Disable an interface.
- **Edit** - Modify the configuration of the interface.
- **Delete** - Remove the interface. **CAUTION: This action cannot be Undone!**

9.2.2. Add a New Interface

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



Complete the Create Interface screen and click <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.

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

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

9.2.3. Select Interfaces Tabs

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



Use these tabs within a specific interface tab to configure the network interfaces.

Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

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

9.2.3.1. 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.

Home | Services | Status | System | VPN | **Network** | Users | Statistics | Logout

Diagnostics | **Interfaces** | Wifi | VLAN Switch | DHCP and DNS | Hostnames | Static Routes | Firewall | Packet Capture | PPP | SQM QoS | DSCP QoS | Failover/Load Balancing

WAN2 | WAN | **BIZ** | PPTP | LAN | CAP | PPP | WAN6

Interfaces - BIZ

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

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Status

Uptime: 14h 24m 45s
 MAC-Address: F4:90:EA:00:01:57
 RX: 0.00 B (0 Pkts.)
 TX: 0.00 B (0 Pkts.)
 IPv4: 192.168.11.1/24

eth3

Protocol: Static address

IPv4 address: 192.168.11.1

IPv4 netmask: 255.255.255.0

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

General Setup | Advanced Settings | IPv6 Settings

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).

Back to Overview | Reset | Save | Save & Apply

9.2.3.2. 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.

The screenshot shows the RedPort web interface for configuring network interfaces. The top navigation bar includes Home, Services, Status, System, VPN, Network, Users, Statistics, and Logout. The main menu has tabs for Diagnostics, Interfaces, Wifi, VLAN Switch, DHCP and DNS, Hostnames, Static Routes, Firewall, Packet Capture, PPP, SQM QoS, DSCP QoS, and Failover/Load Balancing. Under the Interfaces tab, there are sub-tabs for WAN2, WAN, BIZ, PPTP, LAN, CAP, PPP, and WAN6. The current view is for the 'BIZ' interface.

Interfaces - BIZ

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

General Setup | **Advanced Settings** | Physical Settings | Firewall Settings

Bring up on boot	<input checked="" type="checkbox"/>
Use builtin IPv6-management	<input checked="" type="checkbox"/>
Override MAC address	<input type="text" value="F4:90:2A:00:01:57"/>
Override MTU	<input type="text" value="1500"/>
Use gateway metric	<input type="text" value="0"/>

DHCP Server

General Setup | **Advanced Settings** | IPv6 Settings

Ignore interface	<input type="checkbox"/> Disable DHCP for this interface.
Start	<input type="text" value="100"/> <input checked="" type="radio"/> Lowest leased address as offset from the network address.
Limit	<input type="text" value="150"/> <input checked="" type="radio"/> Maximum number of leased addresses.
Leasetime	<input type="text" value="12h"/> <input checked="" type="radio"/> Expiry time of leased addresses, minimum is 2 minutes (2m).

Back to Overview | Reset | Save | Save & Apply

NOTE: Each WAN interface must be assigned a unique number in the "Use gateway metric" field. This number is required for configuring Failover/Load Balancing.

9.2.3.3. Physical Settings

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

The screenshot displays the RedPort web interface for configuring network interfaces. The top navigation bar includes Home, Services, Status, System, VPN, Network, Users, Statistics, and Logout. The main menu shows various network-related options like Diagnostics, Interfaces, Wifi, VLAN Switch, DHCP and DNS, etc. The current page is titled 'Interfaces - BIZ'.

Under the 'Common Configuration' section, there are four tabs: General Setup, Advanced Settings, Physical Settings, and Firewall Settings. The 'General Setup' tab is active. It features a 'Bridge interfaces' section with a checkbox for 'creates a bridge over specified interface(s)'. Below this is a list of available network interfaces for selection:

- Ethernet Adapter: "@wan" (wan6)
- Ethernet Adapter: "eth0" (wan, wan6)
- VLAN Interface: "eth0.11"
- Ethernet Adapter: "eth1" (wan2)
- VLAN Interface: "eth1.11"
- Ethernet Adapter: "eth2" (lan)
- VLAN Interface: "eth2.11"
- Ethernet Adapter: "eth3" (biz)
- Ethernet Adapter: "gretap0"
- Ethernet Adapter: "teql0"
- Ethernet Adapter: "tun0" (cap)
- Ethernet Adapter: "wwan0"
- Wireless Network: Master "wXa-524-0154-2.4GHz" (lan)
- Wireless Network: Master "wXa-524-0154-5GHz" (lan)
- Custom Interface:

Below the interface list is the 'DHCP Server' section, which includes tabs for General Setup, Advanced Settings, and IPv6 Settings. The 'General Setup' tab is active. It contains the following settings:

- Ignore interface: Disable DHCP for this interface.
- Start:**
 - Lowest leased address as offset from the network address.
- Limit:**
 - Maximum number of leased addresses.
- Leasetime:**
 - Expiry time of leased addresses, minimum is 2 minutes (2π).

At the bottom of the configuration area, there are buttons for 'Back to Overview', 'Reset', 'Save', and 'Save & Apply'.

9.2.3.4. Firewall Settings

Use this to select the Firewall Zone you want to assign to the Interface. **See Chapter 9.8** for Firewall Zone details. You can also configure the DHCP Server Settings from this page.

The screenshot shows the RedPort web interface for configuring network interfaces. The navigation bar includes Home, Services, Status, System, VPN, Network, Users, Statistics, and Logout. The main menu has tabs for Diagnostics, Interfaces, Wifi, VLAN Switch, DHCP and DNS, Hostnames, Static Routes, Firewall, Packet Capture, PPP, SQM QoS, DSCP QoS, and Failover/Load Balancing. The sub-menu for Interfaces includes WAN2, WAN, BIZ, PPTP, LAN, CAP, PPP, and WAN5. The page title is "Interfaces - BIZ".

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

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Create / Assign firewall-zone

- cap: cap: [icon]
- lan: lan: [icon] [icon] [icon] biz: [icon]
- ppp: ppp: [icon]
- vpn: pptp: [icon]
- wan: wan: [icon] wan2: [icon]
- unspecified -or- create: [input field]

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

General Setup | Advanced Settings | IPv6 Settings

Ignore interface Disable DHCP for this interface.

Start: [input field: 100] Lowest leased address as offset from the network address.

Limit: [input field: 150] Maximum number of leased addresses.

Leasetime: [input field: 12h] Expiry time of leased addresses, minimum is 2 minutes (2m).

Back to Overview | Reset | Save | Save & Apply

9.2.3.5. DHCP Server - General Setup

The screenshot shows the DHCP Server configuration page for interface BIZ. The navigation bar and main menu are the same as in the previous screenshot. The sub-menu for Interfaces includes WAN2, WAN, BIZ, PPTP, LAN, CAP, PPP, and WAN5. The page title is "DHCP Server".

DHCP Server

General Setup | Advanced Settings | IPv6 Settings

Ignore interface Disable DHCP for this interface.

Start: [input field: 100] Lowest leased address as offset from the network address.

Limit: [input field: 150] Maximum number of leased addresses.

Leasetime: [input field: 12h] Expiry time of leased addresses, minimum is 2 minutes (2m).

Back to Overview | Reset | Save | Save & Apply

9.2.3.6. DHCP Server Advanced

DHCP Server

General Setup | **Advanced Settings** | IPv6 Settings

Dynamic DHCP Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force Force DHCP on this network even if another server is detected.

IPv4-Netmask Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

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

9.2.3.7. DHCP Server IPv6 Settings

DHCP Server

General Setup | **Advanced Settings** | **IPv6 Settings**

Router Advertisement-Service

DHCPv6-Service

NDP-Proxy

Announced DNS servers

Announced DNS domains

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

9.3. WiFi

Requires "superadmin" login.

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

Home | Services | Status | System | VPN | **Network** | Users | Statistics | Logout

Diagnostics | Interfaces | **Wifi** | VLAN Switch | DHCP and DNS | Hostnames | Static Routes | Firewall | Packet Capture | PPP | SQM QoS | DSCP QoS | Failover/Load Balancing

radio0: Master "wXa-524-0154-2.4GHz" radio1: Master "wXa-524-0154-5GHz"

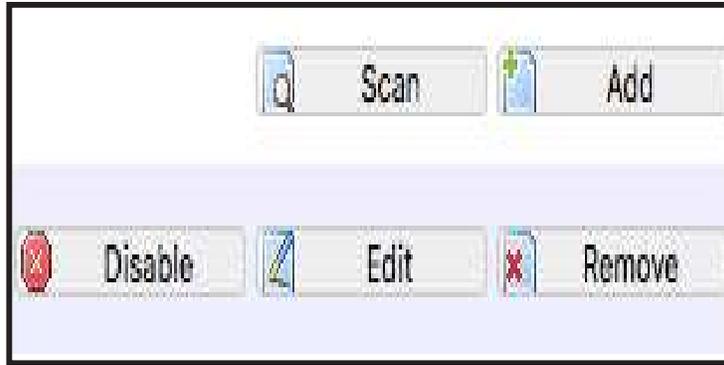
Wireless Overview

Generic MAC80211 802.11abgn (radio0)
 Channel: 6 (2.437 GHz) | Bitrate: ? Mbit/s
 SSID: wXa-524-0154-2.4GHz | Mode: Master
 0% BSSID: F4:90:EA:00:01:56 | Encryption: None

Generic MAC80211 802.11abgn (radio1)
 Channel: 36 (5.180 GHz) | Bitrate: 144.4 Mbit/s
 SSID: wXa-524-0154-5GHz | Mode: Master
 100% BSSID: F4:90:EA:00:01:56 | Encryption: None

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
wXa-524-0154-5GHz	EC:35:86:3B:80:84	?	-32 dBm	0 dBm	130.0 Mbit/s, MCS 15, 20MHz	144.4 Mbit/s, MCS 15, 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.

9.3.1. Rename the Wireless Network

The default name of the Optimizer Enterprise’s wireless network is wXa-524-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.

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
wXa-524-0154-5GHz	EC:35:86:3B:80:84	?	-32 dBm	0 dBm	130.0 Mbit/s, MCS 15, 20MHz	144.4 Mbit/s, MCS 15, 20MHz

Locate the wXa WiFi network and click <Edit>.

Interface Configuration

General Setup | Wireless Security | MAC-Filter

ESSID: wXa-524-0154-2.4GHz

Mode: Access Point

Network

- cap: [icon]
- lan: [icon]
- ppp: [icon]
- pptp: [icon]

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.

9.3.2. 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.

Home | Services | Status | System | VPN | **Network** | Users | Statistics | Logout

Diagnostics | Interfaces | **Wifi** | VLAN Switch | DHCP and DNS | Hostnames | Static Routes | Firewall | Packet Capture | PPP | SQM QoS | DSCP QoS | Failover/Load Balancing

radio0: Master "wXa-524-0154-2.4GHz" | radio1: Master "wXa-524-0154-5GHz"

Wireless Overview

Generic MAC80211 802.11abgn (radio0)
Channel: 6 (2.437 GHz) | Bitrate: ? Mbit/s
SSID: wXa-524-0154-2.4GHz | Mode: Master
0% BSSID: F4:90:EA:00:01:56 | Encryption: None

Generic MAC80211 802.11abgn (radio1)
Channel: 36 (5.180 GHz) | Bitrate: 144.4 Mbit/s
100% SSID: wXa-524-0154-5GHz | Mode: Master
BSSID: F4:90:EA:00:01:56 | Encryption: None

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
wXa-524-0154-5GHz	EC:35:96:3B:80:84	?	-32 dBm	0 dBm	130.0 Mbit/s, MCS 15, 20MHz	144.4 Mbit/s, MCS 15, 20MHz

Locate the wXa WiFi network and click <Edit>.

Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

Encryption: No Encryption

1. Select the Encryption mode from the drop-down menu.
2. Enter your desired password in the Key field.

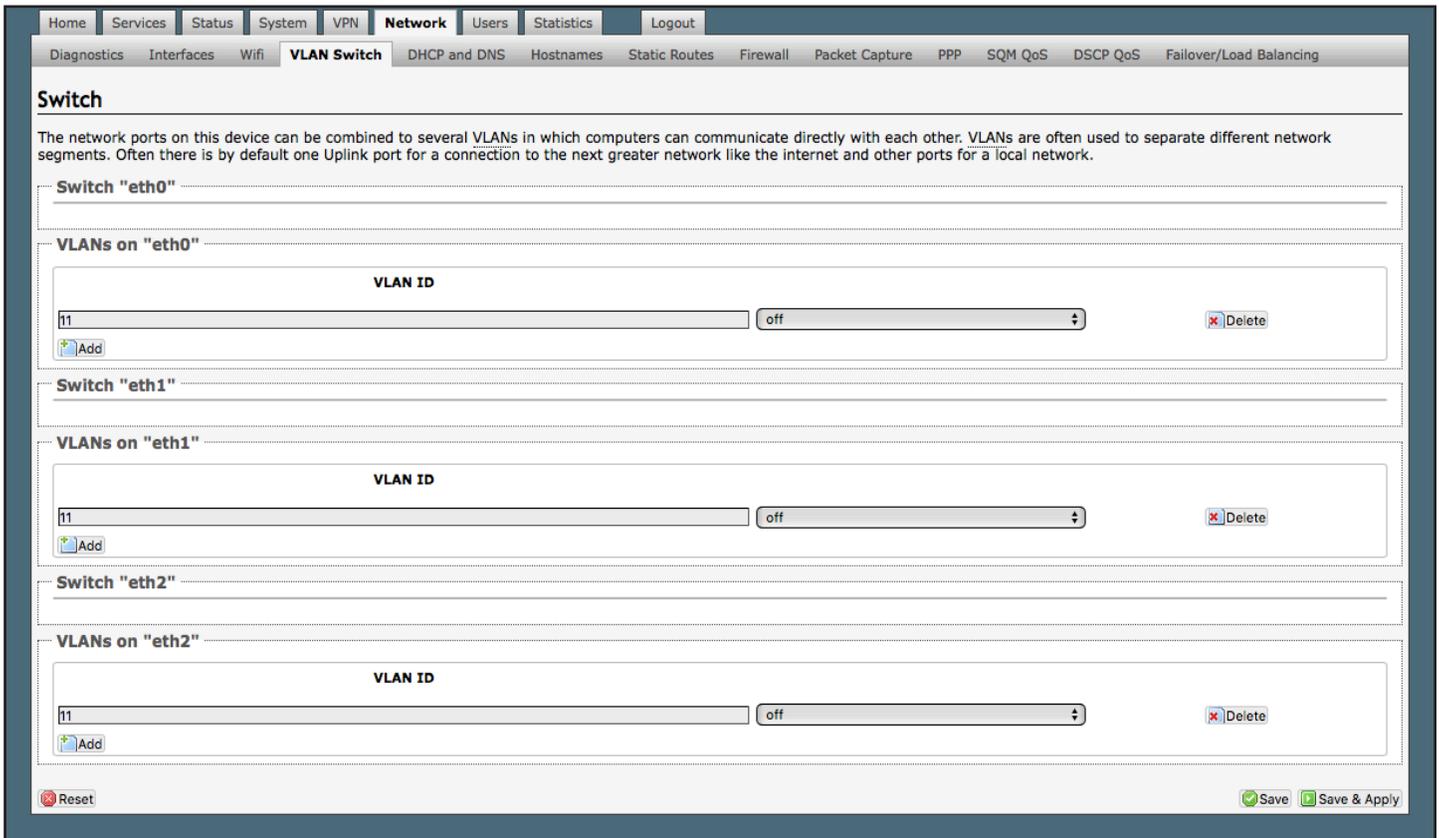
3. Click <Save & Apply>.

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.

9.4. VLAN Switch

VLAN - Virtual Local Area Network

Requires “superadmin” login.



9.5. DHCP and DNS

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

Requires “superadmin” login.

The Optimizer Enterprise is a DNS server.

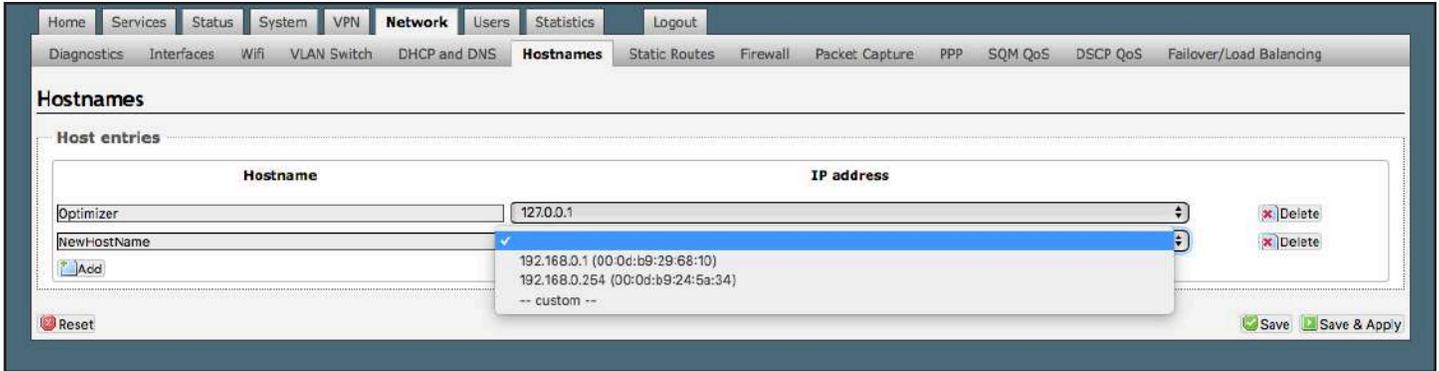
With the Captive Portal enabled, DHCP and DNS all happen within the Captive Portal, therefore there is no reason to modify these settings.

9.6. Hostnames

Requires “superadmin” login.

