Reciport Giobal Marine NETWORKS



RedPort Optimizer Enterprise

Advanced User Guide for Installers/Network Administrators

RedPort Router: wXa-524 (Optimizer Enterprise)





Date

Version

Point of Contact

Nov 9, 2018

Draft Version (v1.0)

Aaron Dickson

RedPort

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

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

RedPort

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	70
7.3.4 Import a Profile	72
7.4. Backup/Elash Firmware	72
7.4.1 Backup/Restore	72
7.4.2 Flash New Firmware Image	73
7 4 3 Flash SD Drive Image	74
7.5. Behoot	75
8 Virtual Private Network (VPNI)	75
8.1 Point-to-Point Tuppeling Protocol PDTP	70
	70
8.3 OpenConnect V/PN	70
8.3. OpenConnect VFN	70
0.4. Openverv	/0
9. Network	00
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

© 2018 RedPort Global Powered by Global Marine Networks, LLC.



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 <u>redportglobal.com</u> 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.

RedPort

- 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.

RedPort

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)





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.

© 2018 RedPort Global

Powered by Global Marine Networks, LLC.





- · 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.

Home Services Status System VPN Network Users Statistic	a Logout
Tasks Traffic Routing MWAN Overview	
Welcome	
C	
 Login - http://10.1.5.1:4990/www/login.chi Status - http://10.1.5.1:4990/www/status.chi Logout - http://logout 	
	I Generate pincodes
	Create users
	Conerate pincode usage reports (CDRs)
	View/Manage pincodes
Email Access	
Email access settings and parameters: • WEB - http://10.1.5.1/webmail • POP - 10.1.5.1:10 • SMTP - 10.1.5.1:25 with no connection or authentication security	
	G to webmail
ε 	
Email Management	
	Create and manage crew email accounts
	Bretrieve, delete, or drop large emails (BigMail) quarantined on the server
	Perform common email tasks
	U View email logs
System Status	
	System status overview
	Realtime bandwidth usage over satellite link
	I Historic bandwidth usage over satellite link
	System message log
SSID and Security	WHFI setup Or and seturity and set password Change hotspot name and/or add security and set password
Sustam	
System	
	Debat cuter
	Mereo du router
1	

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.

Но	ne	Services	Status	System	VPN	Network	Users	Statistics	Logo	ut						
Cr	ew Int	ernet Acce	ss We	b Compress	ion and	Filtering	RedPort E	mail Rem	ote Access	SMS	GPS Tracking	Dynamic DNS	GPS/NMEA Repeater	Voice PBX	SNMP	Network Shares
Se	ttings	Users	Pass-thr	ough MAC	Pincor	des CDR:	Tools									_

DRAFT

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.

Home	Services	Status	System	VPN	Network	Users	Statistics	l	Logout	·
System	Adminis	tration	Profiles 1	Backup /	Flash Firmw	are Re	eboot			

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.

Home	Services	Status	System	VPN	Network	Users	Statistics	Logout						
Diagno	stics	nterfaces	Wifi VI	AN Switc	h DHCP ar	nd DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing

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.

© 2018 RedPort Global Powered by Global Marine Networks, LLC.



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**.

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 Users Pass-through MAC Pincodes CD	Rs Tools
aptive Portal Settings for Crew Internet	Access
are and control access to the Internet by requiring use	ers to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. Use time and amount of data transformed
ssions are logged by Call Data Records (CDR) tracking	ume and amount of data transferred.
ite: Router win report on save & Apply.	
General Settings Advanced Settings Allowed Ho	ists WPAD
Enable	🖉 🐵 Enable/Disable captive portal.
	Caution: Enabling this feature will open the firewall to all traffic. This can result in extremely high traffic usage unless managed properly. High traffic usage can result in very high airtime costs. Best network management practice is
	to configure the firewall and proxy filtering features to reduce usage. Issuing pincodes to users with prudent filters and restrictions will also drastically help manage network access and use.
Enable Fleetwide Pincodes	🗌 🕲 Allow the use of pincodes that can float between vessels.
	Caution: this feature will drive additional administrative airtime overhead that is not accounted for in the pincode CDRs.
	Note: floating pincodes can not be generated on the router. Please contact your provider to acquire floating pincodes should you wish to use this feature.
Enable Transparent Proxy	Image: The second secon
HotSpot Name	RedPort HotSpot
	Image: Second
Reset	Save Save Apr

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.

ings Users Pass-through MAC Pincodes CDRs To	ols
and control access to the Internet by requiring users to en ns are logged by Call Data Records (CDR) tracking time and Router will reboot on Save & Apply.	ter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. d amount of data transferred.
Advanced Settings Allowed Hosts V	VPAD
le Timeout	BCO Default idle timeout in seconds. User will be logged out if no traffic is detected for this period. Set to '0' for unlimited.
ssion Timeout	8800 @ Default session timeout in seconds. User will be logged out at the expiration of this timer. Set to '0' for unlimited.
NS Domain	pcal
mary DNS Server	10,15,1
condary DNS Server	192,168.10.1
date Interval	© Captive portal accounting update interval in seconds. Smaller intervals result in more accurage accounting at the cost of higher CPU loads.
P Ports	BC 443 25 110 22 53 5454 69 5060 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 capitve porta. Port 80 allows access to the web admin, port 110 and 25 to the mail server, etc.
Address	015.1 19 address of captive portal. Must be in the same subnet as the captive portal network.
direct URL	http://10.1.5.14990/www/status.chi Force user to this URL after login. Leave blank string for default URL.
twork Address	0150 Wetwork address of captive portal. Must be in the same subnet as the captive portal IP address.
tmask	165 255 265.0 Retwork address mask.

DRAFT

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

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

DRAFT

through the captive portal.