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

9.6.1. Add Hostname

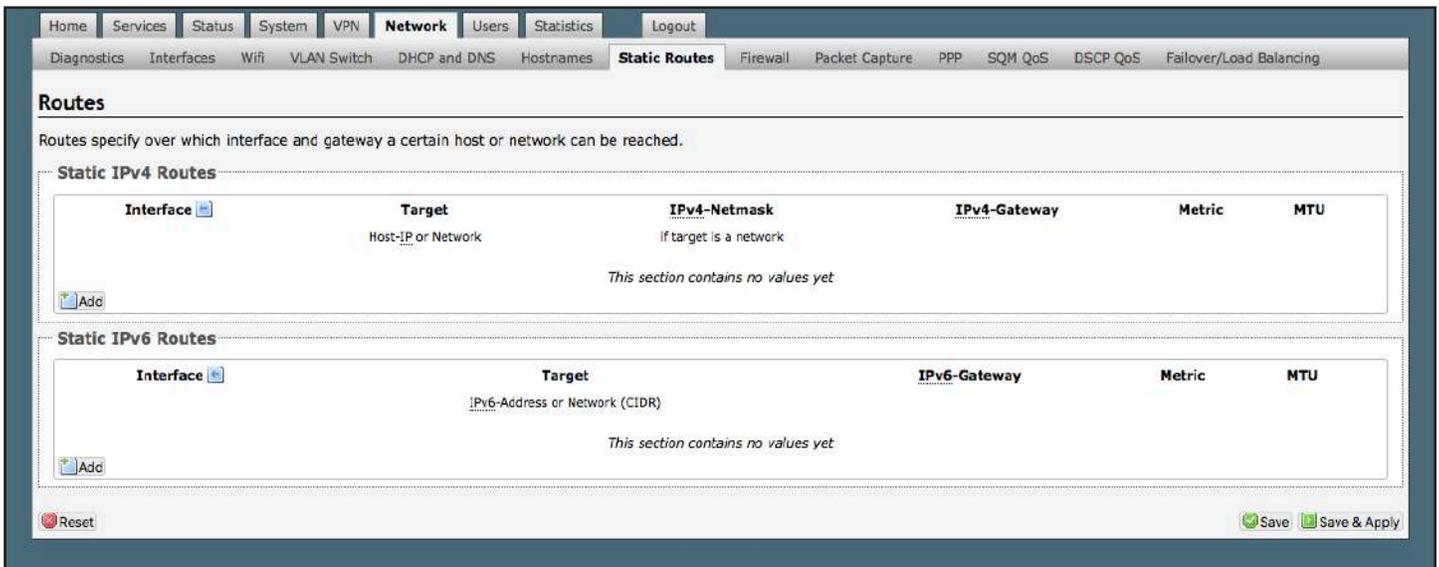


1. Click <Add>.
2. Enter the new Hostname.
3. Select the IP address from the drop-down list OR select custom to enter the IP address.
4. Click <Save & Apply>.

9.7. 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.



Static routes take precedent over Mwan Traffic Rules.

9.8. Firewall

Requires “superadmin” login.

The Firewall allows you to control network traffic flow over each interface. Most installations do not require any firewall modifications due to the flexibility of the Captive Portal configuration (See [Chapter 5.1](#)) and the Failover/ Load Balancing configuration (See [Chapter 9.13](#)).

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

9.8.1. 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.

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
cap: cap: ⇒ ACCEPT	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
lan: lan: biz: ⇒ ppp wan	reject	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan: wan2: ⇒ REJECT	accept	accept	reject	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
vpn: pptp: ⇒ ACCEPT	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete

Buttons: [Reset](#) [Save](#) [Save & Apply](#)

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 through the router via an interface and out of the router. If Forward is allowed, you must configure the Inter-Zone Forwarding.
- **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.

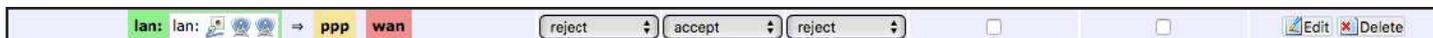
The router is shipped to you with several Firewall Zones configured and interfaces assigned to them:

ppp: ppp: ⇒ REJECT | reject | accept | reject | | | [Edit](#) [Delete](#)

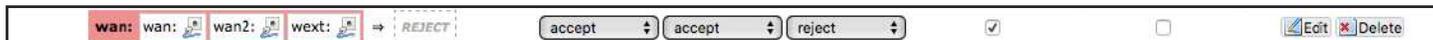
The “ppp” firewall zone has only the ppp interface assigned to it. This is the zone for dialup connections. In this default configuration, only Output traffic is allowed. Input and Forwarded traffic is rejected.

cap: cap: ⇒ ACCEPT | accept | accept | accept | | | [Edit](#) [Delete](#)

The “cap” firewall zone has only the cap interface assigned to it. This is the zone for the Captive Portal. In this default configuration, all traffic is allowed but subject to the Captive Portal settings.



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



The “wan” firewall zone has the wan, wan2 and wext interfaces assigned to it. This is the zone for satellite connections. In this default configuration, only Output traffic is allowed.



The “vpn” firewall zone has the pptp interface assigned to it. This is the zone for virtual private networks.

CAUTION: While it is possible to edit these zones and add new zones, Best Practice is to leave these zones alone and create Mwan Traffic Rules instead, assigning the new rules to a Zone. See **Chapter 9.13.2.5**.

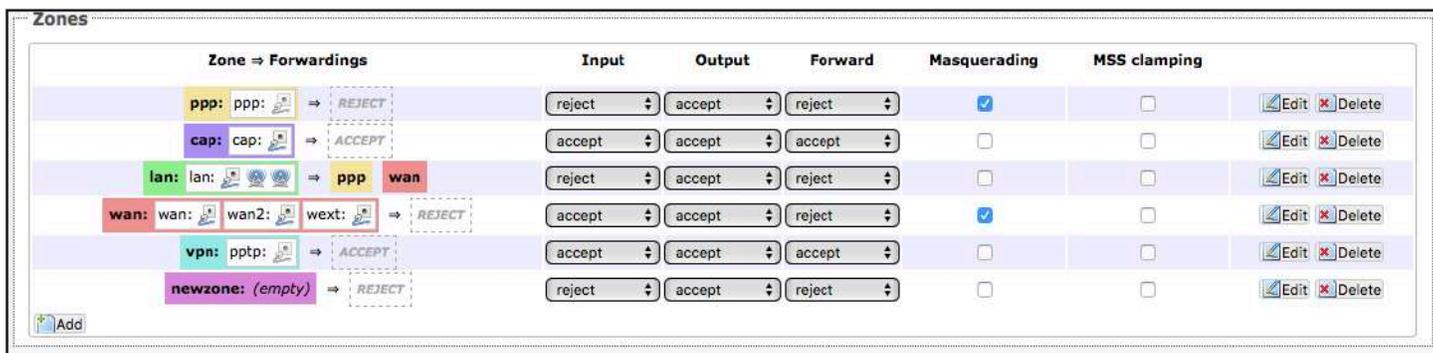
FOR EXAMPLE: If a system administrator wants to create firewall zones that are different for each device, such as firewall rules for WiFi to allow all, rules for vsat to allow dns and http but nothing else, for fbb do not allow anything but email. You could create three new zones; one for each wan interface, then create firewall rules that pertain to each of the new zones. You then edit the lan interface to add the three new zones.

OR, do not create zones but use IP addresses added to the mwan traffic rules (not the firewall rules). Leave the zones the same, use Mwan traffic rules, assigning the rule to a zone and use IP source address or a specific IP address. The destination can be any address and apply to any zone. See **Chapter 9.13.2.5**.

9.8.1.1. Add a Firewall Zone

Requires “superadmin” login.

To add a new Firewall Zone, click <Add> on the General Settings page, in the ‘Zones’ section.



The screenshot shows the 'Firewall - Zone Settings - Zone "newzone"' configuration page. The page has a navigation bar with tabs for Home, Services, Status, System, VPN, Network (selected), Users, and Statistics. Below this is a sub-navigation bar with tabs for Diagnostics, Interfaces, Wifi, VLAN Switch, DHCP and DNS, Hostnames, Static Routes, Firewall (selected), Packet Capture, PPP, SQM QoS, DSCP QoS, and Failover/Load Balancing. The main content area is titled 'Firewall - Zone Settings - Zone "newzone"'. It contains two sections: 'Zone "newzone"' and 'Inter-Zone Forwarding'. The 'Zone "newzone"' section has 'General Settings' and 'Advanced Settings' tabs. The 'General Settings' tab is active, showing fields for Name (newzone), Input (reject), Output (accept), Forward (reject), Masquerading (unchecked), MSS clamping (unchecked), and Covered networks (a list of checkboxes for various network interfaces like cap, lan, ppp, pptp, wan, wan2, wan6, wext, and a 'create' field). The 'Inter-Zone Forwarding' section has a descriptive paragraph and two sections: 'Allow forward to destination zones:' and 'Allow forward from source zones:'. Each section contains a list of checkboxes for various network interfaces, with some interfaces highlighted in colored boxes (purple for cap, green for lan, yellow for ppp, cyan for vpn, red for wan).

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

9.8.1.2. Delete a Firewall Zone

CAUTION: This action CANNOT be undone.

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

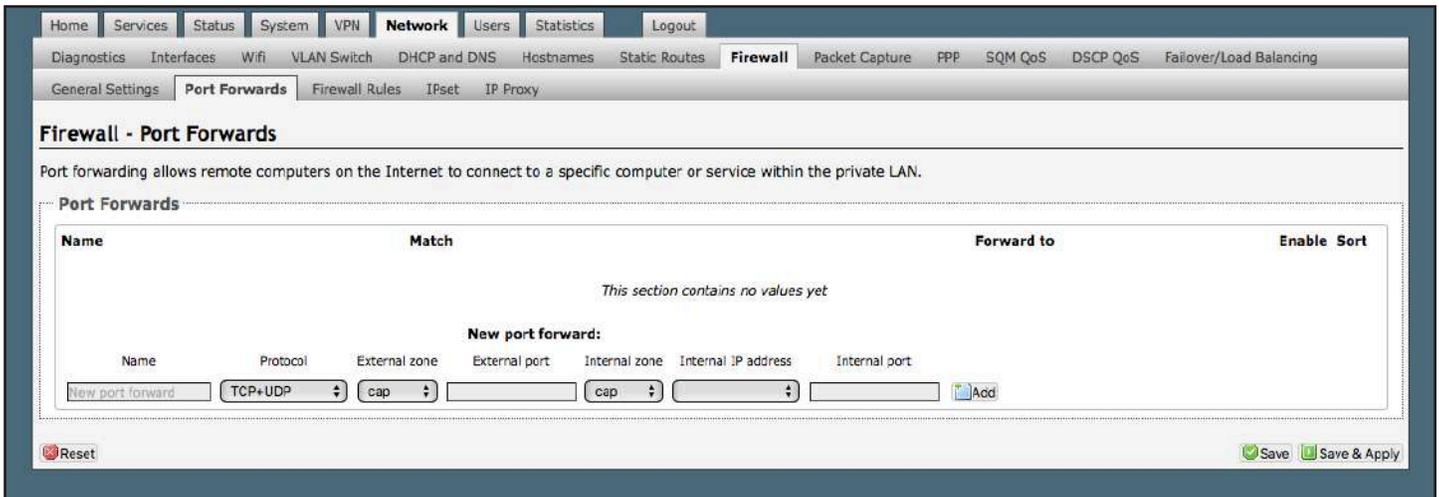


9.8.2. Port Forwards

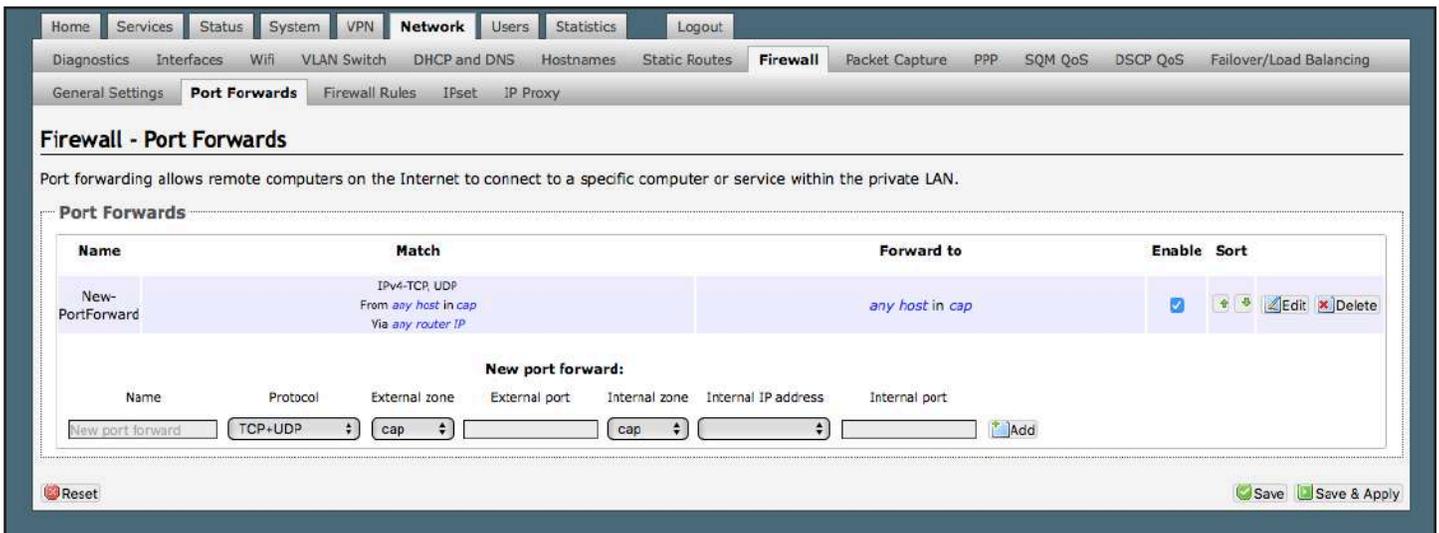
Requires “superadmin” login.

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.



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



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

CAUTION: The Delete function cannot be undone.

9.8.3. Firewall - Traffic Rules

This page is the firewall traffic rules table. The table includes all the firewall rules on the router that will allow you to enable and disable ports and IP address, etc.

While you can add rules, delete rules and each interface can have its own set of rules, BEST PRACTICE is to manage router traffic via the Failover/Load Balancing MWAN Traffic Rules (**See Chapter 9.13.2.5**).

By default, the router is shipped to you with six rules that all say DO NOT MODIFY. They are: ALL, Pass DNS, DNS, HTTP, HTTPS and FTP. These are the rules that the Captive Portal and Proxy Server automatically enable and disable so the components work without you having to make modifications to the Firewall Traffic Rules Table. When enabled, these rules Allow that particular traffic to pass through the firewall. This means that the Firewall is totally OPEN by default. When you configure the Captive Portal and Failover/Load Balancing you can restrict the allowed traffic through an interface.

All the firewall rules can easily be enabled (checked) or disabled (unchecked).

The first 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.

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

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

You can also create a custom rule.

9.8.3.1. Create a Custom Rule

Requires “superadmin” login.

The screenshot shows the 'Firewall - Traffic Rules' configuration page. At the top, there are navigation tabs for Home, Services, Status, System, VPN, Network, Users, Statistics, and Logout. Below these are sub-tabs for Diagnostics, Interfaces, Wifi, VLAN Switch, DHCP and DNS, Hostnames, Static Routes, Firewall, Packet Capture, PPP, SQM QoS, DSCP QoS, and Failover/Load Balancing. The 'Firewall Rules' sub-tab is active.

The main content area is titled 'Firewall - Traffic Rules' and includes a description: '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.'

Below the description is a table of existing traffic rules:

Name	Match	Action	Enable	Sort
BLOCK WAN DO_NOT_MODIFY	Any traffic From any host in wan To any router IP on this device	Discard input	<input type="checkbox"/>	[Up] [Down] [Edit] [Delete]
ALL DO_NOT_MODIFY	Any traffic From any host in any zone To any host in any zone	Accept forward	<input checked="" type="checkbox"/>	[Up] [Down] [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	<input checked="" type="checkbox"/>	[Up] [Down] [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	<input checked="" type="checkbox"/>	[Up] [Down] [Edit] [Delete]
HTTP DO_NOT_MODIFY	Any TCP From any host in any zone To any host, port 80 in any zone	Accept forward	<input checked="" type="checkbox"/>	[Up] [Down] [Edit] [Delete]
HTTPS DO_NOT_MODIFY	Any TCP From any host in any zone To any host, port 443 in any zone	Accept forward	<input checked="" type="checkbox"/>	[Up] [Down] [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	<input checked="" type="checkbox"/>	[Up] [Down] [Edit] [Delete]

Below the table are two form sections:

Open ports on router:

Name: Protocol: External port:

New forward rule:

Name: Source zone: Destination zone:

Below these forms is the 'Source NAT' section, which is currently empty with the message 'This section contains no values yet'.

At the bottom of the page, there is a 'Reset' button and 'Save' and 'Save & Apply' buttons.

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

The close-up shows the 'New forward rule' form with the following fields:

Name:

Source zone:

Destination zone:

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

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

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

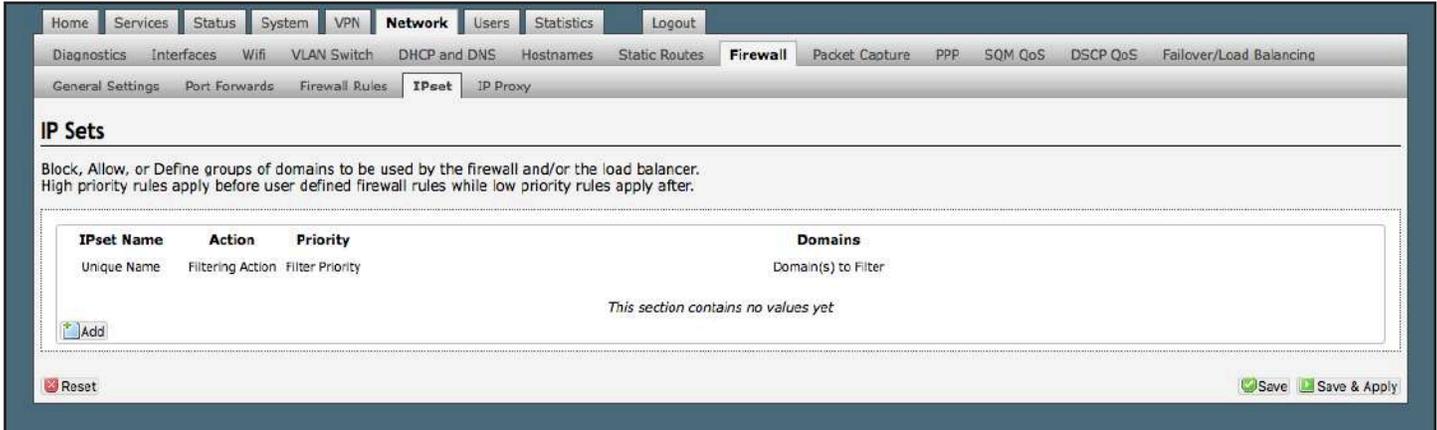
Make the Rules as desired, then click <Save & Apply>.

See IP Sets (**See Chapter 9.8.4**) for creating block and allow rules by domain name instead of IP address.

9.8.4. IP Sets

Requires “superadmin” login.

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.