Crew Internet Access Web Compression and Filtering Renote Access SMG GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SMM Network Shares Setting: Users Pass-through MAC Pincodes CDRs Tools 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 VPAD Note: Router will reboot on Save & Apply. Control: Control: Research Settings: Allowed Hosts VPAD Research Settings: Allowed Hosts Control: VPAD Research Settings: Restaurce Control: Restaurce Restaurce Control: Control: Restaurce Restaurce Restaurce Restaurce Restaurce Restaurce Control: Re	Home Services Status System VPN Network Users Statistic	s Logout				
Setting Users Rase-through MAC Pincedes CDRs Todal 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. Image: Comparison of the com	Crew Internet Access Web Compression and Filtering RedPort Email Re	emote Access SMS G	PS Tracking Dynamic DNS	GPS/NMEA Repeater	Voice PBX SNMP	Network Shares
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 (200170.128.0/19) Base 224.0/22 R 208 79.80.0/22 R 208 79.80.0/22 R 208 79.80.0/22 R 208 79.80.0/22 R 208 79.80.0/21 R 208 79.80.0/22 R 208 79.80.0/21 R 208 79.80.0/21 R 209 186.274.0/22 R 208 179.80.0/21 R 209 186.278.0/21 R 209 186.278.0/21 R 209 186.278.0/21 R 209 180.278.0/22 R 209 180.278.0/21 R 209 180.078.0/22 R 209 180.078.0/24 R 209 180.078.0/24 R 209 180.0/24 R 209 180.0/24 R	Settings Users Pass-through MAC Pincodes CDRs Tools					
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. Comman Settings Advanced Settings Allowed Hosts 200 170.128.0/19 % 203 79.80.0/22 % 204 109.56.0/21 % 204 109.56.0/21 % 204 109.56.0/21 % 204 109.56.0/21 % 204 109.56.0/21 % 204 109.56.0/21 % 204 109.56.0/21 % 203 100.17225 % 204 109.56.0/21 % 205 160.77225 % 209 160.77225 % 209 160.77225 % 208 10.2 % 208 10.2 % 209 160.77225 % 209 160.77225 % 209 160.77225 % 209 160.77225 % 209 160.77225 %						
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 <i>Save & Apply</i> . Seneral Settings Advanced Settings Allowed Hosts WPAD Allowed Hosts D0970128.0/19 E00770128.0/19 E00770128 E0077018 E0	Captive Portal Settings for Crew Internet Access					
General Settings Allowed Hosts WPAD Allowed Hosts 208170.128.0/19 x E088.8.224.0/22 x E04.109.56.0/21 x 199.48.128.0/21 x E08.8.224.0/22 x E04.109.56.0/21 x E09.160.128.0/21 x E09.160.128.0/22 x E09.160.128.0/21 x E09.162.08 x E09.162.18.0 x E08.163.201.104 x E08.163.102.102 x E08.163.202 x	Share and control access to the Internet by requiring users to enter pincodes sessions are logged by Call Data Records (CDR) tracking time and amount of	or username/password l data transferred.	before being granted permissi	ion. Restrict Speed of	access and session	duration as needed. User
General Settings Allowed Hosts Allowed Hosts 208170.128.0/19 208 B5.24.0/22 X 208 B5.24.0/22 X 204 106.86 0/21 X 199.48.128.0/12 X 204.106.86 0/21 X 199.48.128.0/21 X 199.48.128.0/21 X 199.48.128.0/21 X 199.48.128.0/21 X 199.48.128.0/21 X 199.102.78.0/22 X 88.64.64.48 X 88.168.97.37 X 84.150.188.243 X 200.160.722.6 X 200.160.722.6 X 208.85.241.104 X 74.115.212.84/29 X 199.102.168.90.0/24 X 199.102.168.90.0/24 X 199.102.168.90.0/24 X 199.102.102.102.102.102 X 199.102.102.102.102.102.102 X 199.102.102.102.102.102.102 X 199.102.102.102.102.102.102 X 199.102.102.102.102.102.102.102.102 X 199.102.102.102.102.102.102 X	Note: Router will reboot on Save & Apply.					
General Settings Allowed Hosts 209170.128.0/19 # 20879.80.0/22 % 20886.224.0/22 % 204109.56.0/21 % 199.48.128.0/21 % 199.48.128.0/21 % 86.166.0/21 % 199.48.128.0/21 % 86.166.0/21 % 199.48.128.0/21 % 86.166.44 % 86.168.97.37 % 86.168.97.37 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77225 % 209.160.77226 % 209.160.77225 % 209.160.77226 % 192.168.90.0/24 % 192.168.90.0/24 % 192.168.90.0/24 % Hosts, IP Addresses, and Networks that are						
Allowed Hosts 209170.128.0/19 K 208.79.80.0/22 K 208.86.224.0/22 K 204.109.56.0/21 K 199.48.128.0/21 K 199.46.128.0/21 K 199.47.128.0/21 K 199.48.128.0/21 K 199.49.127.00/22 K 199.102.76.0/22 K 209.160.77.226 K 209.160.77.226 K 209.160.78.93 K 208.64.67.148/29 K 192.168.90.0/24 K <th>General Settings Advanced Settings Allowed Hosts WPAD</th> <th></th> <th></th> <th></th> <th></th> <th></th>	General Settings Advanced Settings Allowed Hosts WPAD					
208 79.80.0/22 x 208 86.224.0/22 x 204.109.56.0/21 x 199.48.128.0/21 x 199.102.76.0/22 x 68.168.97.37 x 64.150.188.243 x 209.160.772.26 x 209.160.772.26 x 209.160.783 x 209.160.783 x 209.160.742 x 99.102.76.0/24 x 99.102.76.0/24 x 99.102.772.6 x 209.160.783 x 209.160.782 x 99.102.76.0/24 x 99.102.78.90.0/24 x 99.102.104 x 99.105.5, 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.	Allowed Hosts	209.170.128.0/19	<u> </u>			
208.86.224.0/22 x 204.109.56.0/21 x 199.48.128.0/21 x 199.102.76.0/22 x 69.64.64.48 x 68.168.97.37 x 64.150.188.243 x 209.160.77225 x 209.160.77255 x 209.160.78.93 x 209.160.74.29 x 89.64.67.148/29 x 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24		208.79.80.0/22	<u> </u>			
204.109.56.0/21 * 199.48.128.0/21 * 199.48.128.0/21 * 199.102.76.0/22 * 69.64.64.48 * 68.168.97.37 * 64.150.188.243 * 209.160.77.25 * 209.160.77.25 * 209.160.78.93 * 209.160.78.93 * 208.85.241.104 * 74.15.21.2.64/29 * 192.168.90.0/24 * 192.168.90		208.86.224.0/22	X			
199.48./28.0/21 x 199.102.76.0/22 x 89.64.64.48 x 68.168.97.37 x 64.150.188.243 x 209.160.77.225 x 209.160.78.93 x 208.85.24.104 x 74.15.21.64/29 x 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 * 192.168.90.0/24 *		204.109.56.0/21	<u> </u>			
193.102.76.0/22 x 69.64.64.48 x 68.168.97.37 x 64.150.188.243 x 209.160.7225 x 192.168.90.0/24 x		199.48.128.0/21	<u> </u>			
89.64.64.48 x 68.168.97.37 x 64.150.188.243 x 209.160.77.225 x 209.160.78.93 x 208.85.241.104 x 74.115.212.64/29 x 89.64.67.148/29 x 192.168.90.0/24 * @ 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.		199.102.76.0/22	<u> </u>			
68.198.97.37 x 64.150.188.243 x 209.160.77.225 x 209.160.77.25 x 209.160.78.93 x 209.160.74.93 x 74.115.212.64/29 x 69.64.67.148/29 x 192.168.90.0/24 * 193.169.0/24 <th></th> <th>69.64.64.48</th> <th><u> </u></th> <th></th> <th></th> <th></th>		69.64.64.48	<u> </u>			
64.150.188.243 209.160.77.225 209.160.78.93 209.160.78.93 209.160.78.93 209.160.78.93 209.162.241104 209.162.241104 209.162.241104 209.162.168.90.0/24 192.168.90.0/24		68.168.97.37	<u> </u>			
209160.77225 X 209160.78.93 X 208.85.241104 X 74115.212.64/29 X 69.64.67.148/29 X 192.168.90.0/24 Y Ø 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.		64.150.188.243	*			
209160.78.93 x 208.85.241104 x 74.115.212.64/29 x 69.64.67.148/29 x 192.168.90.0/24 * Ø 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, 8.8.88, 208.45.23.0/24.		209.160.77.225	*			
208.85.241.104 x 74.115.212.64/29 x 69.64.67.148/29 x 192.168.90.0/24 * @ 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, 8.8.88, 208.45.23.0/24.		209.160.78.93	×			
74.115.212.64/29 x 69.64.67.148/29 x 192.168.90.0/24 * W 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.		208.85.241.104	*			
69.64.67.148/29 x 192.168.90.0/24 ** Image: Constraint of the state of		74.115.212.64/29	×			
192.168.90.0/24		69.64.67.148/29	×			
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.		192.168.90.0/24	*			
		Hosts, IP Addresses, hostname, IP address, or	, and Networks that are allowed or network address in CIDR form	without authentication. at. e.g. www.google.com	Valid entries include 1 m, 8.8.8.8, 208.45.23	fully qualified 8.0/24.
Save Save Save Save Save Save Save Save	le Reset					Save Save & Apply

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.

Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shar ,
r pincodes or username/password before being granted permission. Restrict Speed of access and session duration as need amount of data transferred.
AD
Enable Web Proxy Auto Detection. Enabling this option allows client web browsers to automatically detect the we proxy server configuration parameters. This allows administrators to block all firewall ports preventing all internet traffic (including DNS) while still allowing HTTP and HTTPS access. Aministrators can also white/black list HTTP/HTTPS hosts and urls, and filter out HTTP content by customizing web proxy settings. Note: client browsers must enable automatic proxy detection in their settings to use this feature.
We host or networks that should not be proxied. Valid entries include fully qualified hostname, IP address, or network address expressed as shell expression. e.g. 8.8.8, 208.45.23.*, 192.168.*, www.google.com, *.google.com Note: by default RFC1918 private IP addresses (192.168.*, 10.*, 172.16.*) are not proxied.
WRLs or URL expressions that should not be proxied. Valid entries include fully qualified URLs or portions thereof expressed as shell expressions. e.g. http://www.google.com, http://abcdomain.com/folder/*, http://*.youtube.com

DRAFT

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.

	Access Web	Compression a	nd Filtering	RedPort Email	Remote Access	SMS GPS Tracking	Dynamic DNS	GPS/INMEA Repeater	VOICE PBX	SNMP	Network Shares
ngs Use	rass-uno.	IGH PIAC PHA	CODES: CDRS	IUUIS							
's											
in continu	ta avanta alava	daa haaad aa I	la al a la farmant	inn furannan a	and anonyourd). C	normally, this load of a	atustical totage	t according from the Com	tain and cala		
s section	to create pinco	a long period	of time	ion (username	and password). Ge	enerally, this kind of c	ontrolled interne	t access is for the Cap	tain and selei	ct crew n	empers who nee
ing nicen	let access over	a long period	or unite.								
ername	Password	Quota	Reset	Speed	Idle Timeout(s)	Session Timeout(s)		Description			
		None +	Never	Full	System Default	System Default				1	* Delete
mame	issword			1.10	•						
mame p.	assword	ι <u>ς</u>		1000							

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**.

RedPort

- 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)

	tatus System VPN	Network User	rs Statistics	Logo	out					
rew Internet Access	Web Compression and F	Filtering Red Po	rt Email Re	mote Access	SMS GPS Tracking	Dynamic DNS	GPS/NMEA Repeate	r Voice PBX	SNMP	Network Shares
ettings Users Pa	ss-through MAC Pinco	des CDRs T	ools						_	
ss-through MAC										
ling MAC addresses to ewed after assigning eouts for these device Connected Device	o the pass-through list al it a static IP address. No es. S	llows them acces ote that pass thro	ss through the ough MAC add	e captive por dress will be	rtal automatically without disconnected after the	ut authentication captive portal tir	. The device may ne neout period and be	eed to be repow come inoperab	vered or h le. Best p	nave its DHCP lease ractice has setting lo
мас	P Address									
F4-90-EA-10-10-92 10-DD-B1-A2-AD-6C	10.1.5.3 10.1.5.2									
White Listed Devia	ces conds to reasign a static IP	address. Refresh	the page to se	e updated val	lues.					
MAC	IP Address	Quota	Reset	Speed	Idle Timeout(s) Sea	sion Timeout(s)		Description	R.	
- 1 × 2 ×				This sec	ction contains no values ye	et				
ADD										



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 10 Prefix number to be prepended to pincodes. Ouota + None Pincodes will allow users on the internet until their quota is exhausted. Reset + Never + Expire Never Pincodes will unconditionally expire this time period after creation (i.e. drop dead date). This setting takes precedence over the "Reset" period. Speed Full \$ Start Time Unrestricted 4 Unit a data session from start through end time. Times are in the router's local timezone. Stop Time Unrestricted 4 Unit a data session from start through end time. Times are in the router's local timezone. Pincodes Create Create Pincodes. Enter Filename pincodes-2018-02-25.csv Download Download Download a CSV file containing pincodes. To create pincodes for controlled Internet access: Select pincode parameters (guota, reset interval, and speed). - Push 'Create' to create pincodes. - Push 'Download' to downloads 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 pincode number. This might be helpful for tracking pincode inventory. - Quota : size in Mb of the pincode. The user will be able to use their pincode 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 pincode, the user will be able to log back in using the same pincode once the reset period is reached. Reset : Reset period for pincode. This allows for a specified renewal time for the pincode to become active again. If a pincode as a reset period of 'None' the pincode will not renew when it expires (this would be a one-time pincode). - Expire : Drop dead date for pincode. Pincodes will unconditionally expire the selected period after creation. The drop dead date takes presedence over the "Reset" period. - Speed : Maximum bandwidth consumed by the user. - Start/Stop Time: Specifies time slot for which a pincode user is allowed access to the Internet.