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

Action Definitions:

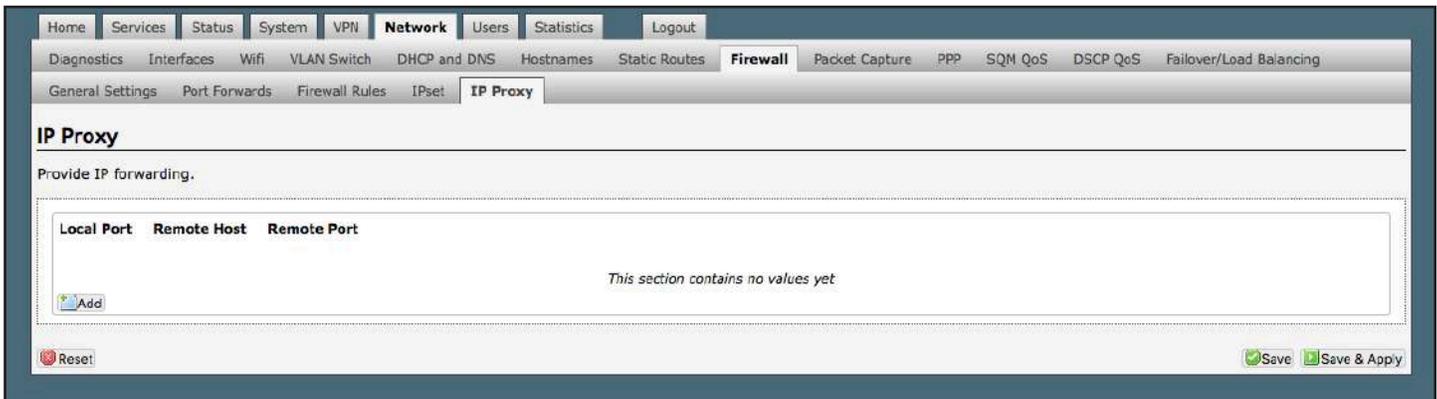
- **Block:** Rejects the domain.
- **Pass:** Allows the domain.
- **Define:** Defines the domain only. It neither blocks nor allows. You can specify how routing occurs for that domain in the Failover/Load Balancing Rules. (See Chapter 9.13).

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

Each IP set rule must be assigned to a Policy (See Chapter 9.13.2.4).

9.8.5. IP Proxy

Requires “superadmin” login.



9.9. Packet Capture

Requires “superadmin” login.



9.10. PPP

Requires “superadmin” login.

It is possible to use a USB connected satellite phone or LTE/GSM modem that does PPP to connect for email and web browsing (for example: IsatPhone Pro or Iridium handheld).

NOTE: web browsing is not recommended when using a low bandwidth device.

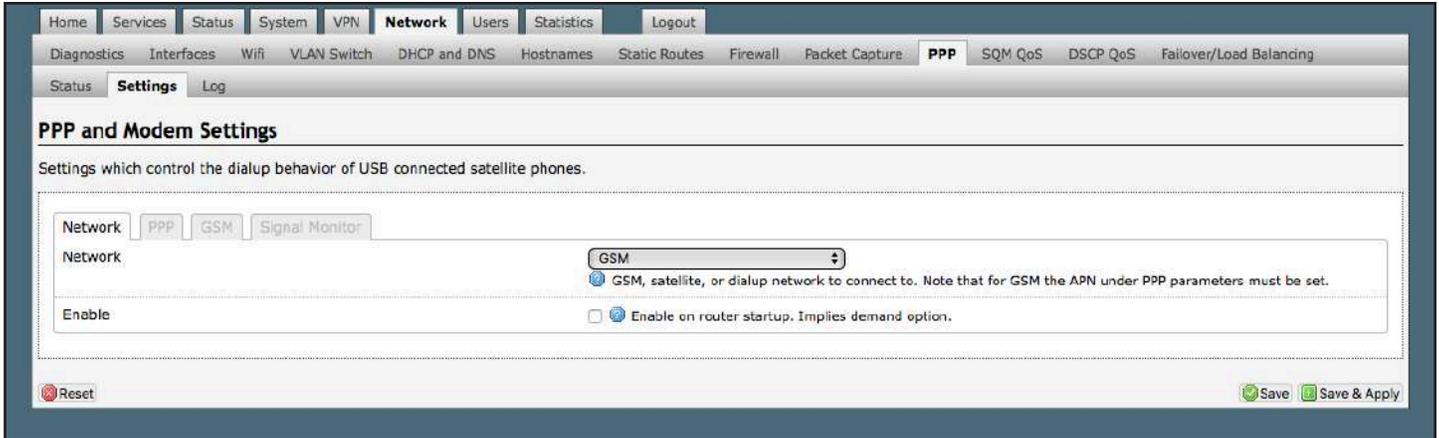


With PPP configured, you can bring up the connection manually; it will stay connected until you disconnect, or the idle timeout is reached. If not using the Demand feature, you must bring up the PPP connection manually. **See Chapter 9.8.1.**

9.10.1. PPP Settings Configuration for USB Connected Satellite Device

Requires “superadmin” login.

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



1. Using the drop-down menu, click the appropriate satellite network.



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

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

Move to the Settings > PPP Tab:

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

Network | **PPP** | GSM | Signal Monitor

Modem Interface: USB2
Select COM port assigned to modem.

Modem Speed: 921600
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 Persist.

Hold Off Timeout: 30
Time in seconds between reconnection attempts.

Maximum Fail: 0
Maximum reconnection fail attempts before giving up. set to 0 for infinite retries.

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.

Reset Save Save & Apply

Configure the PPP Settings as necessary. These PPP Settings apply to both USB connected satellite phones and LTE/GSM (cellular) modems. In addition, LTE/GSM equipped OEs will also require PPP Settings configuration.

- **Reset LTE/GSM Modem:** (Present within LTE/GSM capable OE)
- **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, three additional settings appear:

Demand	<input type="checkbox"/> Initiate the link only on demand, i.e. when data traffic is present. Implies Persist.
Hold Off Timeout	<input type="text" value="30"/> Time in seconds between reconnection attempts.
Maximum Fail	<input type="text" value="0"/> Maximum reconnection fail attempts before giving up. set to 0 for infinite retries.

- **Demand:** Check this box to bring up the link only on demand, such as when data traffic is present. The satphone or LTE/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.
- **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.
- **Best Practice:** When using LTE/GSM in the load-balancing mode, enable this Demand feature so that when there is PPP traffic the modem will go online, when no traffic the connection is terminated.
- **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.

Click <Save & Apply>.

9.10.2. PPP Settings Configuration for LTE/GSM Modems

Requires “superadmin” login.

The LTE/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 an LTE/GSM-based cellular phone, it may be possible to use the LTE/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 LTE/GSM-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 an LTE/GSM modem.

The screenshot shows the 'PPP and Modem Settings' page in the RedPort web interface. The breadcrumb trail is: Home > Services > Status > System > VPN > Network > Users > Statistics > Logout. The sub-menu is: Diagnostics > Interfaces > Wifi > VLAN Switch > DHCP and DNS > Hostnames > Static Routes > Firewall > Packet Capture > PPP > SQM QoS > DSCP QoS > Failover/Load Balancing. The page title is 'PPP and Modem Settings' with sub-headers 'Settings' and 'Log'. Below the title, it says 'Settings which control the dialup behavior of USB connected satellite phones.' There are three tabs: 'Network', 'PPP', 'GSM', and 'Signal Monitor'. The 'Network' dropdown menu is set to 'GSM'. Below it, there is a note: 'GSM, satellite, or dialup network to connect to. Note that for GSM the APN under PPP parameters must be set.' There is an 'Enable' checkbox which is currently unchecked, with a note: 'Enable on router startup. Implies demand option.' At the bottom left is a 'Reset' button, and at the bottom right are 'Save' and 'Save & Apply' buttons.

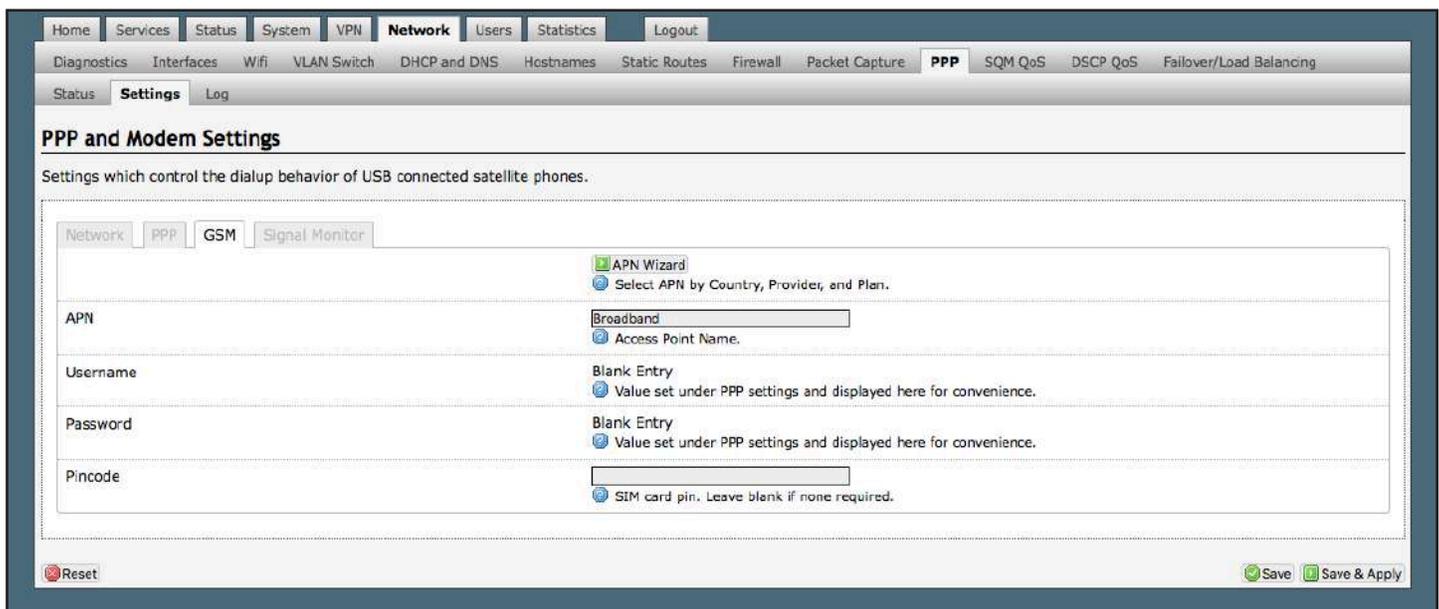
1. Using the drop-down menu, click GSM.



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

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

Move to the Settings > GSM Tab:



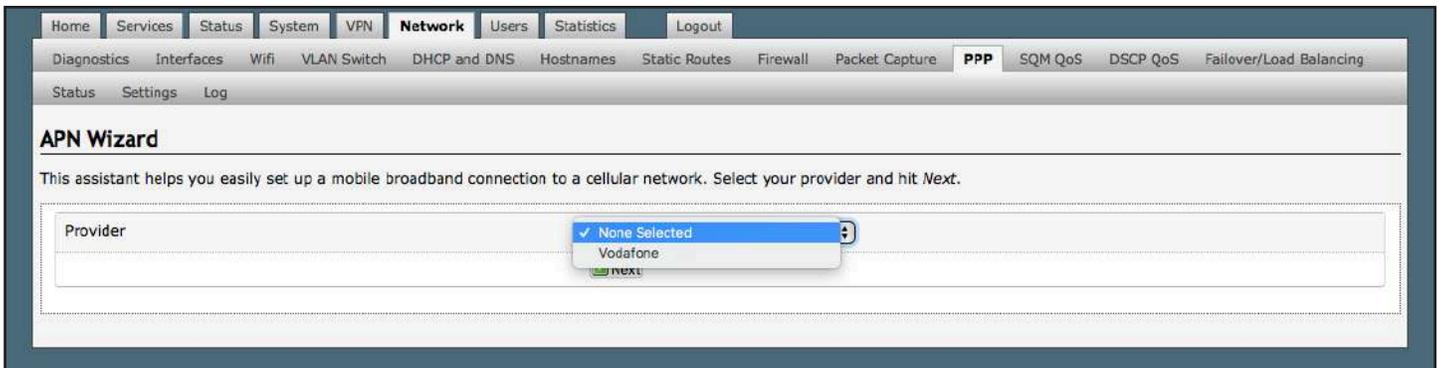
Before you can configure the Optimizer for LTE/GSM, you must:

- Obtain a USB data dongle from your cellular provider. Your provider may 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.

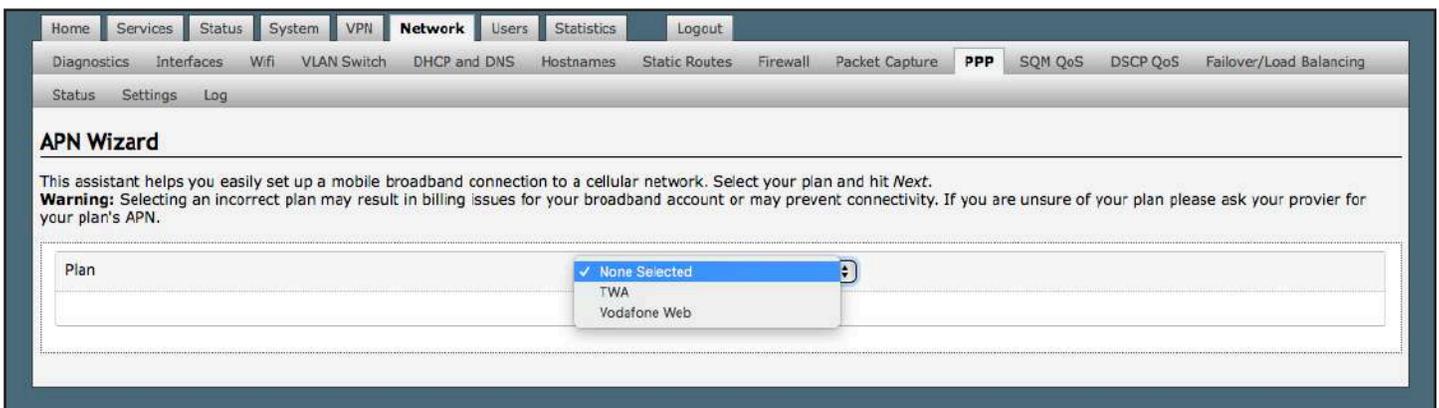
The APN Wizard contains many providers and plans. Using it will automatically set the configuration for you. Click <APN Wizard> to start the configuration:



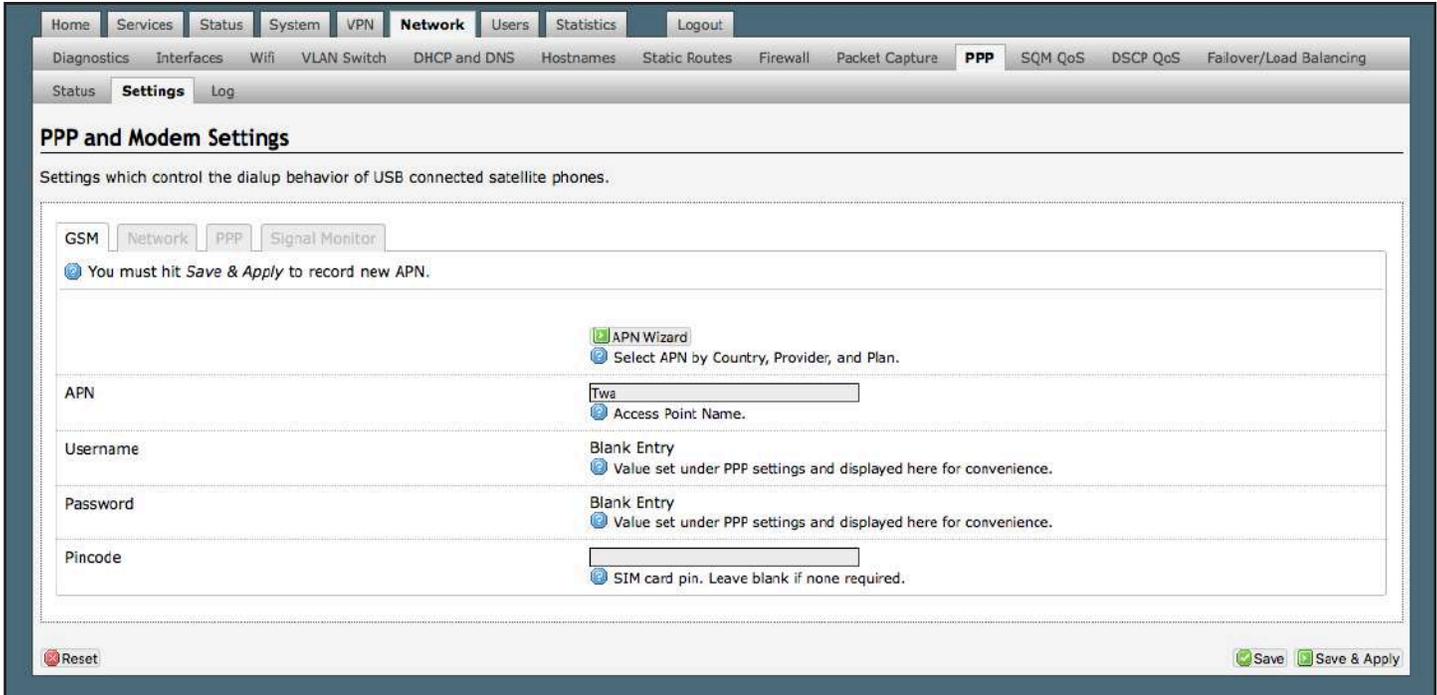
Select the appropriate country from the drop-down list and then, click <Next>.



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



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



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

Click <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 LTE/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 **Chapter 9.13** for additional PPP Settings.

9.10.2.1. Using LTE/GSM

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

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

With the LTE/GSM interface properly configured, it becomes an important component of the Failover sequence.

9.10.2.2. Changing from LTE/GSM service to satellite service

When you travel beyond LTE/GSM range you must:

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

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

9.10.2.3. LTE/GSM capable OE

Requires “superadmin” login.

RedPort Optimizer Enterprise with LTE/GSM capability routers have wireless hardware installed internally and have an externally accessible SIM Card slot. Using LTE/GSM capability will allow (when available) cellular data connections for Email, Web Browsing, and SIP phone calling from the router. You will get the benefits of compression and a faster transfer rate compared to a satellite connection which typically equates to cost savings.