DRAFT

• **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.

The compression and meaning reards	ort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares
ttings Users Pass-through MAC Pincodes CDRs Too	cis
Rs	
erate CDRs (Call Data Records, or the reports for internet usa	ane) for users and hincodes
Username or Pincode	
	Image: Inter "All" to for a complete list of all CDRs. Note this could take some time to complete on systems with many pincodes.
Reporting Period	Enter "All" to for a complete list of all CDRs. Note this could take some time to complete on systems with many pincodes. All All
Reporting Period	 Enter "All" to for a complete list of all CDRs. Note this could take some time to complete on systems with many pincodes. All

- 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.

v Internet Acce	ss Web Comp	ression and Filtering RedPort En	nail Remote Access	SMS GPS Tracking	Dynamic DNS GI	PS/NMEA Repeater	Voice PBX SNMP	Network Shares				
nac llears	Dace through MA											
ngs users	rass-unougn may	L PHICODES CORS TOOIS										
S												
min password			New adm	New admin password								
			🙆 Enter ne	Inter new admin password and then press Set Password below.								
			Set Pass	word								
set database to	factory defaults		🗟 Reset DE	1								
			O Deletes	all pincodes and CDRs but	keeps the users.							
rge expired pin	codes		Purge ex	pired pincodes								
			🙆 Purge a	Il expired pincodes from the	e system.							
rge unused pind	odes		Purge un	used pincodes								
			Ø Purge al	Il unused pincodes from the	e system.							
nage pincodes			🔝 Manage	pincodes								
ssion Status												
us, time, and dat	a usage for curre	ntl <mark>y active sessions.</mark>										
Username	Status	Mac Address	IP Address	Session Time	Idle Time	Data In(b)	Data Out(b)	Logout				
-	dnat	F4-90-EA-10-10-92	10.1.5.3	0	0	0	0	Cogout 🖉				
	deat	10-00-B1-42-40-60	10152	0	0	0	0	() I conut				

DRAFT

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

DRAFT

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

rew Internet Access Web Compression and Filtering RedP	Pert Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Natwork Shares
ettings Users Pass-through MAC Pincodes CDRs To	ools
ols	
Manage Pincodes	
Select All Pincodes	Select
Un-Select All Pincodes	Un-Salect
Remove CDRs	XIReset Plete CDRs for selected pincodes
Delete All Selected	@ Delete
Enter Filename	pins-2018-02-25.csv

Dincode

Pincode	Speed	Quota	Reset	Expire	Time Range	Usage(b)	Time(s)	Select	Reset	Delete	Ed
test	128 kbps	10485760	never	never	unrestricted	nil	nil		Reset	Delete	
jason	open	none	never	never	unrestricted	235267821	4806		Reset	Delete	
C8-E0-EB-53-98-9E	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
C8-E0-EB-53-98-9D	open	none	never	never	unrestricted	17384517	17071		Reset	Delete	
C8-E0-EB-53-98-1A	16 kbps	none	never	never	unrestricted	nil	nil	0	Reset	🙋 Delete	
9295491-7428	open	none	never	never	unrestricted	nil	nil		Reset	🐸 Delete	
8966715-8954	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
6632431-1485	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
5849211-0527	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
4860980-5534	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
4798984-8891	open	none	never	never	unrestricted	nil	nil		Reset	🙆 Delete	
4472760-7312	open	none	never	never	unrestricted	nil	nil		Reset	🙋 Delete	
4461521-7673	open	none	never	never	unrestricted	nil	nil		Reset	😺 Delete	
4298899-8349	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
4139695-3303	open	none	never	never	unrestricted	nil	nil		Reset	🔯 Delete	
4086789-0184	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
4031340-7609	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
3475663-4940	open	none	never	never	unrestricted	nil	nil		Reset	🥘 Delete	
3235248-4060	open	none	never	never	unrestricted	nil	nil	0	Reset	🐸 Delete	
3197847-4155	open	none	never	never	unrestricted	nil	nil		Reset	🙆 Delete	
3156068-7854	open	none	never	never	unrestricted	nil	nil	0	Reset	🙆 Delete	
2788226-4302	open	none	never	never	unrestricted	nil	nil		Reset	Delete	
2567907-4697	open	none	never	never	unrestricted	nil	nil	0	Reset	Delete	
1968416-0520	open	none	never	never	unrestricted	nil	nil		Reset	🔕 Delete	
1510602-2117	open	none	never	never	unrestricted	nil	nil		Reset	Delete	

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.

Home Services Status System VPN Users Statistics Network Logout SMS GPS Tracking Crew Internet Access Web Compression and Filtering RedPort Email Remote Access Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Share Settings Users Pass-through MAC Pincodes CDRs Tee Pincode Editor 8966715-8954 Pincode Ouota None \$ Pincode will allow user on the internet until their quota is exhausted. Reset Never \$) \$) Expire Never Pincode will unconditionally expire this time period after save (i.e. drop dead date). This setting takes precedence over the "Reset" period. Speed Full ; \$) Start Time Unrestricted Limit a data session from start through end time. Times are in the router's local timezone. Stop Time Unrestricted \$) Limit a data session from start through end time. Times are in the router's local timezone. Save Changes Save

DRAFT

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.

fome Services Status System VPN Network Users Stati	tics Logout					
ew Internet Access Web Compression and Filtering RedPort Email ttings Content Filtering Cache Management Traffic Management	Remote Access SMS Access Control Logs	GPS Tracking Help	Dynamic DNS	GPS/NMEA Repeater	Voice PBX S	NMP Network Shares
eb Filtering and Compression Proxy Settings						
able and configure web compression and filtering features.						
General Settings Compression Advanced						
Enable compression	Web compress increasing overall spe your dealer for additi compression for this	ion will, on averag eed. Don't yet hav ional information. device.	e, decrease over e the incredible a They can set you	all bandwidth usage by irtime savings and optir up with an account use	a factor of 3-5X w nization of web co mame and passwo	nile simultaneously mpression? Contact ord to enable
Username	Enter_Compression_U	ser_Name_Here]			
Password	Enter_Compression	n_Password_Here] @			
Compression Level	Maximum	\$]			
Primary Server	xweb.gmn-usa.com	ŧ)			
Secondary Server	xweb2.gmn-usa.com	n 🕴]			
Service Type	Failover	\$]			
Bypass Regex Domain	24] 🍅			
50 50	Bypass compress domain containing .g	ion for listed sites joogle.com. See "E	Enter host regul Domain Syntax" u	ar expression to match. nder Help tab for additio	e.g. '.google.com onal information.	" to bypass any
Reset						Save Usave &

DRAFT

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.

Linga Content Filtering Caule Prenegenerin, in anne Pranegenerik, in	Access Control Logs Help
b Filtering and Compression Proxy Settings	
ble and configure web compression and filtering features.	
Seneral Settings Compression Advanced	
Enable compression	Web compression will, on average, decrease overall bandwidth usage by a factor of 3-5X while simultaneously increasing overall speed. Don't yet have the incredible airtime savings and optimization of web compression? Contact your dealer for additional information. They can set you up with an account username and password to enable compression for this device.
Jsername	Entar_Compression_User_Name_Here
Password	Denter_Compression_Password_Here
Compression Level	Maximum 🗧
Primary Server	xweb.gmn-usa.com 🛟
Secondary Server	xweb2.gmn-usa.com 🛟
Service Type	Failover \$
Bypass Regex Domain	Bypass compression for listed sites. Enter host regular expression to match. e.g. ".gcogle.com" to bypass any domain containing .gocgle.com. See "Domain Syntax" under Help tab for additional information.

DRAFT

- **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.