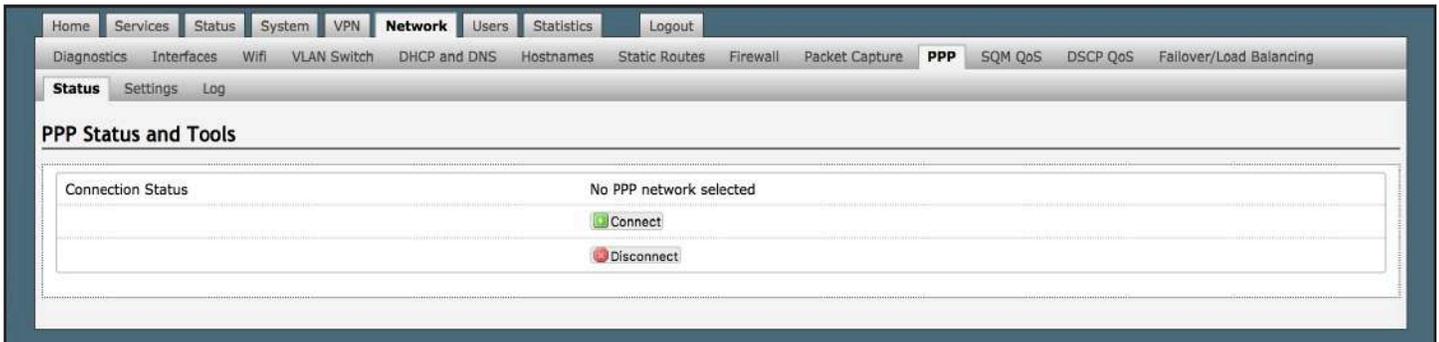
Some recommendations include:

- GSM or LTE SIM cards only, CDMA-based services will not work.
- Some LTE/GSM plans have restrictions and limitations or cost increases when used outside of home range (Country).
- SIM cards will need to be either “Standard” SIM card size or use a SIM card adapter for an ending “Standard” size card.
- Require use of SIM cards provisioned with HOTSPOT, MiFi, or Data capability. Some phone only SIM cards will work depending on Network provider limitations. Some Pre-paid cell phone SIM cards will not work.
- RedPort Global does not support LTE/GSM SIM card issues. The material provided is general in nature but may not be sufficient to establish a connection. If you have issues with the SIM card or connectivity you must contact your cellular network provider for support.

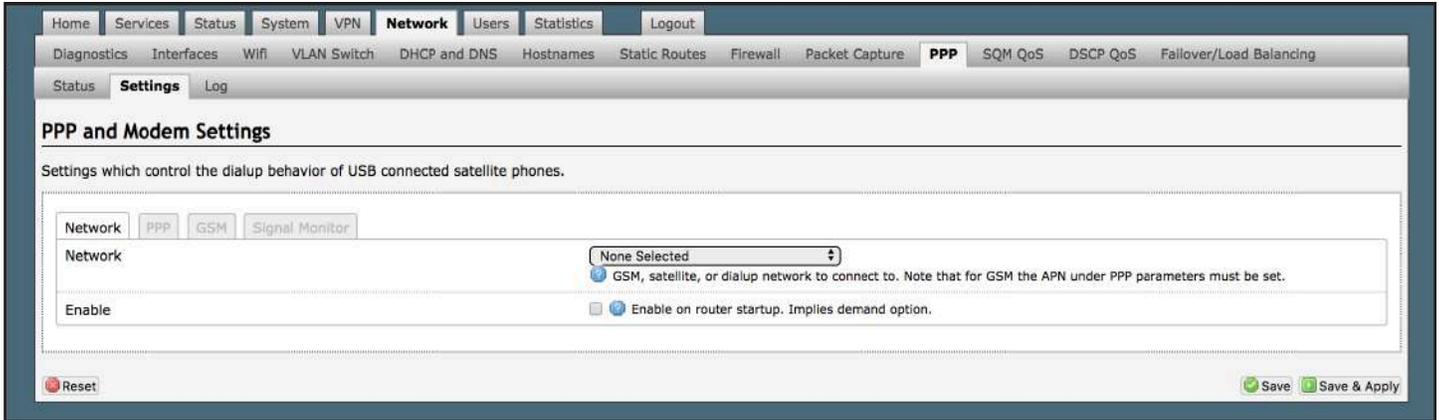
If you have a GSM-based or LTE-based cellular phone, it may be possible to use the LTE/GSM network, when available, for Email and Web Browsing data over the Optimizer. You will get the benefits of compression and a faster data transfer rate than over a satellite phone which typically equates to cost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

Use the following to configure the PPP interface for use with an LTE/GSM modem.

Navigate to <Network> tab, then to <PPP> tab, then to the <Status> tab.



Navigate to the <Settings> tab then to the <Network> tab.



1. Using the drop-down menu, click GSM.



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

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

Move to the <Settings> tab, then to the <PPP> Tab:

PPP and Modem Settings

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

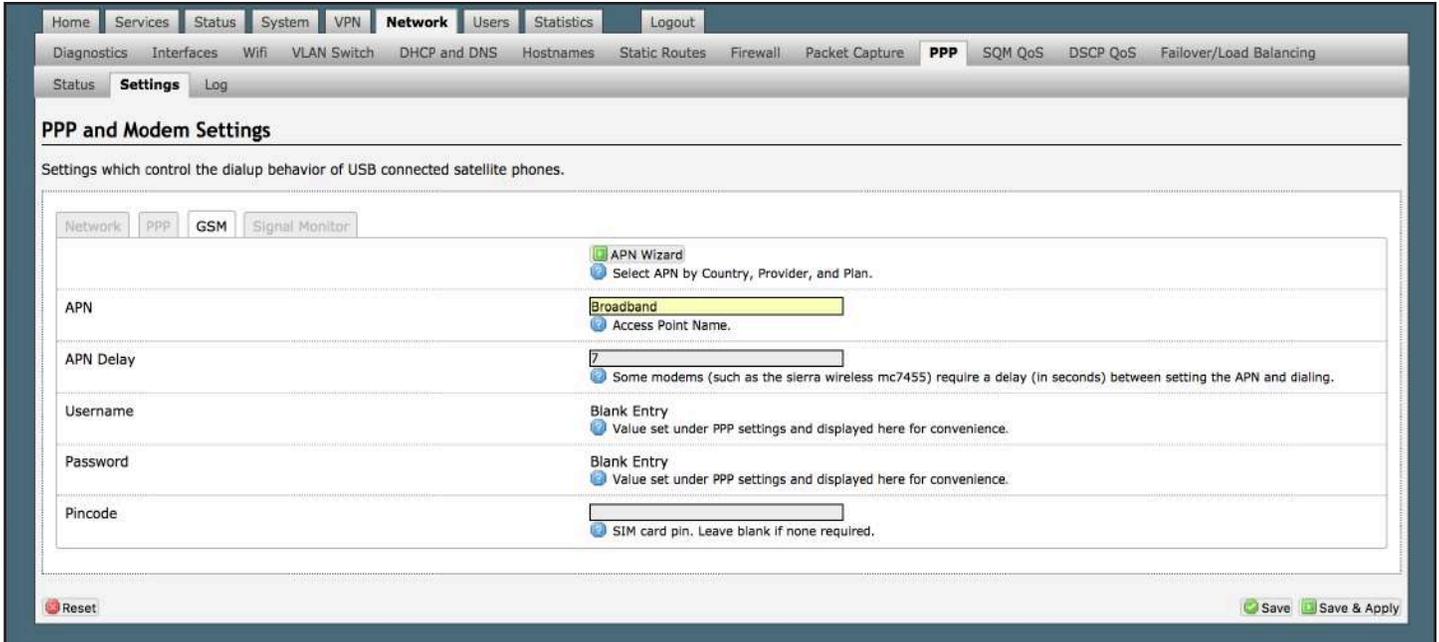
Network
PPP
GSM
Signal Monitor

Reset LTE Modem	<input type="button" value="Reset LTE Modem"/> <ul style="list-style-type: none"> ? Reset modem to factory defaults. This takes 60 seconds to execute.
Modem Interface	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">System Default</div> <ul style="list-style-type: none"> ? Select COM port assigned to modem.
Modem Speed	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">System Default</div> <ul style="list-style-type: none"> ? Baud rate for modem serial interface.
Username	<input style="width: 100%;" type="text"/> <ul style="list-style-type: none"> ? Leave blank if none required.
Password	<input style="width: 100%;" type="password"/> <ul style="list-style-type: none"> ? Leave blank if none required.
Phone Number	<input style="width: 100%;" type="text"/> <ul style="list-style-type: none"> ? Phone number to dial. Leave blank for system default.
Idle Timeout	<input style="width: 100%;" type="text" value="60"/> <ul style="list-style-type: none"> ? Drop connection after X seconds if no network traffic is detected. Note It is not advisable to use this option with the <i>persist</i> option without the <i>demand</i> option. Set to 0 to disable.
Persist	<input checked="" type="checkbox"/> ? Enable persistent connections. Persistent connections forces the modem to reconnect if connection drops.
Demand	<input checked="" type="checkbox"/> ? Initiate the link only on demand, i.e. when data traffic is present. Implies Persist.
Hold Off Timeout	<input style="width: 100%;" type="text" value="30"/> <ul style="list-style-type: none"> ? Time in seconds between reconnection attempts.
Maximum Fail	<input style="width: 100%;" type="text" value="0"/> <ul style="list-style-type: none"> ? Maximum reconnection fail attempts before giving up. set to 0 for infinite retries.
Extra Init	<input style="width: 100%;" type="text"/> <ul style="list-style-type: none"> ? Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before dialing.
MTU	<input style="width: 100%;" type="text"/> <ul style="list-style-type: none"> ? Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.
debug	<input checked="" type="checkbox"/> ? Write PPP connection debugging information to the system log.

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

4. Select the “Enable persistent connections.” This permits reconnection automatically if a connection is lost.
5. Select the “Initiate the link only on demand.” This causes the LTE/GSM to be started when there is a demand.
6. Click <Save & Apply>

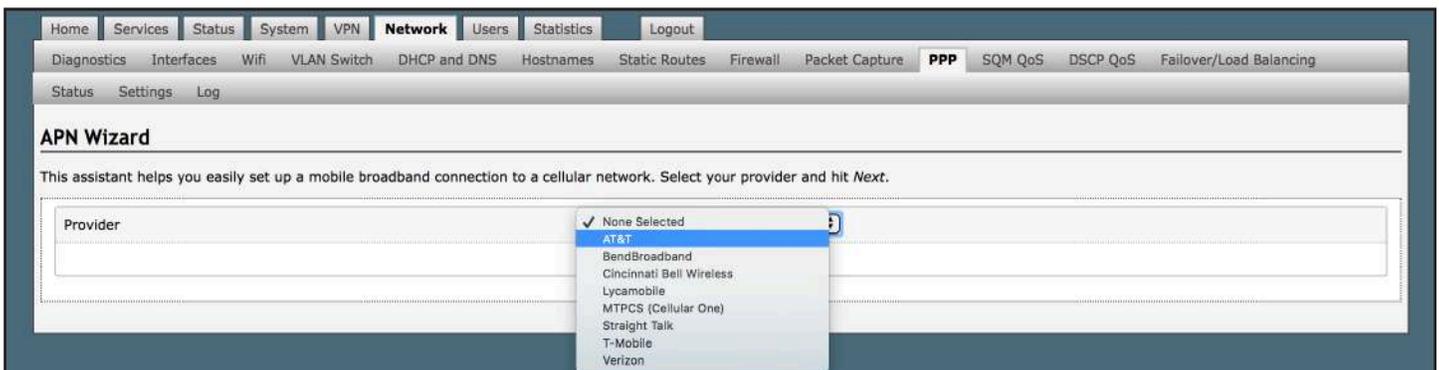
Navigate to the <Settings> tab, then to the <GSM> Tab:



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



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



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

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

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

10. Click <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.

When all actions are complete, navigating to the <Network> tab, then to the <PPP> tab, then to the <Status> tab will display the following:



With the GSM interface properly configured, it becomes an important component of the Failover sequence.

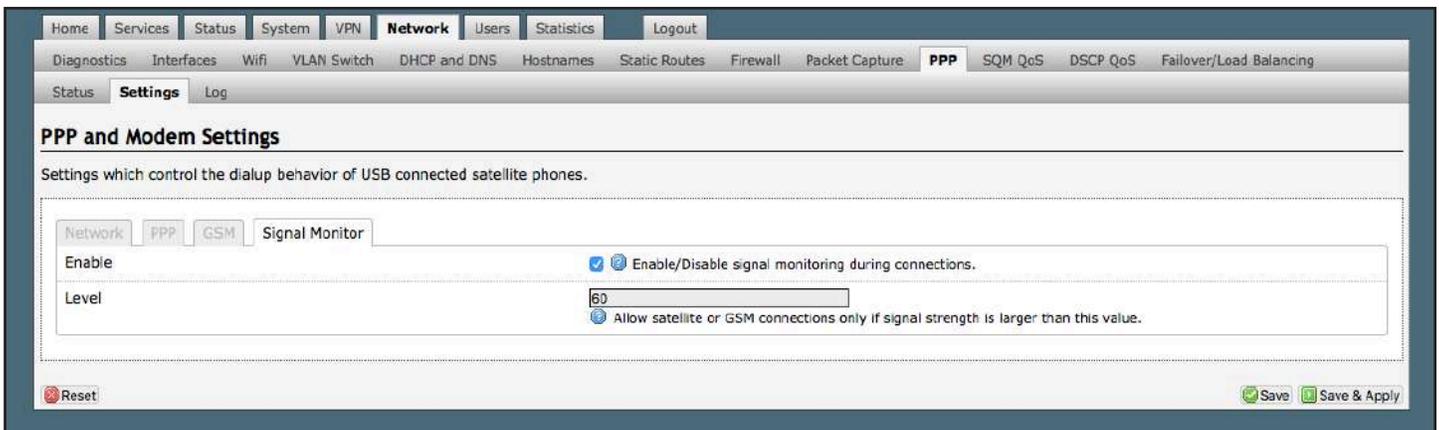
See **Chapter 9.13** for additional PPP Settings.

9.10.3. Signal Monitor

Requires “superadmin” login.

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.



From this screen you can enable or disable signal monitor using the “Enable/Disable signal monitoring during connections.” 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>.

9.11. SQM QoS

Requires “superadmin” login.

The screenshot shows the 'Smart Queue Management' configuration page in the RedPort interface. The navigation bar includes 'Home', 'Services', 'Status', 'System', 'VPN', 'Network', 'Users', 'Statistics', and 'Logout'. The sub-navigation bar includes 'Diagnostics', 'Interfaces', 'Wifi', 'VLAN Switch', 'DHCP and DNS', 'Hostnames', 'Static Routes', 'Firewall', 'Packet Capture', 'PPP', 'SQM QoS', 'DSCP QoS', and 'Failover/Load Balancing'. The main heading is 'Smart Queue Management'. Below it, a text block explains that with SQM, users can enable traffic shaping, better mixing (Fair Queuing), active queue length management (AQM), and prioritisation on one network interface. The 'Queues' section contains a form with tabs for 'Basic Settings', 'Queue Discipline', and 'Link Layer Adaptation'. The form includes:

- An 'Enable this SQM instance.' checkbox.
- An 'Interface name' dropdown menu set to 'eth1'.
- A 'Download speed (kbit/s) (ingress) set to 0 to selectively disable ingress shaping:' input field with the value '85000'.
- A 'shaping:' label.
- An 'Upload speed (kbit/s) (egress) set to 0 to selectively disable egress shaping:' input field with the value '10000'.
- A 'shaping:' label.
- A 'Create log file for this SQM instance under /var/run/sqm/\${Interface_name}.debug.log. Make sure to delete log files manually.' checkbox.
- A 'Verbosity of SQM's output into the system log.' dropdown menu set to 'info (default)'.

 At the bottom of the form are 'Add', 'Reset', 'Save', and 'Save & Apply' buttons.

9.12. DSCP QoS

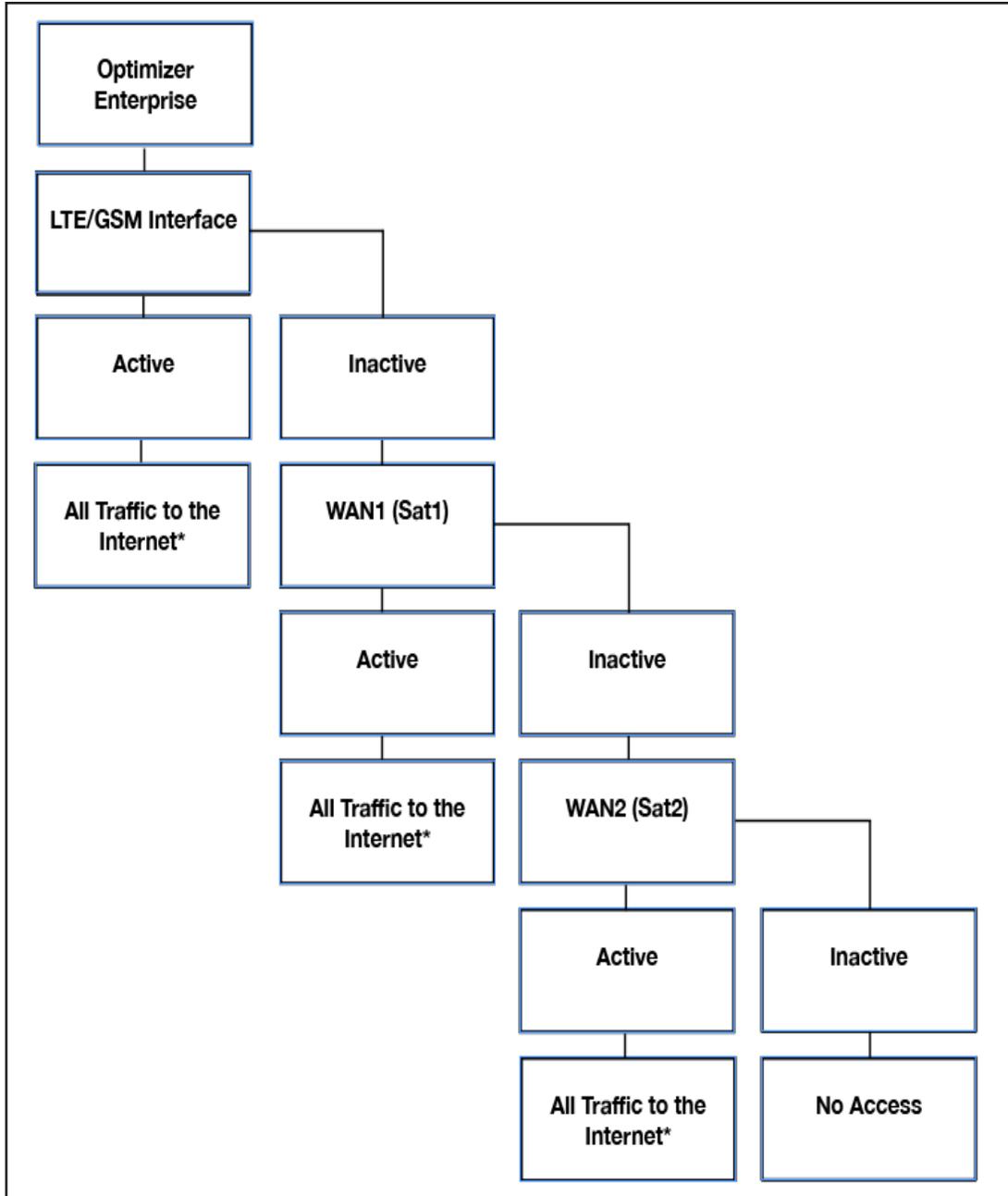
Requires “superadmin” login.