RedPort

		11200000200000	1000	11111					
ttings Content Filtering Cache Managemen	t Traffic Management	Access Control	Logs	Help					
b Filtering and Compression Prov	cy Settings								
	() betting								
ble and configure web compression and filtering	ng features.								
General Settings Compression Advanced									
nable Web Proxy		🖸 🙆 Enable	e/Disable	e web proxy service	ce.				
ransparent Proxy		O Enable compression Caution: En result in high Note: This r automatical	e transpa without abling tr h traffic node is r y to prev	arent proxy. i.e. tr having to modify ransparent mode r usage. not compatible wit vent conflicts.	ansparently redin the end user's br requires opening 1 th the captive port	ect HTTP web traffic to t owser settings. 'CP ports 53 (DNS), 80 (al. The captive portal, if	he web proxy f (HTTP), and 44 ^r enabled, will c	or filterin 3 (HTTPS disable thi	a and/or) which can (will) s feature
folkla Hankaraa		Optimizer Displaye	d in prox	v error messages	to end user.				
Isible Hostname		Co Displayer							

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.

rew Internet Access Web Compression and Filtering RedPort F	mail Remote Access SMS GPS tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares	
ettings Content Filtering Cache Management Traffic Managem	ent Access Control Logs Help	
/eb Filtering and Compression Proxy Settings		
able and configure web compression and filtering features.		
General Settings Compression Advanced		
Listen address	3128	
	Interfaces. With the second point of	
Listen interfaces	🕑 lan(br-lan) - 192.168.10.1	
	biz(eth3) - 192.168.11.1 10.1.5.1	
	Bind proxy to the following interfaces	
Log rotation	weeky a	
	Log rotation schedule.	
Rotate now	Rotate	
Purge cache	UPurge	
	Purge and rebuild cache	

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>.

mote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares cess Control Logs Help						
cess Control Logs Help						
sements, prevent access to various categories of web sites and block resources with explicit content.						
😰 🕼 Enable content filtering						
Configure Content Filtering Setup blocking by category, usage reporting, and much more.						
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.						
Never 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.						

Obtain license from RedPort authorized dealers.

Click "Enable content filtering".

Click "Configure Content Filtering".

	Sign in to Diladele Web Safety		
	Default login name is root		
ایران ایک اور اور اوران اوران اوران ایک اوران و ایران	Sign In		
n Marin Profession			

Enter Diladele login and password supplied by RedPort authorized dealer.

5.2.3. Cache Management

Requires 'superadmin' login.

ew Internet Access Web Compression and Filtering Red	Port Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares						
ttings Content Filtering Cache Management Logs H	leip						
che Management							
lard disk cache size	3072						
Hard dick cache system	auts \$						
and one work system	Specify the kind of storage system to use.						
	ufs is the old well-known Squid storage format that has always been there.						
	aufs uses POSIX-threads to avoid blocking the main Squid process on disk-1/O. (Formerly known as async-io.)						
	diskd uses a separate process to avoid blocking the main Squid process on disk-1/O.						
	null Does not use any storage. Ideal for embedded systems						
Aemory cache size							
	This is the amount of physical RAM (in megabytes) to be used for negative cache and in-transit objects. This value should not exceed more than 50% of the installed RAM. The minimum value is 1MB.						
linimum object size							
	Objects smaller than the size specified (in kilobytes) will not be saved on disk. The default value is 0, meaning there is no minimum.						
faximum object size	1048576						
	Objects larger than the size specified (in kilobytes) will not be saved on disk. If you wish to increase speed more than you want to save bandwidth, this should be set to a low value.						
evel 1 subdirectorie							
	Each lowel 1 directory contains 2E6 subdirectories, so a value of 2E6 lowel 1 directories will use a total of 6EE26 directories						

DRAFT

	(Heap GDSF +)
	The memory replacement policy determines which objects are purged from memory when space is needed. The default
	policy for memory replacement is GDSF.
	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.
	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.
	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.
	Heap LRU: Last Recently Used - Works like LRU, but uses a heap instead.
	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.
Cache replacement policy	(Heap LFUDA +)
	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.
Low-water-mark in %	90
	Cache replacement begins when the swap usage is above the low-low-water mark and attempts to maintain utilisation near the low-water-mark.
High-water-mark in %	95 Ø As swap utilisation gets close to the high-water-mark object eviction becomes more aggressive.
Enable offline mode	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	Contraction of the address of the state of t

5.2.4. Traffic Management

Requires 'superadmin' login.

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

tings Content Filtering Cache Management Traffic Manage	ement Access Control Loos Help						
ffic Management							
laximum download size	<u>6</u>						
	Limit the maximum total download size to the size specified here (in kilobytes). Set to 0 to disable.						
1aximum upload size	b Dimit the maximum total upload size to the size specified here (in kilobytes). Set to 0 to disable.						
Overall bandwidth throttling	0 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.						
Per-host throttling	0 It is value specifies (in kilobytes per second) the download throttling per host. Set to 0 to disable this.						
Throttle only specific extensions	Our Check this to enable throttling by extension type. Leave unchecked to throttle all downloads/uploads by host or network.						
inish transfer if less than X KB remaining	0 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.						
Abort transfer if more than X KB remaining	Retrieval will be aborted if browser connection is closed and the transfer has more than X kilobytes remaining. Set to to abort the transfer immediately.						
Finish transfer if more than X % finished	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.						

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.

tings Content Filtering Cache Management Traffic Managen	rent Access Control Logs Help						
ess Control Filters							
nrestricted IPs	Enter source IP address that are to have unrestricted access to proxy server.						
anned host addresses	Enter source IP address that are not allowed to use the proxy server.						
/hitelist	Enter destination domains that will be accessable to the users that are allowed to use the proxy. You also can use regular expressions.						
lacklist	Enter destination domains that will be blocked (such as ".windowsupdate.microsoft.com" or ".update.") to the users that are allowed to use the proxy. You also can use regular expressions.						
ustom Options	refresh_pattern guru.avg.com/*\.(bin) 4320 100% 43200 reload-into-ims refresh_pattern windowsupdate.com/*\.(cabjexe) 4320 100% 43200 reload-into-ims refresh_pattern download.microsoft.com/*\.(cabjexe) 4320 100% 43200 reload-into-ims refresh_pattern au.download.windowsupdate.com/.*\.cabjexe) 4320 100% 43200 reload-into-ims						
	I 22 You can put your own custom options here, separated by newlines. They'll be added to the configuration. They need to be squid.conf netive options, otherwise squid will NOT work.						

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**).

g page inche log Accress log Clear log entry Download 2018/02/25 18:54:18 storeDirWriteCleanLogs: Starting 2018/02/25 18:54:18 forbieRotate: daemor:/var/og/squid/access.log	attings Content Filtering Cache Man	accoment Traffic Management	Access Control	Lone	Help	Dynamic Diva	the synamics repeated	VUILE FOX	Janier	Network Islates
g page Iche log Access log Clear log entry ICLEAR Download log 2018/02/25 18:54:18 storeDirWriteCleanLogs: Starting 2013/02/25 18:54:18 Finished. Wrote 2165 entriles. 2013/02/25 18:54:18 logfileRotate: daemon:/var/og/squid/access.log 2018/02/25 18:54:18 logfileRotate: daemon:/var/og/squid/access.log	currigs concentrationing caute net	agement france Hanagement.	Mucess current	LUGS	nety			_	_	
Access log Clear log entry Clear log entry Download log Diverse Stating 2018/02/25 18:54:18 storeDirWriteCleanLogs: Starting 2018/02/25 18:54:18 logfileRotate: daemor:/var/og/squid/access.log 2018/02/25 18:54:18 logfileRotate: daemor:/var/og/squid/access.log	g page									
Clear log entry Download log Download log Download Downlo	che log Access log									
Download log C018/02/25 18:54:18 storeDirWriteCleanLogs: Starting 2018/02/25 18:54:18 Finished. Wrote 2165 entries. 2018/02/25 18:54:18 Took 0.00 seconds (1467479.67 entries/sec). 2018/02/25 18:54:18 logfileRotate: daemon:/var/log/squid/access.log 2018/02/25 18:54:18 logfileRotate: daemon:/var/log/squid/access.log	Clear log entry		Clear							
2018/02/25 18:54:18 storeDirWriteCleanLogs: Starting 2018/02/25 18:54:18 Finished. Wrote 2165 entries. 2018/02/25 18:54:18 logfileRotate: daemon:/var/og/equid/access.log 2018/02/25 18:54:18 logfileRotate: daemon:/var/og/equid/access.log	Download log		Download	d						
	2018/02/25 18:54:18 StoreUnWinteCleanLo; 2018/02/25 18:54:18 Finished. Wrote 216 2018/02/25 18:54:18 Took 0.00 seconds (2018/02/25 18:54:18 logfileRotate: daemon 2018/02/25 18:54:18 logfileRotate: daemon	s: starting 5 entries. 1467479.67 entries/sec), :/var/log/squid/access.log :/var/log/squid/access.log								

RedPort

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.

5-042 - <u>1</u> ,0 (100, 141)	and the second se	and the second	 U something and 	1100000-sull			 000000000	
ngs Content	Filtering Cache Managem	ent Traffic Managemen	Access Control	Logs	Help			
umentation	1			0.170.190.20		 		
A detailed desc	ription all proxy options and	settings may be found at ;	vww.redportglobal.co	m				

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.

	t Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNNP Network Shares					
neral Connection Filters Primary Accounts Crew Acco	ounts File Transfer Spool Tools BigMail Logs					
neral Settings						
Webmail login						
Redirect to webmail	Redirect G Users can access webmail by using <u>http://10.1.5.1/webmail</u>					
POP Server Address: Port	2 10.1.5.1:110					
SMTP Server Address: Port, Connection Security: None, Auther	ntication:None					
General Settings Wehmail Settings Network Settings	Log Settings Mail Filtering					
Main identity userid	A main identity.UserD_Here @ A main identity must be configured to use the meil system. Contact your provider for a main identity username and password.					
Main identity password	🧈 Enter, Main, Identity, Password, Here 🛛 💋					
Domain	redportglobal.com					
	60 Send/Receive email to/from server at this interval in minutes.					
Update interval(min)	Send/Receive email to/from server at this interval in minutes.					



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:

General Settings Webmail Settings Network Settings Log Set	iettings Mail Filtering
Enable email server	0
Main identity userid	Enter Main Jdentity UserID Here A main identity must be configured to use the mail system. Contact your provider for a main identity username and password.
Main identity password	Penter_Main_Identity_Password_Here
Domain	redportglobal.com Image: state of the state of
Update interval(min)	80 Send/Receive email to/from server at this interval in minutes.
Send and Receive mail concurrently	@ A duplex channel allowing email to be sent and received at the same time will be created if this option is selected.

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:

Home Services Status System VPN Network Users Statistics Logout Network Shares Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP General Connection Filters Primary Accounts Crew Accounts File Transfer Spool Tools BigMail Logs **Connection Settings** Gateway TCP/IP Port # 443 + Primary XGate Server xgate.gmn-usa.com + Network Connection Network Connection ÷ Select satellite connection method. Dial Override Leave blank to use interface default. **IP Device Password** 2 IP dialer device password. Leave blank for default. Must have a value if the system password is changed. IP Dial Override IPAddress: Port (where the port number is optional) of the satellite terminal to control. Leave blank to use default gateway. Hint: Should be left blank for most installations. Leave Open C Q Leave network connection active when done Use if Open 🗌 🙆 Use another connection if already open. Override network timeouts 🗌 🧐 Override default connection timeouts. Should not be required. Persistent Connections Persist with connections until transfer completes or num times Save Save & Apply Reset

DRAFT

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.

Home NSD Services Status System VPN Network	Users Statistics Logout				
Crew Internet Access Web Compression and Filtering RedPort	Email Remote Access SMS GPS Tr	cking Dynamic DNS	GPS/NMEA Repeater	Voice PBX SNN	1P Network Shares
Remote Access				_	
Options					
emote access urls: http://remote.redportglobal.com:53636 ssh://remote.redportglobal.com:53635					
Enable Remote Access	🕜 🙆 Open up a tunnel to rem	te.redportglobal.com all	owing remote access to t	he router and keep	it running.
Access Port	3635				
					<i></i>
@ Reset					Save 🔲 Save & Apply

RedPort

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.

Home	NSD	Services	Status	System VPN	Network	Users	Statistics	Logout
Tasks	Traffic	Routing	MWAN Ove	erview				
Welcor	me							
Crew I	ntern	et Servic	es - DIS.	ABLED				
							Enable Cre	ew Internet
Email	Acces	5						
Email a	ccess se	ttings and p	arameters:					
WE POF	B - <u>http:</u> - 127.0	//127.0.0.1/	/webmail					
• SMT	TP - 127	.0.0.1:25 wi	th no conn	ection or authent	cation securit	τ γ		
							Go to web	
Email	Manag	ement						
							Create and	d manage crew email accounts
							🔲 Retrieve, o	delete, or drop large emails (BigMail) quarantined on the server
							Perform c	ommon email tasks
							View emai	il logs
[
System	n State	JS						
							System st	atus overview
							Realtime b	andwidth usage over satellite link
							Historic ba	andwidth usage over satellite link
							System me	essage log
Local	WiFi s	etup						
SSID	and Sec	curity					W Fi setup	D.
							Change h	notspot name and/or add security and set password
L								
Remot	e Sup	port						
Remote http ssh	access o://remo ://remot	uris: te.redportgi e.redportgio	obal.com:5	3636 3635				
							Disable Re	amote Support
							U Terminate	e remote support
System	n							
							Router par	ssword
							Reboot ro	uter
-		_	_			_	_	

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.

ew internet Access web compression and Fitzening Reproit enhant Rem	te Access and oralized ing ovirallic ons oralismed repeated voice roc along include	AUR Shares
ttings Management		
s parameters		
figure the parameters for SMS		
Enabled	D	
nterval in seconds between LOCAL send attempts	240	
number of days that messages stay in queue when receiving messages	3	
Satellite device	(Iridium 🛟	
Check for received messages (in seconds)	360	
Configure extensions to receive SMS	Redirect	

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

V	Iridium.	
	iSavi	
	Sailor FBB	

- 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.

RedPort

lemet	Access Web	compression and Pin	ening kedPort Email	Kemole Access	SHS GPS macking Dynan	IIIC DIVIS GPS/IMEA Repeater	VOICE PBX	SMILL	Network Share
E	xtensions V	picemail CDR L	ogs Sat SIP Trunk	RedPort VoIP					
ions									
	11 Telepho	na							
910	TT Telepho								
Pay	ment Mode	Extension	Caller ID			Description			
	v	alue larger than 200	Free text		You may enter a	description here for your reference			
prep	aid 🗘 🕄	01 [3	01 Capta	ain analog line 0					
xten	sions								
SMS	Payment Mod	le Extension	Password	Caller ID		Description			
		Value larger than	200 SIP extension passwo	rd Free text	You may en	nter a description here for your refer	ence		
0	postpaid	\$ 201	1234	201	Captain line	30 US			Delete
	prepaid	\$ 202	1234	202	Crew line 1]	Delete
	postpaid	\$ 203	1234	203	Crew line 2				Delete
-	postpaid	\$ 204	1234	204	Crew line 3				Delete
	E ions g RJ Pay prepart exten SMS	Extensions Vi ions g RJ-11 Telepho Payment Mode v prepaid \$34 xtensions SMS Payment Mode g postpaid g prepaid	Extensions Voicemail CDR L ions g RJ-11 Telephone Payment Mode Extension Value larger than 200 prepaid \$ 301 31 extensions SMS Payment Mode Extension Value larger than 0 (pestpaid \$ 202 0 (prepaid \$ 202 0 (pestpaid \$ 202) 0 (pestpai	Extensions Voicemail CDR Logs Sat SIP Trunk ions g RJ-11 Telephone Payment Mode Extension Caller ID Value larger than 200 Free text prepaid) [301 [301 Value larger than 200 Free text prepaid) [301 [301 Value larger than 200 SIP extension password Perspaid) [201 [1234 Perspaid) [202 [1234	Extensions Voicemail CDR Logs Sat SIP Trunk RedPort VoIP ions g RJ-11 Telephone Payment Mode Extension Caller ID Value larger than 200 Free text prepaid \$ [301] [301] Captain analog line 0 Ktensions Caller ID Value larger than 200 SIP extension password Caller ID Value larger than 200 SIP extension password Free text © pestpaid \$ [201 [1234] [201 © prepaid \$ [202 [1234] [202 © prepaid \$ [202 [1234] [202	Extensions Voicemail CDR Logs Sat SIP Trunk RedPort VoIP ions g RJ-11 Telephone Payment Mode Extension Caller ID Value larger than 200 Free text You may enter a prepaid j 01 301 Captain analog line 0 Ktensions Password Caller ID Value larger than 200 SIP extension password Free text Value larger than 200 SIP extension password Caller ID Value larger than 200 SIP extension password Free text Value larger than 200 SIP extension password Free text value larger than 200 SIP extension password Caller ID Value larger than 200 SIP extension password Free text You may ender Prepaid 201 1234 201 Captain line Prepaid 202 1234 202 Drew line 1	Extensions Voicemail CDR Logs Sat SIP Trunk RedPort VoIP ions g RJ-11 Telephone Description You we larger than 200 Free text You may enter a description here for your reference prepaid 301 301 Caller ID Description Ktensions Payment Mode Extension Password Caller ID Description SMS Payment Mode Extension Password Caller ID Description Value larger than 200 SIP extension password Free text You may enter a description here for your refer © pestpaid 201 1234 201 Captain line © prepaid 202 1234 202 Crew line 1 © prepaid 202 1234 202 Crew line 2	Extensions Voicemail CDR Logs Sat SIP Trunk RedPort VoIP ions g RJ-11 Telephone Description You way enter a description here for your reference Description You way enter a description here for your reference Description prepaid \$301 301 Caller ID Description Ktensions Payment Mode Extension Password Caller ID Description Value larger than 200 SIP extension password Free text You may enter a description here for your reference Peppeid \$201 \$1234 \$201 Captain line You may enter a description here for your reference Peppeid \$202 \$1234 \$201 Captain line You may enter a description here for your reference Perpaid \$202 \$1234 \$202 Crew line 1 You may enter a description here for your reference Perpaid \$202 \$1234 \$202 Crew line 1 You may enter a description here for your reference Perpaid \$202 \$1234 \$202 Crew line 1 You may enter a description	Extensions Voicemail CDR Logs Sat SIP Trunk RedPort VoIP ions g RJ-11 Telephone Description You way enter a description here for your reference Description You may enter a description here for your reference Description Prepaid 301 301 Captain analog line 0 Ktensions Payment Mode Extension Password Caller ID Description Value larger than 200 SIP extension password Free text You may enter a description here for your reference Postpaid 201 1234 201 Captain line Prev line 1 Prestraid 202 1234 202 Drew line 1 Prev line 2

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'.