The screenshot shows the 'DSCP Rules' configuration page in the RedPort interface. The navigation bar and sub-navigation bar are identical to the previous screenshot. The main heading is 'DSCP Rules'. Below it, a text block explains that Differentiated services or DiffServ is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks. It also notes that DiffServ can be used to provide low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers. Further text explains that addresses can be network names, hostnames, or IP addresses with masks, and that masks of 24 are equivalent to 255.255.255.0. Ranges can be specified with '-' or ':' characters. Below the text is a table with the following columns: 'DSCP Value', 'Proto', 'Source IP', 'Source Port', 'Dest IP', 'Dest Port', and 'Comment'. The table is currently empty, with a message below it stating 'This section contains no values yet'. At the bottom of the table area are 'Add', 'Reset', 'Save', and 'Save & Apply' buttons.

DSCP Value	Proto	Source IP	Source Port	Dest IP	Dest Port	Comment
		IP/Net/Range	Port/Range	IP/Net/Range	Port/Range	

9.13. Failover/Load Balancing

The default Failover sequence and Load Balance configuration are as follows:



Setup is required for the LTE/GSM Interface.

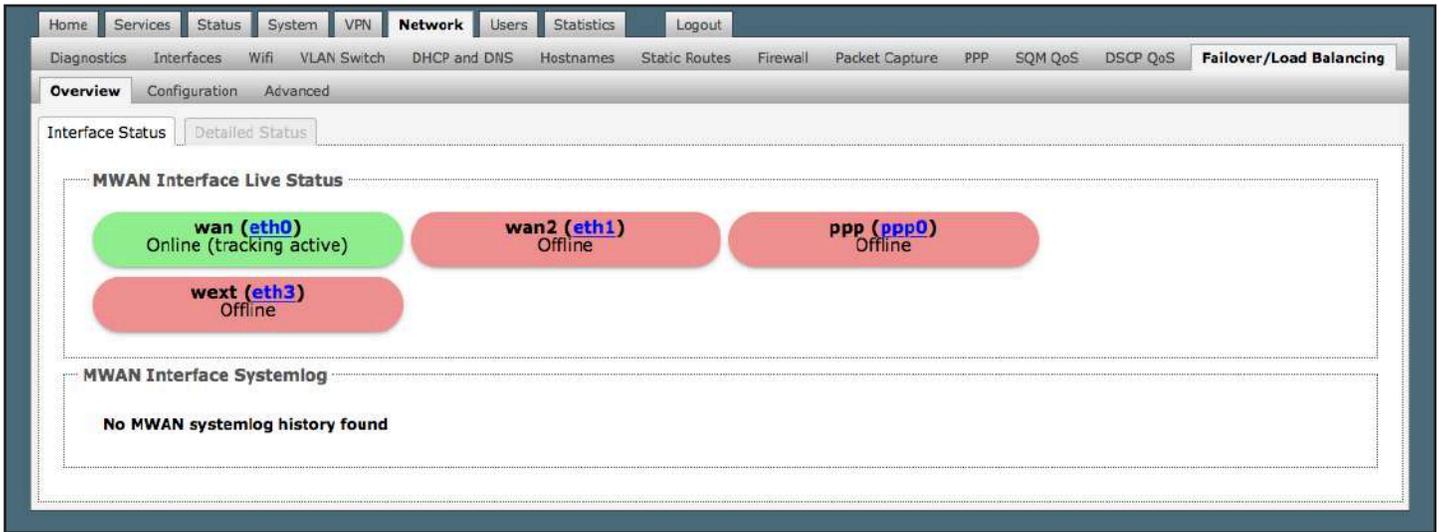
*All traffic to the Internet is subject to the firewall and the load balance configuration. You can change the Failover configuration and you can Load Balance between and among the interfaces. For example, you can create rules to send all http traffic through the LTE/GSM Interface but never through the WAN ports. See **Chapter 9.13.2** MWAN Configuration.

This default configuration will work out-of-the-box for those with a LTE/GSM connection and one or two satellite systems. If your setup differs from the default you will need to modify the Failover/Load Balancing configuration using the information in this chapter. There are examples of a few failover/load balancing configurations in **Chapter 9.13**.

9.13.1. MWAN Overview

The Interface Status screen shows you an at-a-glance view of which interfaces are currently online and which

interfaces are offline. In addition, the MWAN Interface System Log shows the most recent log entries.



The Detailed Status screen shows more details of the current state of the router.

The screenshot shows the RedPort Network Manager interface. The top navigation bar includes Home, Services, Status, System, VPN, Network (selected), Users, Statistics, and Logout. Below this is a secondary menu with Diagnostics, Interfaces, Wifi, VLAN Switch, DHCP and DNS, Hostnames, Static Routes, Firewall, Packet Capture, PPP, SQM QoS, DSCP QoS, and Failover/Load Balancing. The main content area is titled 'Overview' and has sub-tabs for 'Interface Status' and 'Detailed Status'. The 'Detailed Status' tab is active, displaying the 'MWAN Detailed Status' section. This section contains the following text:

```

Interface status:
interface wan is online (tracking down)
interface wan2 is offline (tracking down)
interface ppp is offline (tracking down)
interface wext is offline (tracking down)

Policy balanced:
wan (100%)

Policy gsm_sat_sat2:
wan (100%)

Policy sat2_only:
unreachable

Policy sat2_sat:
wan (100%)

Policy sat_only:
wan (100%)

Policy sat_sat2:
wan (100%)

Policy wi_gsm:
unreachable

Policy wi_gsm_sat_sat2:
wan (100%)

Known networks:
10.1.5.0/24
192.168.10.0
127.0.0.0/8
192.168.0.79
192.168.90.0
192.168.90.0/24
10.1.5.1
10.1.5.0
192.168.10.1
192.168.0.255
192.168.10.255
127.0.0.1
192.168.0.0
192.168.0.0/24
127.0.0.0
192.168.0.254
192.168.90.1
224.0.0.0/3
192.168.90.255
127.255.255.255
10.1.5.255
192.168.10.0/24

Active rules:
504 38860 - wi_gsm_sat_sat2 all -- * * 0.0.0.0/0 0.0.0.0/0
    
```

9.13.2. MWAN Configuration

Requires “superadmin” login.

The Optimizer Enterprise offers sophisticated Failover and Load Balancing options. You can block or allow certain traffic over one or more specific interfaces.

First, let’s define the various components discussed in this section:

- **MWAN Interfaces:** This is the connection “type” to the Internet. The default is four interfaces.
- **MWAN Members:** These are profiles whereby each interface is assigned a level of importance relative to the other interfaces. The default is 16 members.
- **MWAN Policies:** These are member groupings that control how traffic is distributed among the interfaces. The default is 7 policies.
- **MWAN Rules:** These are rules that specify which traffic will use a particular interface. The default is 1 rule.

9.13.2.1. Interfaces

Requires “superadmin” login.

MWAN Interface Configuration

There are currently 3 of 250 supported interfaces configured

WARNING: some interfaces have no default route in the main routing table!

WARNING: some interfaces have no metric configured in /etc/config/network!

Interfaces

MWAN supports up to 250 physical and/or logical interfaces
 MWAN requires that all interfaces have a unique metric configured in /etc/config/network
 Names must match the interface name found in /etc/config/network (see advanced tab)
 Names may contain characters A-Z, a-z, 0-9, _ and no spaces
 Interfaces may not share the same name as configured members, policies or rules

Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort
wan	Yes	8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4	1	1	2s	5s	3	3	10		
wan2	Yes	8.8.8.8 8.8.4.4 208.67.220.220	1	1	2s	10s	3	3	20		
ppp	Yes	8.8.8.8 8.8.4.4 208.67.220.220	1	1	2s	5s	3	3	—		

An MWAN Interface represents the connection type to the Internet. The default interfaces are:

- **wan:** The primary satellite device.
- **wan2:** The backup satellite device.
- **ppp:** The LTE/GSM device.

If you have added a new interface to Network > Interfaces (**See Chapter 9.2.2**) and want to include that new interface into the MWAN Failover/Load Balancing distribution it must be added to the MWAN Interface Configuration:

Enter the name of the interface into the text box and click <Add>.

You may accept these settings as they are or modify if required.

- **Enabled:** Select Yes to Enable or select No to Disable this MWAN interface. The default is “Yes”.
- **Tracking IP:** The IP address(or addresses) to be pinged to determine if the link is up or down. If left blank, it is assumed the interface is always online.

NOTE: In some cases, it may be advantageous and more cost effective to track the IP address of the interface itself rather than an IP address on the Internet.

- **Tracking reliability:** Number of IP addresses (in Tracking IP above) that must respond in order for the link to be determined as Up. The default is “1”.
- **Ping count:** Number of pings to be sent in the ping burst. The default is “1”.
- **Ping timeout:** How long (in seconds) to wait to see if the ping fails. The default is “2”. Iridium Pilot users please see suggestions below.
- **Ping interval:** How long (in seconds) to wait between pings. Iridium Pilot users please see suggestions below.
- **Interface down:** Number of failed responses before determining that the interface is Down.
- **Interface up:** Number of successful responses before determining that the interface is Up.
- **Metric:** Read-only display of the gateway metric assigned to the interface when it was created in Network > Interfaces. **See Chapter 9.2.**

Click <Save & Apply>.

Some suggestions:

When you have a PPP interface in the failover sequence you may want to set the Ping Timeout to 10 seconds, set the Ping Count to 2. The PPP interface has to come up at least once, so the system knows that it is a viable interface, so it must ping at least once. In addition, you may want to change the Tracking IP to the IP of the router, so you are pinging yourself instead of pinging an address on the Internet.

For Iridium Pilot Users:

The default settings for wan2 is Ping Timeout = 5 seconds and Ping Interval = 1 minute. This is designed to keep bandwidth usage low. If you have an Iridium Pilot as your wan2 interface, however, these settings are not helpful because the Pilot automatically goes offline after 20 seconds of idle time and it takes about 10-15 seconds to bring it back online. Doing a ping every minute with a 5 second timeout is most likely to fail. Changing the Tracking IP to the IP Address of the Pilot unit itself assures that the ping will always work so the interface will show as available for failover. With wan2 at the end of your failover sequence, this tricks the Optimizer into believing there is connectivity, minimizing bandwidth usage.

MWAN interface Configuration

There are currently 5 of 250 supported interfaces configured

WARNING: some interfaces have no default route in the main routing table!

WARNING: some interfaces are configured incorrectly or not at all in /etc/config/network!

WARNING: some interfaces have no metric configured in /etc/config/network!

Interfaces

MWAN supports up to 250 physical and/or logical interfaces
 MWAN requires that all interfaces have a unique metric configured in /etc/config/network
 Names must match the interface name found in /etc/config/network (see advanced tab)
 Names may contain characters A-Z, a-z, 0-9, _ and no spaces
 Interfaces may not share the same name as configured members, policies or rules

Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort
wan	Yes	8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4	1	1	2s	5s	3	3	10		
wan2	Yes	8.8.8.8 8.8.4.4 208.67.220.220	1	1	2s	10s	3	3	20		
ppp	Yes	8.8.8.8 8.8.4.4 208.67.220.220	1	1	2s	5s	3	3	—		
wext	Yes	8.8.8.8 8.8.4.4 208.67.222.222 208.67.220.220	1	1	2s	5s	3	3	5		
NewADf	Yes	—	—	—	—	—	—	—	—		

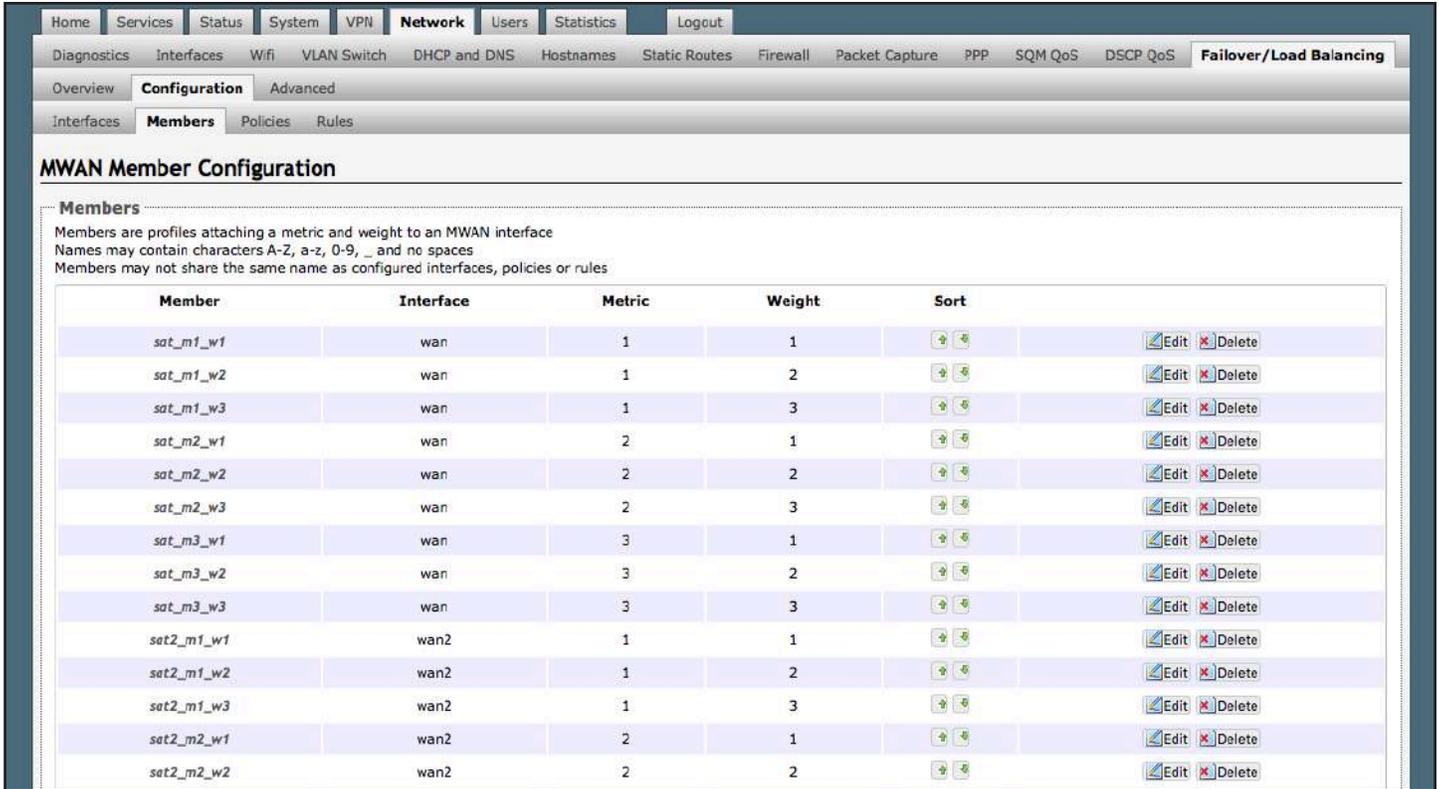
The new MWAN Interface is now available for Failover/Load Balancing configuration.

Use the <Edit> button to edit a MWAN Interface.

Use the <Delete> button to remove a MWAN Interface. The Delete action cannot be undone.

9.13.2.2. Members

Each MWAN Interface should have one or more Member profiles.



There are 16 default Members (four profiles for each of the four default interfaces).

Each Member is assigned a Metric and a Weight.

The Metric hierarchy is lowest number to highest number; therefore Metric 1 (m1) has a higher standing than Metric 2 (m2), etc.

The Weight hierarchy is the reverse; highest number to lowest number; therefore Weight 4 (w4) has a higher standing than Weight 3 (w3), etc.

Metric and Weight play an important role in controlling the distribution of traffic.

9.13.2.3. Creating New Member

Requires “superadmin” login.

To add a new Member, enter the Member name in the text box and click <Add>.



When creating new Members, it is a good idea to include the metric number and weight number in the Member name for easy identification on the page.

Select the MWAN Interface associated with this Member and assign a Metric (1-4) and a Weight (4-1).

MWAN Policy Configuration - NewMbrAD1_M1_W1

Member used:

Last resort: ne use this behavior for matched traffic

Currently Configured Members

--

Select the MWAN Interface associated with this Member and assign a Metric (1-4) and a Weight (4-1).

MWAN Policy Configuration - NewMbrAD1_M1_W1

Member used:

Last resort: ne use this behavior for matched traffic

Currently Configured Members

--

Click <Save & Apply>.

The new Member now appears on the list.

NewMbrAD1_M1_W1	sat_m1_w1	unreachable (reject)			Edit Delete
-----------------	-----------	----------------------	--	--	--------------

Click <Edit> button to edit a Member.

Click <Delete> button to remove a Member. The Delete action cannot be undone.

9.13.2.4. Policies

Requires “superadmin” login.

Policies are groupings of members. Each policy must have one or more members. As you create Rules (**See Chapter 9.8.3**) you must assign the rule to one of these policies.

These policies will be used to control how MWAN distributes traffic.