VZW Wi-Fi 🗢	10:19 AM	100% 💻 🗲
🚊 🛛 Registra	tion in progress	
Enter a	a number o	ra 🖾
1∞	2	3
4	5	6
7	8	9
*	0+	#
20	Q	5) 1)
Θ	<u>ک</u>	Ø

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.

ATTACK AND AN ADDRESS OF TO AN ADDRESS AND	nd Filtering RedPort E	mail Remote Access SMS GPS	Tracking Dynamic DNS G	PS/NMEA Repeater Voice PBX	SNMP Network Shares
attings Management					
nagement					
reate Message					
Destination Phone Number		202			
Enter your SIP extension		201			
Message				and a second	
					A
Send Message		Send Message			
		Send the text messa	ige to the specified number		
Received Messages					
Filename	From	Message D	ate Respon	d delete	Select
		This spection contain	e eo universit		
		This secuon contains	s no values yet		
Sent Messages					
Sent Messages Filename	to	Message	Date	Delete	Select
Sent Messages Filename	to	Message This section contain:	Date s no volues yet	Delete	Select
Sent Messages Filename Remove messages	to	Message This section contain:	Date s no volues yet	Delete	Select
Sent Messages Filename Remove messages Select all messages	to	Message This section contain:	Date s no volues yet	Delete	Select
Sent Messages Filename Remove messages Select all messages Delete selected messages	to	Message This section contain Select MDelete Selected	Date s no values yet	Delete	Select
Sent Messages Filename Remove messages Select all messages Delete selected messages Delete all sent messeges	to	Message This section contain: Select MDelete Selected MDelete All Sent	Date s no valuas yat	Delete	Select
Sent Messages Filename Remove messages Select all messages Delete selected messages Delete all sent messages Delete all received messages	to	Message This section contain: Select Molete Selectod Molete All Sent Molete All Received	Date s no volues yet	Delete	Select

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 Er	mail Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares
Fracking	
racking Parameters	
able/disable tracking and set parameters. Standard airtime cha	rges apply.
General Tracking Parameters	
Enable Tracking	0
Tracking Interval	60 Specify the tracking interval in minutes.
Tracking powered by RedPort	
Please visit www.RedPortGlobal.com for registration information	
INMARSAT FleetBroadband	
Iridium OpenPort/Pilot	Ö
INMARSAT Isatphone	
VSAT or broadband satellite	🗌 🔘 A valid NMEA/GPS feed is required. Tracking IME1: 28913469999902.
Globalstar phone	🗌 🥝 A valid NMEA/GPS feed is required. Tracking IME1: 28913469999902.
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 Si	MS service
Iridium terminal/Aurora/MCG-101	A valid NMEA/GPS feed is required.
Recipient Email Address	user@domain.com
Yessel name	Enter optional vessel name and/or other free text.
Reset	Save & App

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.



E	
0	
Ū.	
🗌 🔞 A valid NMEA/GPS feed is required. Tracking IMEI: 626083925868886.	
🗌 🎯 A valid NMEA/GPS feed is required. Tracking IMEI: 626083925868886.	
🗌 🗐 A valid NMEA/GPS feed is required.	
1 1 1	A valid NMEA/GPS feed is required. Tracking IMEI: 626083925868886. A valid NMEA/GPS feed is required. Tracking IMEI: 626083925868886. 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. Star	dard airtime charges apply.								
General Tracking Parameters		1							
Enable Tracking	0								
Tracking Interval	80 Specify the tracking interval in minutes.								

-- / / --

r's SMS service	
🗌 🙆 A valid NMEA/GPS feed is required.	
user@domain.com	
Enter optional vessel name and/or other free text.	
	's SMS service

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.

RedPort



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.

Services Status System VPN Network Users Statistics Logout Home GPS Tracking Dynamic DNS GPS/NMEA Repeater Crew Internet Access Web Compression and Filtering RedPort Email Remote Access SMS Voice PBX SNMP Network Shares Dynamic DNS Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address. Hints Follow this link You will find more hints to optimize your system to run DDNS scripts with all options Show more 📄 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_jpv4' and 'myddns_jpv6' To change global settings click here Hostname/Domain Last Update Process ID Configuration Enabled **Registered IP** Next Update Start / Stop yourhost.example.com Never myddns_ipv4 Edit Nolete No data Disabled yourhost.examp<mark>l</mark>e.com No data Never Disabled myddns_ipv6 Edit Delete Add Reset Save Save & Apply

DRAFT

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.

Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Natwork Shares						
data over WiFi and Ethernet.						
😰 🖗 Enable GPS montioring and repeating.						
🗌 🎱 Pass raw binary data through without parsing for NNEA-183 sentenses.						
Use USB connected GPS or NMEA feed as a source. Note: Not compatible with RS-232 based satellite phones.						
IDIDI III Listen on UDP port number and rebroadcast.						
11101 Broadcast to UDP port number.						
11102 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.

ettings Extensions Voicemail CDR Logs Sat SIP Trun	inen hennite henese and era recking officially and erayment repeate the rack and recking and r
X Services	
Enable PBX	🔽 🞯 Enable/Disable PBX VOIP service.
Listen port	5060 Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.
Listen interfaces	ALL - 0000 +
Auto attendand (IVR)	Enable IVR to prompt for extension number and route call appropriately.
Enable voicemail	[9] Enable voicemail and directory dialing. Also create a default system voicemail box at extensions 0.

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.

RedPort

- 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.

ing	js E	Extensions Voicen	nail CDR Logs	Sat SIP Trunk F	RedPort VoIP					
en	sion	s								
IP	Exte	nsions								
Ring	SMS	Extension Value larger than 200	Password SIP extension password	Caller ID Free text		You may er	Description he	n re for your reference		
		201	1234	201	Captain line					Delete
		202	1234	202	Crew line 1					Delete
\Box		203	1234	203	Crew line 2					Delete
\square	\Box	204	1234	204	Crew line 3					Delete
1 Ad	d									

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**)

VZW Wi-Fi 🗢	10:19 AM	100% 🚥 🔸
🗮 🛛 Registra	tion in progress	
Enter a	number o	ra 🖾
1∞	2	3
4	5	6
7	8	9
*	0+	#
2	Q	\$ \$
Θ	A 🗱	Ø

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:

attings Sutansians Valcomail CDD Long Sat CDD	
errings extensions voicement core cogs becare	Hunk - Henrik Vur-
X Services	
Enable PBX	🖉 🗿 Enable/Disable PBX V01P service.
Listen port	F060 Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.
Listen interfaces	ALL - 0.0.0.0 9 Bind proxy to the following interfaces.
Auto attendand (IVR)	🗐 😳 Enable IVR to prompt for extension number and route call appropriately.
Enable voicemail	🗷 😳 Enable voicemail and directory dialing. Also create a default system voicemail box at extensions 0.
Volcernail password	1234 Password for system voicemail box.
Voicemail to email	😿 🔘 Deliver voicemail destined for system voicemail box via email.
Voicemail email address	adickson@globalmarinenet.com Deliver volcemail to default system mailbox to this email address.
Delete voicemail	📄 🟮 Remove volcemail sent to default system mailbox after deliver via email.

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:

ettings	s Exte	ensions	Voicem	ail CDR Lo	is Sat SIP Trunk	RedPort VoIP	racking bynamic bivo	GF3/NHLA Nepeater	VOICE PBA	June	Network Sindle
icen	nail Se	etup									
Exten	nsion 41	1 for co 9 to ac	ompany din cess voicen	ectory. nail. Enter extens	on 0 to access com	ipany mailbox.					
Exten Exten RedPo	nsion 41 nsion 99 ort Ema Extensi	1 for co 9 to ac 1 must	per enabled	ectory. nail. Enter extens I when using ema	on 0 to access com il delivery of voicer	ipany malibox. nail.					
Exter Exter RedPo SIP E Ring	nsion 41 nsion 99 ort Ema Extensi Enable	I for co 9 to ac il must ons Email	be enabled	ectory. nail. Enter extens I when using ema Extension 📄	ion 0 to access com il delivery of voicer Password	ipany mailbox. nail. Users Name		Email Add	iress		
Exter Exter RedPo SIP E Ring	nsion 41 nsion 99 ort Ema Extensi Enable	I for co 9 to ac 1 must 0ns Email	Del after send	ectory. nall. Enter extens I when using ema Extension 📄	ion 0 to access com il delivery of voicer Password VM password	ipany mailbox. nail. Users Name Used by company directory dial by na	ne	Email Add	fress for voicemail		
Exter Exter RedPo SIP E Ring I	nsion 41 nsion 99 ort Ema Extensi Enable	I for co 9 to ac il must ons Email	Del after send	ectory. nall. Enter extens I when using ema Extension e 201	on 0 to access com il delivery of voicer Password VM password 1234	pany mailbox. nail. Users Name Used by company directory dial by na Aaron Dickson	ne adickson@globalmarine	Email Add Email destination net.com	dress for voicemail		
Exter Exter RedPo SIP E Ring	Insion 41 Insion 99 Instema Extensi Enable	I for co 9 to ac 1 must 0ns Email	Del after send	ectory. nail. Enter extens i when using ema Extension 201 202 202	Password VM password 1234 1234	pany mailbox. nail. Users Name Used by company directory dial by na Aaron Dickson	ne adickson@globalmarine	Email Add Email destination net.com	dress for voicemail		
Exter Exter RedP	Enable	I for co 19 to ac ill must ions Email	Del after send	ectory. nail. Enter extens i when using ema Extension 201 202 203 204	on 0 to access com il delivery of voicer Password VM password 1234 1234 1234	pany mailbox. nail. Users Name Used by company directory dial by na Aaron Dickson	ne adickson@globalmarine	Email Add Email destination net.com	for voicemail		

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.