There are 7 default Policies:

Policies

Policies are profiles grouping one or more members controlling how MWAN distributes traffic
 Member interfaces with lower metrics are used first. Interfaces with the same metric load-balance
 Load-balanced member interfaces distribute more traffic out those with higher weights
 Names may contain characters A-Z, a-z, 0-9, _ and no spaces. Names must be 15 characters or less
 Policies may not share the same name as configured interfaces, members or rules

Policy	Members assigned	Last resort	Errors	Sort
sat_only	sat_m1_w1	unreachable (reject)		
sat2_only	sat2_m1_w1	unreachable (reject)		
sat_sat2	sat_m1_w1 sat2_m2_w1	unreachable (reject)		
sat2_sat	sat2_m1_w1 sat_m2_w1	unreachable (reject)		
balanced	sat_m1_w1 sat2_m1_w1	unreachable (reject)		
gsm_sat_sat2	ppp_m1_w1 sat_m2_w1 sat2_m3_w1	unreachable (reject)		
wi_gsm_sat_sat2	wext_m1_w1 ppp_m2_w1 sat_m3_w1 sat2_m4_w1	unreachable (reject)		
wi_gsm	wext_m1_w1 ppp_m2_w1	unreachable (reject)		
NewMbrAD1_M1_W1	sat_m1_w1	unreachable (reject)		

Reset Save Save & Apply

When there is only one Member assigned to a Policy, all traffic matching the Rule will flow through the one interface.

sat2_only	sat2_m1_w1	unreachable (reject)		
-----------	------------	----------------------	--	--

When multiple Members are assigned to a policy, the traffic will be distributed based on the Metric and Weight of the Members assigned.

balanced	sat_m1_w1 sat2_m1_w1	unreachable (reject)		
----------	-------------------------	----------------------	--	--

gsm_sat_sat2	ppp_m1_w1 sat_m2_w1 sat2_m3_w1	unreachable (reject)		
--------------	--------------------------------------	----------------------	--	--

Here are some examples:

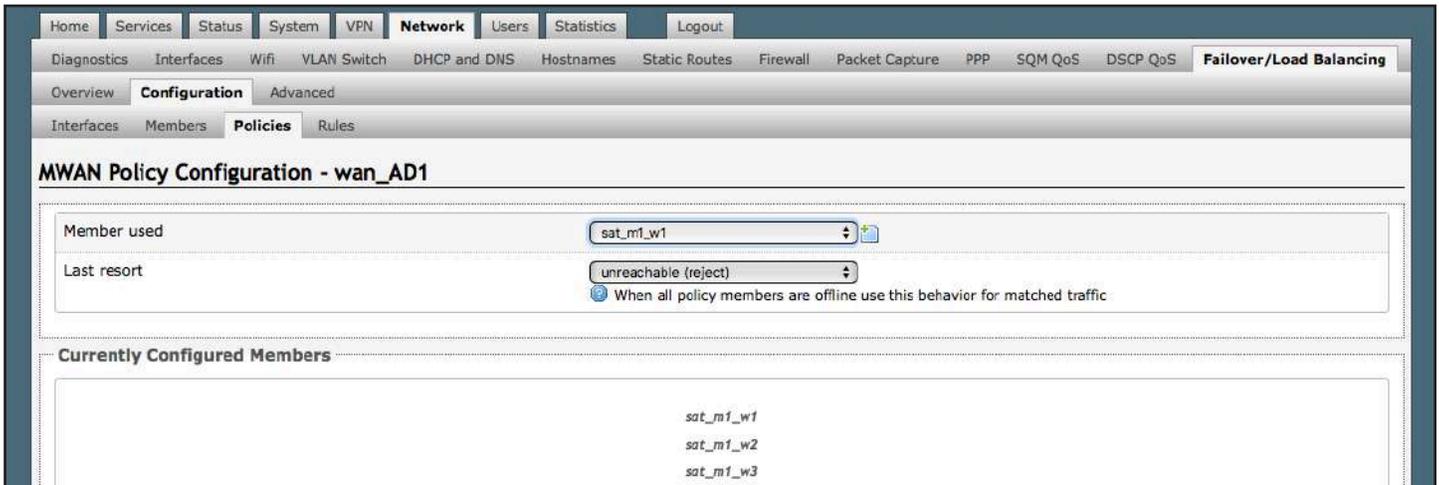
- **balanced:** Because the Metric is 1 for both Member profiles, 1/2 the traffic will flow through the wan interface and 1/2 the traffic will flow through the wan2 interface.
- **wan_wan2:** Because the Metric is 1 for the wan and the Metric is 2 for the wan2 and the Weight is 1 for both; all traffic will flow through the wan interface if it is Active. If the wan interface is not available, the traffic will automatically failover to the wan2 interface.
- **wan2_wan:** This policy is the reverse of the one above. All traffic will flow through the wan2 interface if it is active and if not, it will failover to the wan interface.
- **wan_heavy:** This example is not on the default list but helps further explain how Metric and Weight are applied. In the fictional Policy “wan_heavy” there are two Members assigned to it: “wan_m1_w4” and “wan2_m1_w1”. This looks a lot like the balanced policy, however, because the Weight value is higher for the wan interface

(w4) than it is for the wan2 interface (w1), the wan interface will pass more traffic than the wan2 interface. On average, for every four packets that flow through the wan, only one packet will flow through the wan2.

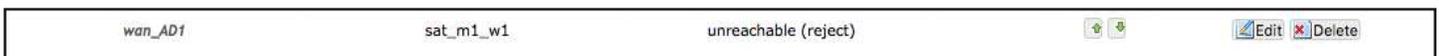
To add a new Policy, enter the new Policy name in the text box and click <Add>.

A screenshot of a web interface showing a text input field with the text 'wan_AD1' and an 'Add' button to its right. The input field is highlighted with a blue border.

Using the drop-down list, select one or more Members to assign to the new Policy in accordance with how you want traffic distributed when a Rule invokes this Policy. Click <Save & Apply>.

A screenshot of a web interface showing the 'MWAN Policy Configuration - wan_AD1' page. The page has a navigation bar with tabs for Home, Services, Status, System, VPN, Network, Users, Statistics, and Logout. Below the navigation bar are several sub-tabs: Diagnostics, Interfaces, Wifi, VLAN Switch, DHCP and DNS, Hostnames, Static Routes, Firewall, Packet Capture, PPP, SQM QoS, DSCP QoS, and Failover/Load Balancing. The main content area shows the 'Configuration' tab selected, with sub-tabs for Overview, Configuration, and Advanced. Under 'Configuration', there are sub-tabs for Interfaces, Members, Policies, and Rules. The 'Policies' sub-tab is active, showing the configuration for 'wan_AD1'. The configuration includes a 'Member used' dropdown menu set to 'sat_m1_w1', a 'Last resort' dropdown menu set to 'unreachable (reject)', and a checkbox for 'When all policy members are offline use this behavior for matched traffic'. Below the configuration is a section titled 'Currently Configured Members' which lists 'sat_m1_w1', 'sat_m1_w2', and 'sat_m1_w3'.

The new Policy now appears on the list. Notice that when this Policy is used traffic will be balanced between wan interface and the db1 interface.

A screenshot of a table listing policies. The table has four columns: Policy Name, Member, Last resort, and Actions. The first row shows 'wan_AD1', 'sat_m1_w1', 'unreachable (reject)', and 'Edit Delete'.

Click <Edit> to edit a Policy.

Click <Delete> to remove a Policy. The Delete action cannot be undone.

9.13.2.5. Rules

Requires “superadmin” login.

Rules allow you flexibility in the distribution of MWAN traffic. They can be based on IP address, port, or protocol.

Rules are matched from top to bottom. When a Rule is matched, the rules below that match are ignored. If traffic does not match any rule, it is routed to the main routing table. (The main routing table can be found in under the Status Tab > Routes.) If traffic does match a rule, but the interface is down for that policy, the traffic will be blackholed.

There is one default rule:

MWAN Rule Configuration

Traffic Rules

Rules specify which traffic will use a particular MWAN policy based on IP address, port or protocol
 Rules are matched from top to bottom. Rules below a matching rule are ignored. Traffic not matching any rule is routed using the main routing table
 Traffic destined for known (other than default) networks is handled by the main routing table. Traffic matching a rule, but all WAN interfaces for that policy are down will be blackholed
 Names may contain characters A-Z, a-z, 0-9, _ and no spaces
 Rules may not share the same name as configured interfaces, members or policies

Rule	Source address	Source port	Destination address	Destination port	Protocol	Sticky	Sticky timeout	IPset	Policy assigned	Errors	Sort
default_rule	—	—	0.0.0.0/0	—	all	No	—	—	wi_gsm_sat_sat2		
<input type="text" value=""/>											

With this Default Rule, any traffic FROM any source and TO any destination (i.e. ALL traffic) will use the Policy “wi_gsm_sat_sat2”.

Taking a look at the Policy “wi_gs_w_w2” we can see the Members assigned to this policy and determine the failover/load balancing sequence. Because the Weight value is 1 (w1) for each Member this means that all traffic will be routed through the “wext” interface if it is up. If “wext” is down, all traffic will be routed through the “ppp” interface if it is configured and up. If the “ppp” interface is down, then all traffic will be routed through the “wan” interface, if it is up. If the “wan” interface is down, then all traffic will be routed through the “wan2” interface, if it is up. If the “wan2” interface is down, then all traffic will be blackholed. If the Weight values varied traffic would be allocated among the interfaces in accordance with the Weight values assigned to the Members.

MWAN Policy Configuration - wi_gsm_sat_sat2

Member used

- wext_m1_w1
- ppp_m2_w1
- sat_m3_w1
- sat2_m4_w1

Last resort

unreachable (reject)

When all policy members are offline use this behavior for matched traffic

MWAN Rule Configuration - AD_rule

Source address: Supports CIDR notation (eg "192.168.100.0/24") without quotes

Source port: May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes

Destination address: Supports CIDR notation (eg "192.168.100.0/24") without quotes

Destination port: May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes

Protocol: View the contents of /etc/protocols for protocol descriptions

Sticky: Traffic from the same source IP address that previously matched this rule within the sticky timeout period will use the same WAN interface

Sticky timeout: Seconds. Acceptable values: 1-1000000. Defaults to 600 if not set

IPset: Name of IPset rule. Requires IPset rule created under [Network->Firewall->IPset](#)

Policy assigned:

Currently Configured Policies

Complete this screen in accordance with the Rule you want to create:

- **Source address:** Restrict incoming traffic arriving from a specific IP address or range.
- **Source port:** Restrict incoming traffic arriving from a certain port or multiple ports.
- **Destination address:** Restrict outgoing traffic to a specific IP address or range.
- **Destination port:** Restrict outgoing traffic to a specific port or multiple ports.
- **Protocol:** Restrict only traffic of a certain protocol, select from the drop-down list, or select -- custom-- and enter the protocol here.
- **Sticky:** This is important for smooth traffic flow when load-balancing among interfaces with different Weight values. With <Yes> selected, once connected, the same interface will be used for that traffic up to the Sticky Timeout period.
- **Sticky Timeout:** This is like an idle timeout period. If Sticky is set to <Yes> above, Sticky Timeout represents the number of seconds the system will wait for more traffic to flow through the specific interface. Once the Sticky Timeout period is reached it will revert back to the original load balance configuration.
- **IPset:** If you have an IPset defined in Network > Firewall > IPset (**See Chapter 9.8.4**), you can restrict traffic to that location by selecting the IPSet rule from the drop-down list.
- **Policy assigned:** Select which Policy you want this Rule assigned to using the drop-down menu. Every Rule MUST be assigned to a Policy.

Click <Save & Apply>.

Rule	Source address	Source port	Destination address	Destination port	Protocol	Sticky	Sticky timeout	IPset	Policy assigned	Errors	Sort
default_rule	—	—	0.0.0.0/0	—	all	No	—	—	wi_gsm_sat_sat2		
AD_rule	—	—	—	—	all	No	—	—	—		
<input type="text"/>											

The new rule now appears on the list. This Rule will never allow Facebook traffic over the wan2 interface. However, in order for the Rule to apply, it must be moved up the list using the Sort Up button so that it appears before the default rule that allows all traffic.

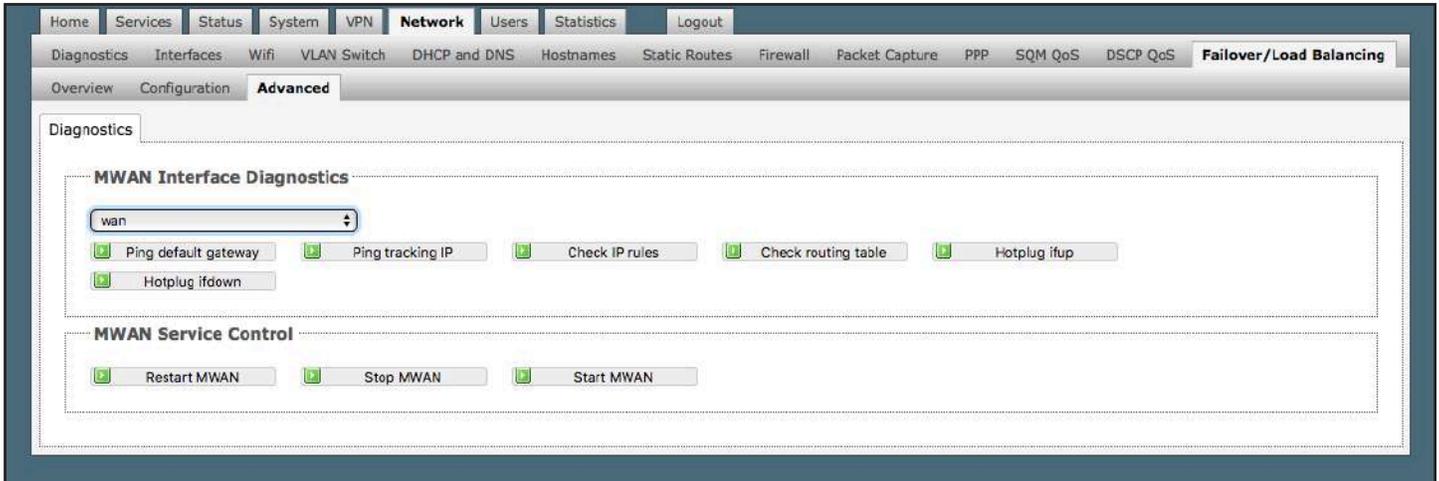
Click <Edit> to edit a Rule.

Click <Delete> to remove a Rule. The Delete action cannot be undone.

9.13.3. Advanced

Requires “superadmin” login.

Select the MWAN Interface using the drop-down list and run diagnostics for that interface.

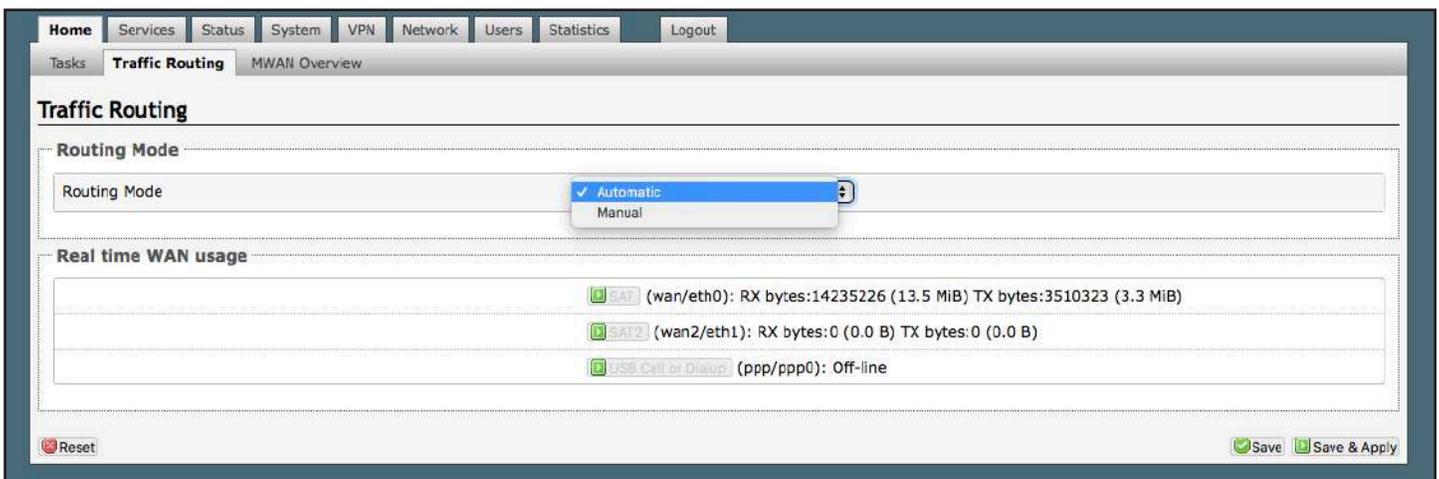


Use MWAN Service Control to manually bring up or take down interfaces.

9.13.4. Failover Mode - Automatic or Manual

Requires “superadmin” login.

There are two Failover modes available:



Automatic Failover (default setting) requires no intervention; if a MWAN interface is unavailable, traffic will automatically be routed per the Failover/Load Balancing Rules. Real time WAN usage is also displayed on this screen.

Manual Failover requires the “superadmin” or “admin” to select which available interface to use for ALL traffic. Real

time WAN usage is also displayed on this screen. Only available interfaces can be enabled. Unavailable interfaces with no route to the Internet are disabled. Only one can be selected. The “Default Route” designation indicates which interface is currently routing traffic.

Some Important Things to Know:

- Only the ‘superadmin’ login can change the Failover Traffic Routing mode.
- The “admin” login displays the Failover Traffic Routing mode as read-only.
- Real time usage for each interface is displayed in either automatic or manual mode.
- The currently selected Default Route only displays in Manual mode.
- When set to Manual mode both “superadmin” and “admin” logins can select which interface to use for routing.

9.13.5. Failover/Load Balancing Scenarios

The scenarios below represent some commonly requested configurations.

9.13.5.1. Scenario 1

SatCom setup is a FleetBroadband Terminal, a handheld satphone like an Iridium 9555 and GSM.

A more useful Failover configuration may be: GSM >FBB > PPP.

1. Configure the PPP interface for the Iridium 9555 satphone under Network > PPP (**See Chapter 9.2**).
2. Connect the Iridium satphone to the Optimizer Enterprise’s USB port with the appropriate cable.
3. Create a MWAN Policy in Network > Failover/Load Balancing > Configuration > Policies (**See Chapter 9.13.2.4**).

The Policy might be named “wext_wan_ir”.

The Members Assigned should be “wext_m1_w1”, “wan_m1_w1” and “ppp_m1_w1”.

4. Create a MWAN Rule in Network > Failover/Load Balancing > Configuration > Rules (**See Chapter 9.13.2**). Give the rule a unique name.

When defining the Rule, the only field that requires an entry is the Policy Assigned field. Select the Policy name that you created in step 3 “wext_wan_ir”.

5. Move this new Rule to the top of the list using the Sort Up button.

With this setup, all traffic will flow through the GSM, if it is up. If the GSM is not up, all traffic will flow through the FleetBroadband satellite terminal, if it is up. If the FBB is not up, all traffic will flow through the Iridium 9555.

9.13.5.2. Scenario 2

Allow all http traffic through the GSM interface only and never through the satellite terminal.

Use the following to restrict all http traffic to the GSM interface only.

1. Create a MWAN Policy in Network > Failover/Load Balancing > Configuration > Policies (**See Chapter 9.13.2**).

The Policy might be named “gsmonly”.

The Members Assigned should be “wext_m1_w1”.

Last resort should be set to “reject” as you do not want the last resort to route through the default rule.

2. Create a MWAN Rule in Network > Failover/Load Balancing > Configuration > Rules (See **Chapter 9.13.2**). Give the rule a unique name. When defining the Rule, set:
Destination Port = 80,443 Protocol = tcp.
Policy Assigned = select the Policy name that you created in step 1 “gsmonly”.