RedPort

3	
erate CDR (Call Data Records).	
claimer: CDR call duration and billing seconds may	differ from the actual billed units. These records are approximate values and should not be used to resolve billing disputes.
Reporting Period	(24 hours 🛟)
	Current Date/Time through selected interval.
Submit	Submit
Enter Filename	cdr-2018-02-25.csv
Download CSV	🖉 Download
Trim CDR	* Delete
	Ø Delete CDRs from system older than the reporting interval.
Purge CDR	Purge
	e remove di constront system.

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.

ome Services Status System	/PN Network Users Statistics Logout
rew Internet Access Web Compression	nd Filtering RedPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares
ettings Extensions Voicemail CD	Logs Sat SIP Trunk RedPort VoIP
gs and Status	
Active Calls	
Hangup all calls	quaneti
Channel Location State App O active channels O active calls O calls processed	ation(Data)
Vobal Decoder	
Decoder is disabled. Please contact your pr	ider for an activation code should you wish to enable the service.
PBX Status	
Restart PBX	Restart
SIP Status	
Name/username Host 100 (Unspecified) 101 (Unspecified) 201 (Unspecified) 202 (Unspecified) 203 (Unspecified) 204 (Unspecified) 6 sip peers [Monitored: 0 online, 6 offline U	Dyn Forcerport Comedia ACL Port Status Description D Auto (No) No 0 UNKNOWN D D online, 0 offline] ////////////////////////////////////
00	
Clear log entry	Ciear .
Download log	Download
[Apr 16 14:14:02] Asterisk 11.12.0 built by Isi [Apr 16 14:14:02] NOTICE[14012] edr.: CDF [Apr 16 14:14:02] WARNING[14012] eal.c: C [Apr 16 14:14:02] WORNING[14012] leader.c: 4 [Apr 16 14:14:02] WARNING[14012] leader.c. [Apr 16 14:14:02] NOTICE[14012] res_smdi. [Apr 16 14:14:02] NOTICE[14012] res_smdi. [Apr 16 14:14:02] WARNING[14012] leader.c.	ero @ ubuntu on a x86_64 running Linux on 2018-04-10 18:46:46 UTC imple logging enabled. Id not load cel.conf modules will be loaded. irror loading module 'res_musiconhold.so': File not found Unable to load config smol.conf: SMDI disabled No SMDI interfaces are available to listen on, not starting SMDI listener. irror loading module 'res_musiconhold.so': File not found

DRAFT

- 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.

RedPort

v internet Access web compression and Fittering Rei	dPort Email Remote Access SMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP Network Shares
ings Extensions Voicemail CDR Logs Sat S	IP Trunk RedPort VoIP
or FBB and iSavi VOIP Configuration	
tion Sailor users. Refer to the IP Handset configuration	n section in the Sailor FBB users guide.
IP Handset compatability under "Settings->IP Hands	ets->Server settings" on the Sailor FBB needs to be set to "version 1.8 or newer".
able	
rce Terminal Selection	💋 🕲 Do not auto-detect satellite terminal
itellite Terminal	Sailor F8B \$
Address of Terminal	System default
	Leave blank for system default.
P Extension	0501
	Value must be 501 through 504.
P Password	0501

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

5.8.6. 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.

ettings Extensions Volcemail CDR Logs Sat SIP Trunk	adPort VoIP
bal Decoder	
Mac Address	F490EA000156
Mode	[IAX +] IAX uses one socket for all communication. SIP uses a socket for control and a different socket for RTP media.
Activation Key	U2Fsd@VkX1/NH3T3tqD9SsudLZR2K+wfqF7TCOxxkjBKOrQDmgIF1XVKLPAgRf06OKpKbL1oH9Lhlojs6//pdw==
	A valid activation key must be entered to use this service. Additional charges will apply. Please contact your provider for a key.

Enter the Key and click <Save & Apply>.

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/INEA Repeater Voice PBX SNMP Network Shares
Settings Extensions Volcemail CDR Logs Sat SIP Trunk	RedPort VoIP
Vobal Decoder	
	3
Mac Address	F490EA000156
Mode	AX A
Activation Key	U2FsdGVkX1/NH3T3lqD95sudLZR2K+wlqF7TC0xxkjBKOrQDmglF1XVKLPAgRfG80KpKbL1oH9Lhlejs6//pdw≈ =
	A valid activation key must be entered to use this service. Additional charges will apply. Please contact your provider for a key.
	Deactivate Wote: This action disables voice calling through this unit but does not deactivate the service. You must contact your provider to terminate service. Pushing this button will not cancel your subscription.
UID	21481
DID	12148121481
Reset	💭 Save . 🛄 Save & Apply

DRAFT

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**.

ng	s E	t Access We Extensions	b Com Voicen	pression and Filtering	RedPort Erna Sat SIP Trunk	II Remote RedPort V	Access S	IMS GPS Tracking Dynamic DNS GPS/NMEA Repeater Voice PBX SNMP	Network Shares
en	sion	s							
ng	Pay	yment Mode	one	Extension	Caller ID			Description	
			Value	larger than 200	Free text			You may enter a description here for your reference	
2	prep	aid 🕈	301	301		Captain analog	g line 0		
	prep	aid 🕴	302	302		Crew analog li	ne 1		
	prep	baid 🕴 🕇	303	303]	Crew analog li	ne 2		
0	prep	aid 🛟	304	304		Crew analog li	ne 3		
IP	Exter	sions							
ling	SMS	Payment M	lode	Extension	Password	i (aller ID	Description	
				Value larger than 200	SIP extension pas	isword	Free text	You may enter a description here for your reference	
		prepaid	\$	201	1234	201		Captain line	Delete
O		prepaid	\$	202	1234	202		Crew line 1	Delete
0		prepaid	\$	203	1234	203		Crew line 2	Delete
0	0	prepaid	;	204	1234	204		Crew line 3	Delete
	9 1910 - 1				89	222		24	

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.

MP Settings	
ecute "Save & Apply" to apply settings and restart SNMP daemon. General	
Enable	🖉 😰 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	bffice
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.
sys5ervices	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 SML enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining "what kind of box's is being managed.

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

work shares					
amba					
Seneral Settings Edit Template					
Hostname		Optimizer			
Description		RedPort Optimizer Shares			
Workgroup		RedPort			
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 			
hared Directories	Path	Allowed users	Read-only	Allow guests	
Share name	Relative directory path	A comma separated list			
ransferio	transferin	adtest			Delete
MINT NO. 11	transferout	16		2	Delete
ransferOut					
iransferOut					
randferOut *]Add Isers					
ransferOut _Add Isers	Username	Password			
iraneferOut i Add Jsers adtest	Username	Password	I		()Delete

DRAFT

Click <Add> to create a new Shared Directory:

Name	Path	Allowed users	Read-only	Allow guests	
Share name	Relative directory path	A comma separated list			
ansferIn	transferin	adtest			Delete
ansferOut	transferout				Delete

- **Name:** This is the Share Name that is visible on the network. It is the 'volume' name that you will use when connecting to the shared directory.
- Path: This is the name of the Folder that appears on the Optimizer that will be used to store files.
- Allowed users: You can limit the users that have access to the files in the Path Folder by assigning usernames and passwords to selected individuals (see Add Users below). Enter the usernames here, separated by a comma if more than one user will have access to the files.
- **Read-only:** Use this checkbox to protect the files in the Path Folder from being changed.
- Allow guests: Use this checkbox to make the files available to anyone with network access. With this box checked, users will not be prompted to enter a username and password when accessing the Path Folder.
- **Delete:** Use this to delete the Shared Directory. 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.



 Users		
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.

Conne Conne	et to Server	
Server Addrees:		
smb://10.1.5.1/transferin		+ 0*
Favorite Servers:		
2 Banoya	Browse	Consect

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.

***	Enter your na "10.1.5.1".	me and password for the server
	Connect As:	 Guest Registered User
	Name:	adtest
	Password:	••••
	C Rememb	er this password in my keychain
		Cancel Connect

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.

© 2018 RedPort Global Powered by Global Marine Networks, LLC.





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.

Specify the dr	ive latter for the co				
	IAG ACTECT TEX ALC CO	nnection and the fold	er that you	want to connect i	tor
	~	./			
Unive:					
Folder	\192.168.10.1\trans	lerin 🦰		Browse.	
E	xample: \\server\sh	are			
	Reconnect at log	on			
	Connect using dif	ferent credentials			
0	innect to a Web si	te that you can use to	store your o	tocuments and o	lictures.
					1

Click <Finish>.

inter Ne	twork Password	
nter your p	assword to connect to: 192.168.10.1	
	User name	
	Password	
	Domain: WIN7X64	

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).