3. Move this new Rule to the top of the list using the Sort Up button.

With this setup, all http traffic (i.e. port 80 and port 443) will flow through the LTE/GSM interface only, if it is up. If the LTE/GSM is not up, all http traffic will be rejected.

9.13.5.3. Block Skype or other P2P applications

Skype and other Peer-to-Peer Applications are designed to circumvent firewalls allowing users to communicate and share data. They consume a lot of satellite airtime resources and are very difficult to block. In order to block Skype or other Peer-to-Peer Applications you must configure the firewall to block all traffic and then route all http and https traffic through Optimizer Enterprise Proxy Server that allows you to Block sites. The Captive Portal must be Enabled.

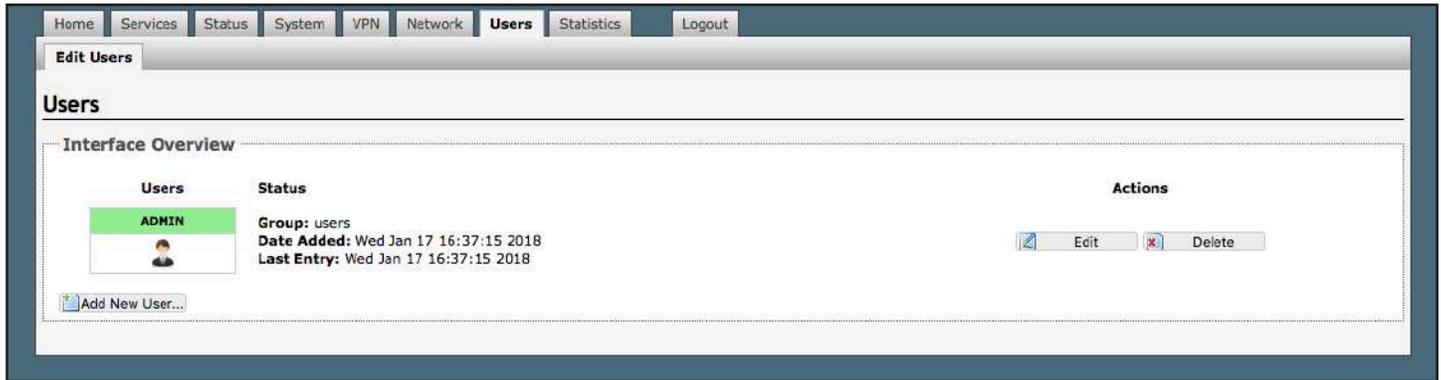
This configuration blocks all traffic to the Internet. Users must log in through the Captive Portal to have access to http and https traffic.

1. Captive Portal must be enabled. (See **Chapter 5.1**).
2. Go to Services > Web Compression and Filtering > Filters to enter the sites you wish to block. (See **Chapter 5.2.2**).
3. Go to Network > Firewall > Firewall Rules and disable (uncheck) these six rules:
 - ALL.
 - PASS DNS.
 - DNS.
 - HTTP.
 - HTTPS.
 - FTP.
4. Click <Save & Apply>. This will modify the firewall to block access to all traffic, including DNS.
5. The web browser configuration of each end user’s device must be modified to enable “Automatic Proxy Detection.” (PC users with Firefox do this in Preferences > Advanced > Network > Settings by selecting “Auto-detect proxy settings for this network”. Other browsers can be configured similarly.)
6. Users will log in to the Captive Portal by entering: <http://10.1.5.1:4990/www/login.chi>.

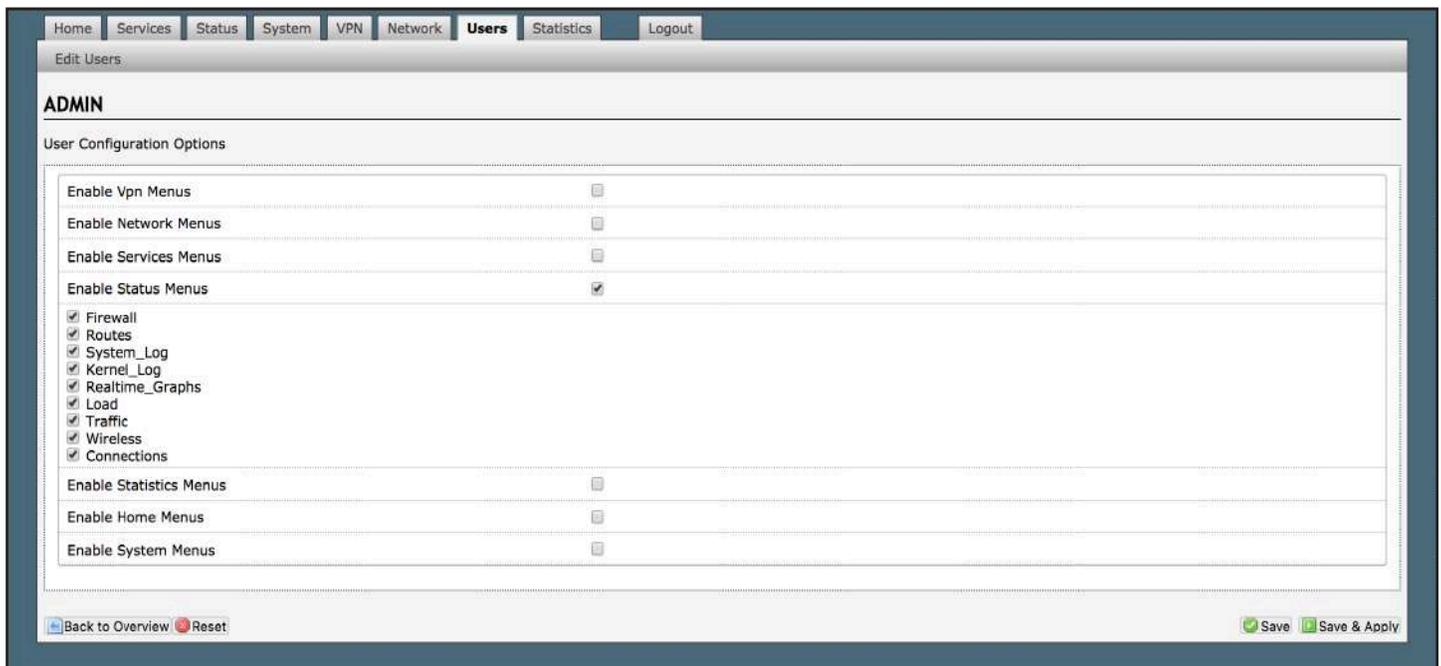
10. Users

Requires “superadmin” login.

The User tab permits the Superadmin login to manage both the Admin login as well as additional desired logins. Through the <User> tab, Superadmin may permit or restrict User log in access.

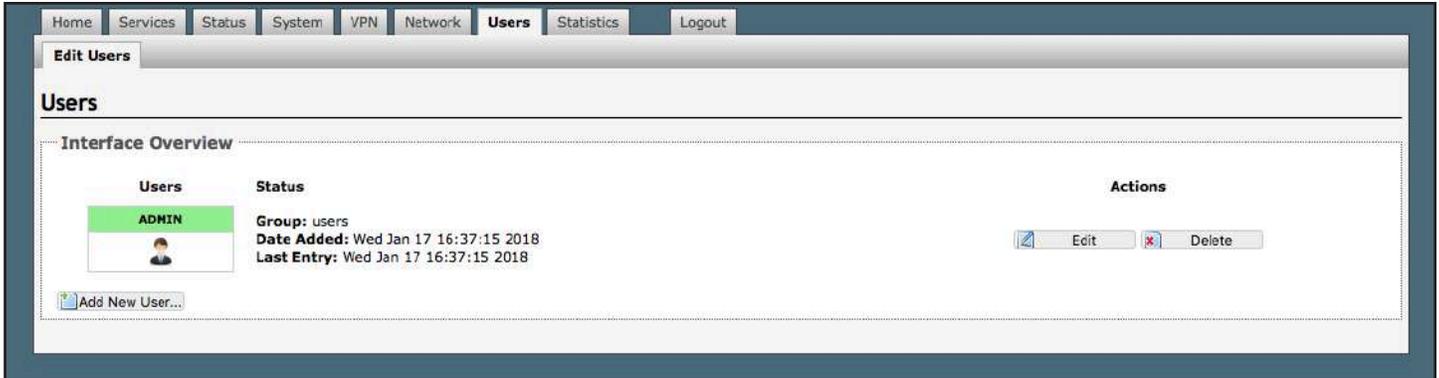


To manage Admin login, click <Edit> located under “Actions”.

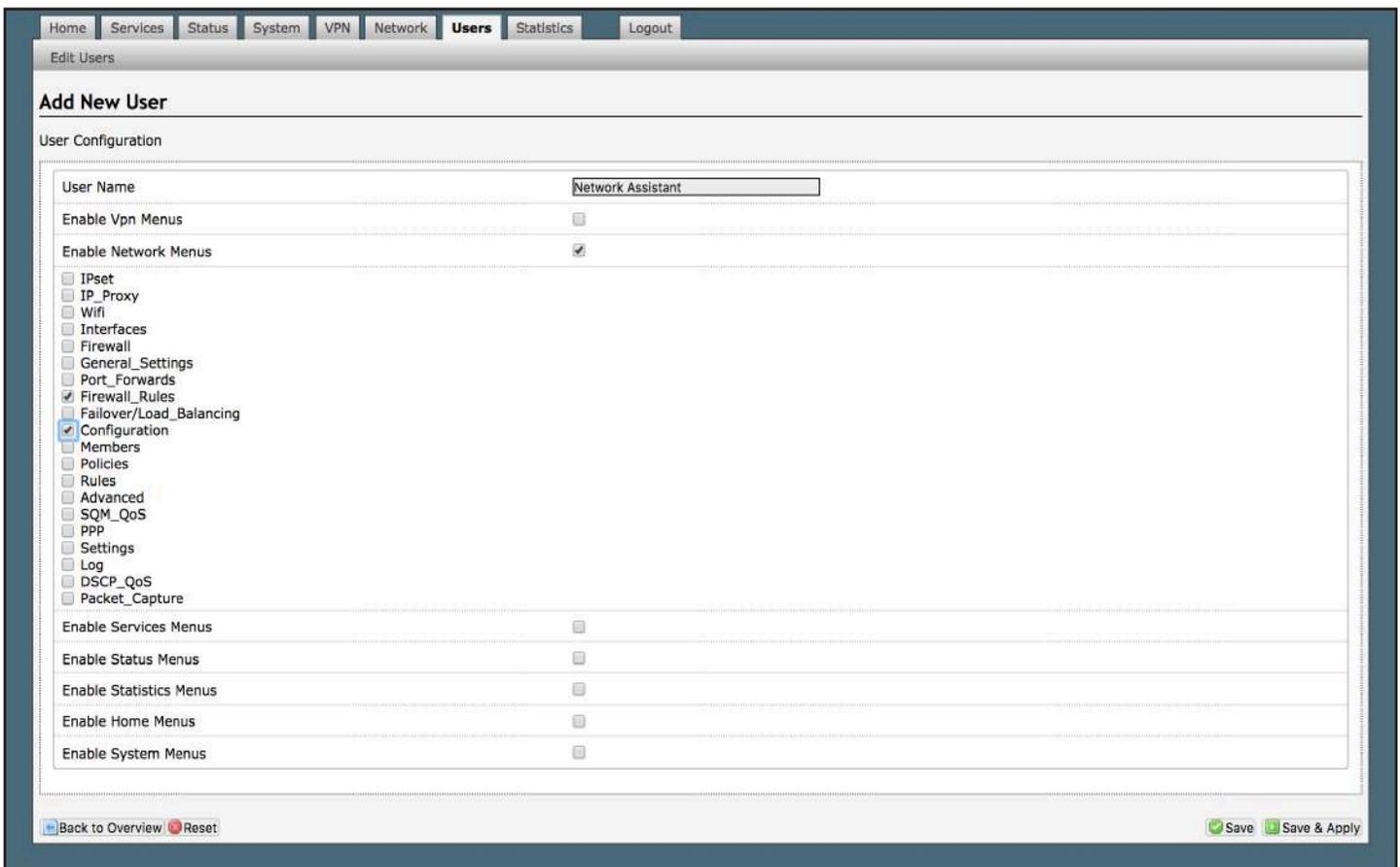


Manage options by clicking (enabling and disabling) options. Click <Save & Apply> when complete.

To create new a new User, Navigate back to <User> tab.



Click <Add New User...>



Create desired User Name.
Click desired menus.
Click <Save & Apply>.

Home Services Status System VPN Network **Users** Statistics Logout

Edit Users

ADMIN

Users

Interface Overview

Users	Status	Actions
NETWORK ASSISTANT ?	Collecting data...	Edit Delete
ADMIN ?	Collecting data...	Edit Delete

Add New User...

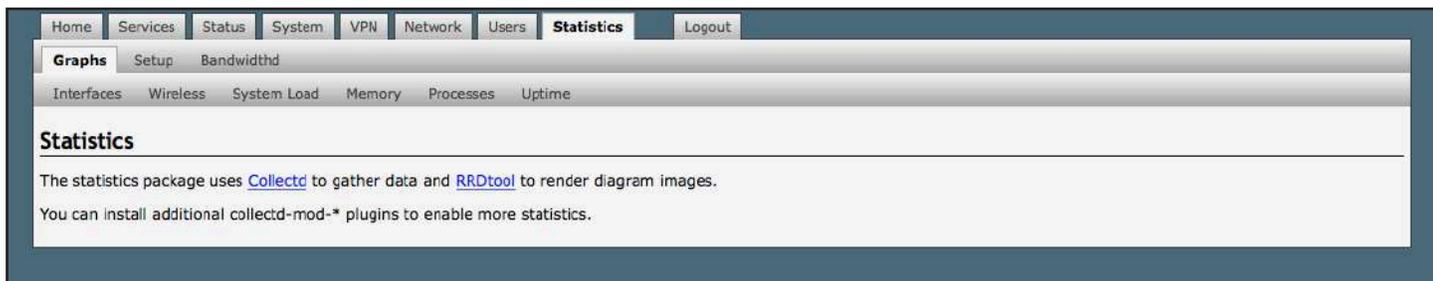
11. Statistics

Requires “superadmin” login.

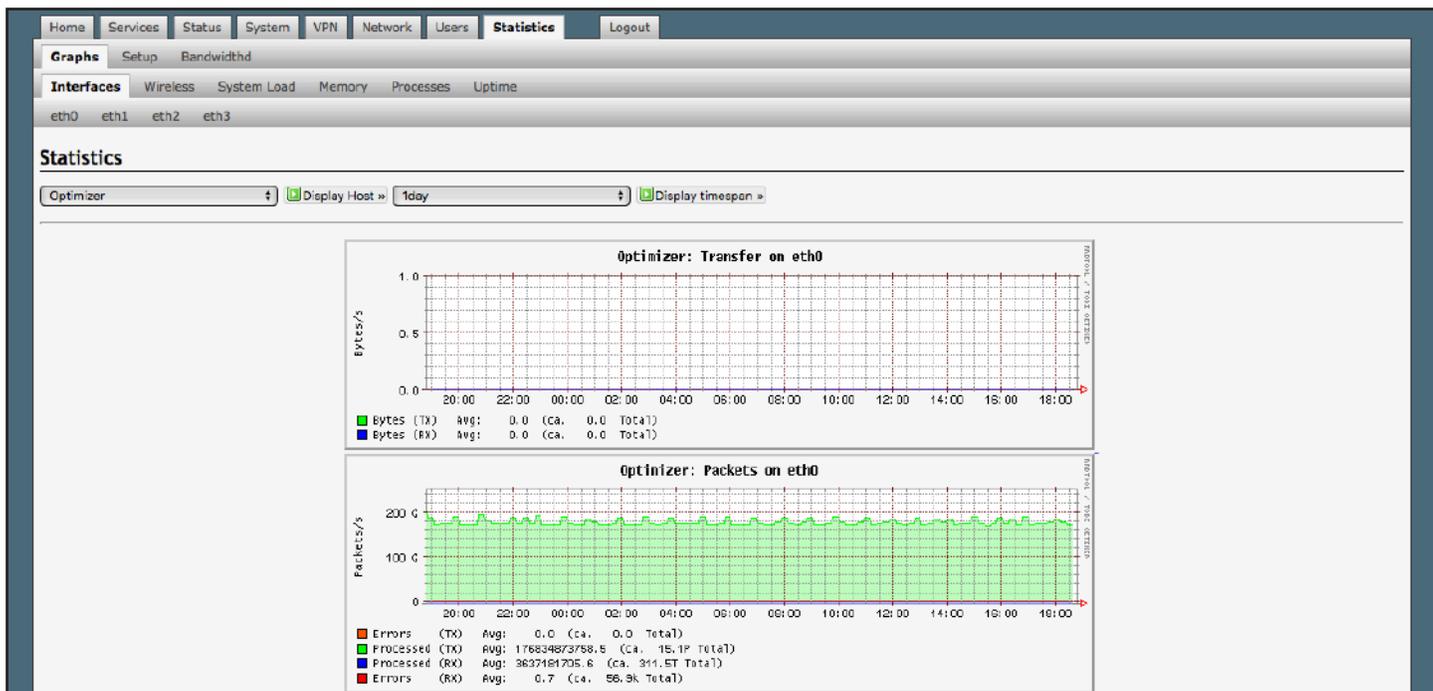


11.1. Graphs

Requires “superadmin” login.



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

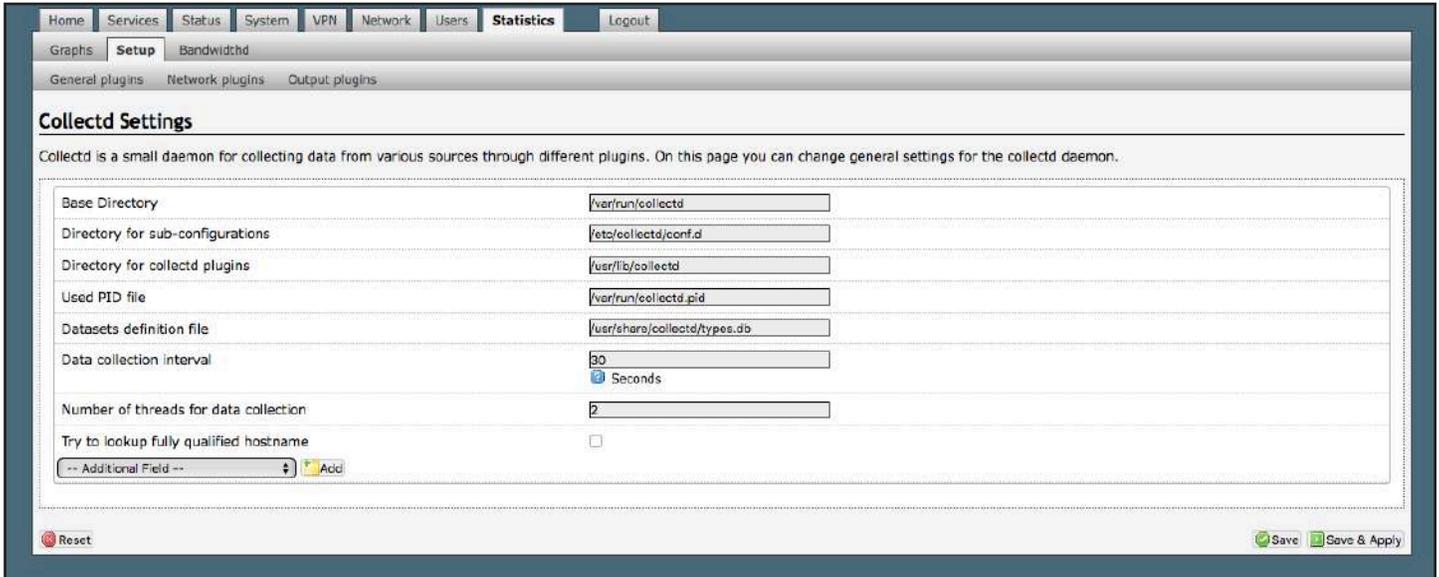


To modify the time span, use the down arrow next to <Display timespan>, then click <Display timespan> to view the graph.

11.2. Setup

Requires “superadmin” login.

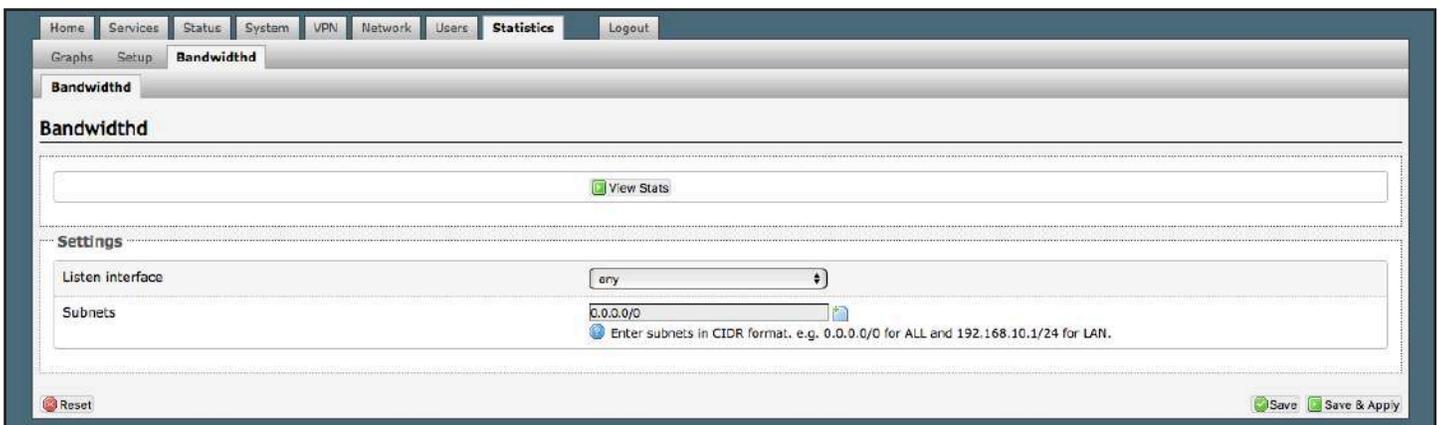
The Optimizer Enterprise uses several tools for collecting data statistics. Use Setup to change general settings for the collectd.



11.3. Bandwidth

Requires “superadmin” login.

Bandwidth tracks TCP/IP subnet and data usage and provides a formulated representation.



Click <View Stats> to be presented with the chart:

Tue Sep 11 19:55:06 2018



Programmed by David Hinkle, Commissioned by [DerbyTech](#) wireless networking.

- [Daily](#) -- [Weekly](#) -- [Monthly](#) -- [Yearly](#) -

Pick a Subnet:
- [Top20](#) -- [0.0.0.0](#) -

Top 20 IPs by Traffic - Daily

Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	SMTP	TCP	UDP	ICMP
Total	5.8G	2.9G	2.9G	0	5.7G	0	5.7G	32.9M	3.7M
199.48.130.178	2.6G	28.0M	2.6G	0	2.6G	0	2.6G	0	0
10.1.5.4	1.6G	1.5G	117.9M	0	1.6G	0	1.6G	5.7M	60.9K
172.16.0.186	692.7M	584.9M	107.9M	0	688.8M	0	689.0M	2.9M	805.4K
10.1.5.10	493.2M	488.7M	4.4M	0	491.4M	0	492.9M	271.7K	4.5K
23.72.224.56	147.6M	138.1M	9.5M	0	147.6M	0	147.6M	0	0
10.135.144.136	61.1M	40.2M	21.0M	0	54.9M	0	55.3M	4.9M	1.0M
10.1.5.15	32.1M	29.4M	2.7M	0	30.5M	0	31.7M	342.6K	2.4K

12. Remote Support

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

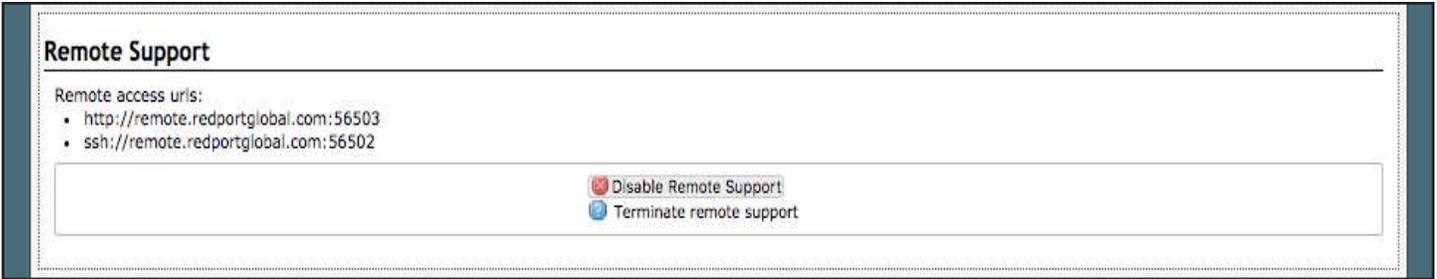
Option 1 - navigate to <Home> tab, scroll down to the “Remote Access” section

The screenshot displays the RedPort web interface. At the top, there is a navigation menu with tabs: Home, Services, Status, System, VPN, Network, Users, Statistics, and Logout. Below this is a 'Tasks' section with sub-tabs for Traffic Routing and MWAN Overview. The main content area is titled 'Welcome' and is divided into several sections:

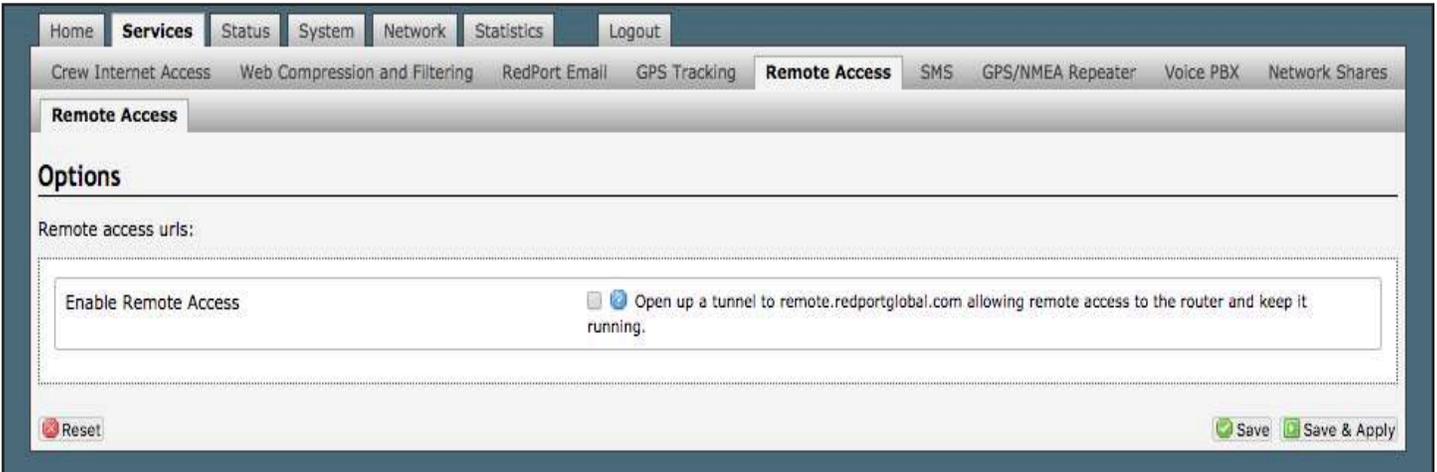
- Crew Internet Services:** Lists Captive Portal URLs (Login, Status, Logout) and provides buttons for 'Generate pincodes', 'Create users', 'Generate pincode usage reports (CDRs)', and 'View/Manage pincodes'.
- Email Access:** Lists email access settings (WEB, POP, SMTP) and a 'Go to webmail' button.
- Email Management:** Provides buttons for 'Create and manage crew email accounts', 'Retrieve, delete, or drop large emails (BigMail) quarantined on the server', 'Perform common email tasks', and 'View email logs'.
- System Status:** Provides buttons for 'System status overview', 'Realtime bandwidth usage over satellite link', 'Historic bandwidth usage over satellite link', and 'System message log'.
- Local WiFi setup:** Under the 'SSID and Security' sub-tab, it provides buttons for 'WiFi setup' and 'Change hotspot name and/or add security and set password'.
- Remote Support:** Provides buttons for 'Enable remote support' and 'Allow remote personal access to your router via a broadband satellite, WiFi, or cell phone link'.

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

When remote support is enabled Remote Access URLs are displayed.

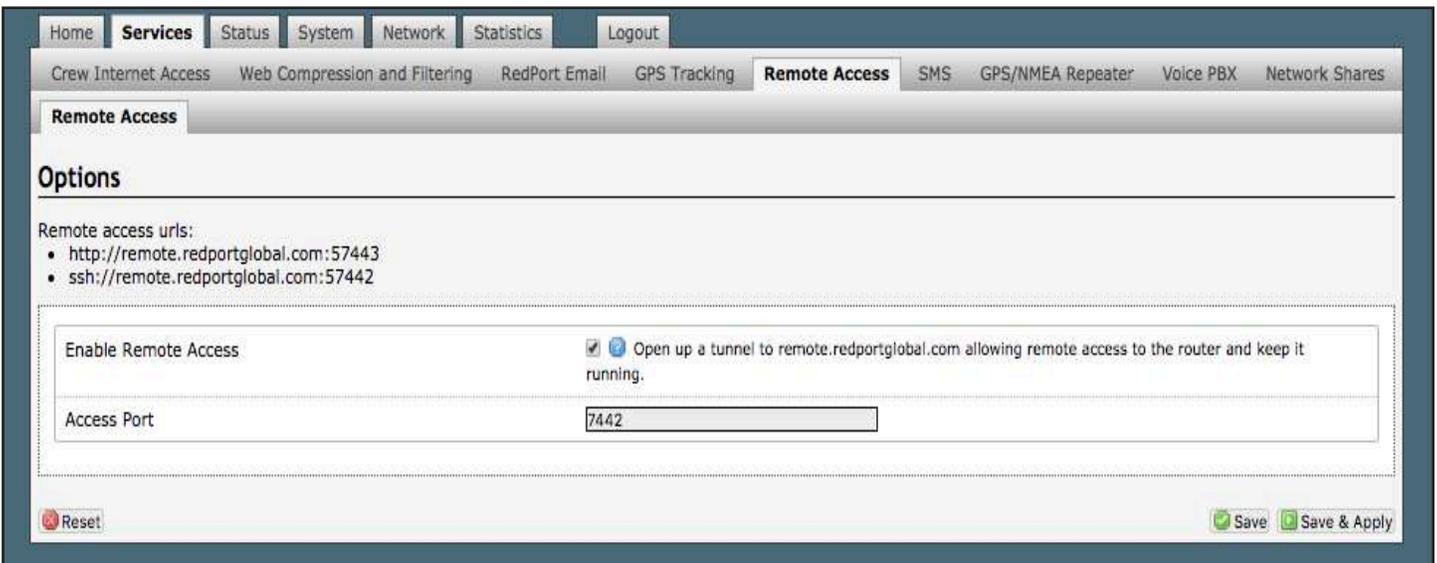


Option 2 - Navigate to <Services> tab, then to <Remote Access>



Click “Enable Remote Support”

When remote support is enabled Remote Access URLs are displayed.



Remote Support will remain enabled until Disabled or the router’s firmware / SD Image is updated.

13. Appendix A

Optimizer Enterprise Guidelines		
The router is shipped in the following Default State: (Legend: E=Enabled, D=Disabled, O=Open)		
Captive Portal	E	
Transparent Proxy	E	
Firewall	O	
DNS	O	
Web Compression	D	
RedPort Email	D	
SMS	E	
GPS Tracking	D	
Voice	D	
RedPort VoIP	D	
Automatic Failover	*	
The list below is designed as a general guideline for customizing the router to meet your needs. Be sure to read Chapter ??? "How to Secure Your Router" before you begin.		
Configuration	Actions	Location in the UI
Captive Portal Use		
	1 Change Captive Portal Admin Password	Services > Crew Internet Access > Tools
	2 Add user account	Services > Crew Internet Access > Users
	3 Add to Allowed Hosts table	Services > Crew Internet Access > Settings > Allowed Hosts
	4 Set Content Filtering Sceme	Services > Web Compression and Filtering > Content Filtering
	5 Firewall Rules	Network > Firewall > Firewall Rules
	6 Add end user accounts	Services > Crew Internet Access > Users
	7 Create Pincodes for Users	Services > Crew Internet Access > Pincodes
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 Filtering > Content Filtering
	5 Establish Domain and Path Filters	Services > Web Compression and Filtering > Content Filtering
	6 Firewall Rules	Network > Firewall > Firewall Rules
RedPort Email (Premium Service - fees may apply)		
	1 Must be enabled	Services > RedPort Email > General > General Settings
	2 Enter Main Identify 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	Services > RedPort Email > Crew Accounts
SMS		
	1 Set Satellite Device	Services > SMS > Settings
	2 Configure Extensions	Services > Voice PBX > Extensions
GPS Tracking via SMS		
	1 Configure Tracking Parameters	Services > GPS Tracking > Tracking Via SMS

GPS Tracking via RedPort (Premium Service - fees may apply)			
	1	Configure Tracking Parameters	Services > GPS Tracking > Tracking powered by RedPort
Voice			
	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
Failover / Load Balancing			
	1	Configure PPP/GSM, if needed	Network > PPP > Settings
	2	Create Network Interface(s), if needed	Network > Interfaces
	3	Create MWAN Member(s), if needed	Network > Failover/Load Balancing > Configuration > Members
	4	Create MWAN Policie(s), if needed	Network > Failover/Load Balancing > Configuration > Policies
	5	Create MWAN Traffic Rule(s), if needed	Network > Failover/Load Balancing > Configuration > Rules
Firewall (See Advanced User Guide before attempting modifications to the firewall)			
	1	Create additional firewall zone(s), if needed	Network > Firewall > General Settings
	2	Assign each interface to a firewall zone	Network > Interfaces
	3	Create new firewall rule(s) if needed	Network > Firewall > Firewall Rules

14. Appendix B

Access to Optimizer Enterprise User Interface (UI) Based on Login Credentials							
SUPERADMIN ACCESS		Services Tab continued		Network Tab continued		Users Tab Continued	
Home Tab		SNMP		Interfaces continued			Interfaces
Tasks			General		WEXT		Wireless
Traffic Routing			Community		WAN6		
MWAN Overview			Com2Sec	Wifi			Output plugins
Services Tab			Group	VLAN Switch			Network
Crew Internet Access			View	DHCP and DNS		Bandwidth	RRDTool
	Settings		Access	Hostnames			
	Users		Log	Static Routes		Bandwidthd	
	Pass-through MAC	Network Shares		Firewall		Logout Tab	
	Pincodes	Status Tab			General Settings	ADMIN ACCESS	
	CDRs	Overview			Port Forwards	Status Tab	
	Tools	Firewall			Fireall Rules	Overview	
Web Compression and Filtering		Routes			IPset	Firewall	
	Settings	System Log			IP Proxy	Routes	
	Content Filtering	Kernel Log		Packet Capture		System Log	
	Cache Management	Realtime Graphs		PPP		Kernel Log	
	Traffic Management	System Tab			Status	Realtime Graphs	
	Access Control	System			Settings		Load
	Logs	Administration			Log		Traffic
	Help	Profiles		SQM QoS			Wireless
RedPort Email		Profiles		DSCP QoS			Connections
	General	Tools		Failover/Load Balancing		Admin Options Tab	
	Connection	Backup / Flash Firmware			Overview	Password	
	Filters	Reboot			Configuration	Logout Tab	
	Primary Accounts	VPN Tab					
	Crew Accounts	PPTP			Interfaces		
	File Transfer		Settings		Members		
	Spool		Users		Policies		
	Tools	IPSec		Users Tab			
	BigMail		IPSec Configuration	Edit Users			
	Logs		Connections	Graphs			
Remote Access			Phase 1 proposals		Interfaces		
	Remote Access		Phase 2 proposals		Wireless		
SMS			Tunnels		System Load		
	Settings		IPSec Logs		Memory		
	Management	OpenConnect VPN			Processes		
GPS Tracking			Server Settings				
	Tracking		User Settings		asterisk		
Dynamic DNS		OpenVPN			chill		
		Network Tab			radiusd		
GPS/NMEA Repeater		Diagnostics			xgate		
	GPS/NMEA Repeater	Interfaces			Uptime		
Voice PBX			PPTP	Setup			
	Settings		WAN		General plugins		
	Extensions		WAN2		System Load		
	Voicemail		PPP		Memory		
	Logs		LAN		Processes		
	Sat SIP Trunk		RedPort: VoIP		Uptime		
	RedPort: VoIP		CAP		Network plugins		



15. Corporate Contact Information

For any questions, concerns, or recommendations, please contact us:

RedPort Company Information

For product orders, support or returns, please contact:

Phone: International: +1 865.379.8723

USA: 877.379.8723

Email: info@redportglobal

Sales: sales@redportglobal.com

Web: redportglobal.com

RedPort Corporate Address

RedPort Global

3224 Wrights Ferry Road

Louisville, TN 37777