RedPort

G () + 🖙 + Computer + Transferlin(W38	2.168.10.1(V)				• 4;] Search Transferk	- (N.192360.02	2 14 (V.)	P
Organize + Bum Newfolder						道•		0
🔆 Favorites	Name	Datemodified	Type	Size				
Desktop Downloadt	+ Atlantic_precipitation	9/20/2016-6-23 ADA	giób file	24 KB				
Documents Music Pictures								
1 Videos								
🖏 Homegroup								
Computer								
Transferio(9.192.168.10.1)(V)								



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).

seem secongs	
e you can configure the basic aspects of your device like	e its hostname or the timezone.
ystem Properties	
General Settings Logging Language and Style	
local Time	Sun Feb 25 19:51:30 2018 Sync with browser
Hostname	Dptimizer
Fimezone	(UTC ¢)
Disable anti-lockout rule	The ani-lockout rule prevents creating firewall rules that block access to the web admin and ssh ports. Note that this could cause security issues since these ports will remain open on all interfaces. The rule is enabled when option is unchecked.
ime Synchronization	
Enable NTP client	0
Provide NTP server	0
NTP server candidates	0.openwrt.pool.ntp.org
	3.openwrt.pool.ntp.org

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.

RedPort

uter Password			
hange Password			
ange password for the superadmin user.			
Password		21 22	
Confirmation	2		
hange Password pance the password for the admin user. This pass	word does not apply to the superadmin account.		
Password	3	8	
Confirmation			
contribution		IV	

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.

system Administration	Profiles Backup / Flash Firmware Reboot	
Profiles Tools		
rofile Manager		
morizon the current re	the south a south a south to the south of south a s	
Manage Profiles	Description	
Manage Profiles Profile WiffExtenderProfile	Description Removes the BIZ port and converts it to a wifi extender port for use with the Halo Wifi extender	Install 💌 Dolot
Manage Profiles Profile WiffExtenderProfile Factory	Description Removes the BIZ port and converts it to a wifi extender port for use with the Halo Wifi extender Factory default settings	instali X Delet

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:

Profiles Tools					
ofile Manager					
Manage Profiles	uter configuration and stores it in the named profile.				
Floring	Removes the BIZ port and converts it to a wifi extender part for use with the Halo Wifi extender	🛄 Install 💌 Delete			
WifiExtenderProfile		Industrial Manager			
WifiExtenderProfile Factory	Factory default settings				

- 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:

System Administration	Promies Backup / Hash Firmware Reboot	
Profiles Tools		
rofile Manager		
create predenined roat		- 1월 4월 28일 6월 5월 28일 8월 28일 8월 18일
Manage Profiles Profile	ter configuration and stores it in the named profile. Description	
Manage Profiles Profile WiflExtenderProfile	ter configuration and stores it in the named profile.	🚺 Install 💌 Defet
emorizes the current ro Manage Profiles Profile WiflExtenderProfile Factory	Iter configuration and stores it in the named profile.	Instell XDelet

- 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:

ome Services Status System VPN Network	Users Statistics Logout
ystem Administration Profiles Backup / Flash Fin	are Reboot
rofiles Tools	
ols	
elect and Install Profiles	
Profiles	Factory Defaults \$
	Select profile to install and then Apply
	ДАрруу
mport/Export Profiles	
Export Filename	profiles-2018-02-25.1gz
	Export
	Export all profiles and download
Import Filename	Choose File no file selected
	Import
	Import previously exported profiles

- 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.

elect and Install Profiles		
Profiles	Factory Defaults +	
	САрру	
nport/Export Profiles		
Export Filename	profiles-2018-02-25.tgz	
	Export Export all profiles and download	
Import Filename	Choose File no file selected	
	mport mort previously exported profiles	

- 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.

667 - Will Malay	
Factory Defaults Select profile to install and then Apply	
Шарру	
profiles-2018-02-25.tgz	
Export Export Export all profiles and download	
Choose File no file selected	
Import Import previously exported profiles	

- 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.
Status System VPN Network Users Statistics Logout Services System Administration Profiles Backup / Flash Firmware Rebo Flash operations Actions Configuration Backup / Restore Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images). Generate archive Download backup: Reset to defaults: Perform reset To restore configuration files, you can upload a previously generated backup archive here. Restore backup Choose File no file selected Upload archive... Flash new firmware image Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Optimizer compatible firmware image). It is usually best to leave "Keep settings" unchecked. Keep settings: Image: Choose File no file selected Flash image... Flash SD drive image Restore SD drive configuration files factory defaults. Reset to defaults: Perform SD reset Upload an SD image here to replace the current disk image. Check 'Download from Internet' to download image over the Internet (Note that this requires a fast Internet connection). Reformat SD drive before updating image: Download from Internet: SD image: Choose File no file selected Elash SD image... SD Disk Upgrade A new version "1.05" of the SD disk image is available. The current SD disk image version is "no current version". Update SD Image...

DRAFT

7.4.1. Backup/Restore

lick "Generate archive" to download a tar archive	of the current configuration files. To reset the firmware to its initial	state, click "Perform reset" (only possible with squashfs images).
Download backup:	Cenerate archive	
Reset to defaults:	Perform reset	
restore configuration files, you can upload a pre	viously generated backup archive here.	
		(Final Control of Cont

- **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).

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

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

DRAFT

Flash new firmware image Upload a sysupgrade-compatible image here to	place the running firmware. Check "Keep settings" to retain the current configuration (requires an Optimizer compatible firmware image).	It is usually
Keep settings:	0	
Image:	Choose File no file selected IFlash image	

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.

Optimizer wXa-524 v2.10 Load: 0.11 0.16 0.08	Optimizer wXa-524 v2.10

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.

Reset to defaults:	Perform SD reset					
pload an SD image here to replace the current disk image. Che	ck "Download from Internet" to download image ove	r the Internet (Note that this requires a fast Internet connection).				
Reformat SD drive before updating image:	0					
Download from Internet:	D.					
SD image:	Choose File no file selected					
5D Disk Upgrade						
new version "1.05" of the SD disk image is available. The curre	ent 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:

Home Services Status System VPN Network Users Statistics Logout									
System Administration Profiles Backup / Flash Firmware Reboot									
System									
Reboot									
boots the operating system of your device									
Warning: There are unsaved changes that will be lost while rebooting!									
Perform reboot									



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

tings Users			
ettinge			
ettings			
nable			
ocal IP		192.168.20.1 Usually an IP on a unique subnet (ic. not LAN)	
emote IP Range		20-30 Remote host IP range in the same network as the local IP, i.e. 20-30 for 192.168.20.20-50	
iset		🦉 Sav	e 🛄 Save E
me Services Status System	VPN Network Users Statis	Sav	e Save B
me Services Status System TP IPSec OpenConnect VPN Op	VPN Network Users Statis	Sav	e USave &
me Services Status System TP IPSec OpenConnect VPN Op ttings Users TP VPN	VPN Network Users Statis pen/VPN	Sav	e Save &
me Services Status System TP IPSec OpenConnect VPN Op ttings Users TP VPN PN users	VPN Network Users Statis penVPN	Sav stics Logout	e Save 8
re Services Status System TP IPSec OpenConnect VPN Op ttings Users TP VPN PN users Name	VPN Network Users Statis penVPN Password	Elics Logout	e Save 8
eset TP Services Status System TP IPSec OpenConnect VPN Op ttings Users TP VPN PN users Name Add	VPN Network Users Statis penVPN Password	Rikes Logout Comment This section contains no values yet	e USeve &

8.2. IPSec

IPSec - Internet Protocol Security

PPTP IPSec OpenConnect VPN OpenVPN IPSec Configuration Connections Phase 1 proposals	Phase 2 proposals Tunnels IPSec Logs
IPSec Configuration	
Note: IPSec tunnels are torn down and restarted only whe	nitting "Save & Apply" on this screen. "Save & Apply" on other screens will save the settings but not restart the tunnels.
IPsec Configuration	
Listen Interfaces	loopback lan V biz ppp ptp cap wan wan
Firewall Zone	lan 🗘
Add to Routing Table	Yes Adds routes for ipsec tunnel to the system routing table.
Debug Level	(Basic 4)

DRAFT

8.3. OpenConnect VPN

Home Services Status System VPN Network Users	Statistics Logout
PPTP IPSec OpenConnect VPN OpenVPN	
Server Settings User Settings	
penConnect VPN	
OpenConnect	
General Settings CA certificate Edit Template	
Enable server	0
Server's certificate SHA1 hash	F9A4BDEEC58471661657FE303D2D8F97C4A8F670 That value should be communicated to the client to verify the server's certificate
Server's Public Key ID	sha1:CE097B2A92599658D9D102A1C29814D3CAB61BD3 An elternative 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: Ian: Ian: ppp: ppp: ppp: ppp: vpn: ppto: wan: wan2:
Port	The firewall zone that the VPN clients will be set to
Max clients	
Max same clients	2
Dead peer detection time (secs)	
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	
IF	P Address
8.6.8.8	M Delete
bbA	
Routing table The routing table to be provided to clients: you can mix IPv4 and IPv5	i routes, the server will send only the appropriate. Leave empty to set a default route
IP Address	Netmask (or IPv6-prefix)
192.168.10.0	255,255,255,0 ± 1
1 Add	
Resct	Save Save S Apply
Management of the second s	

DRAFT

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 Start custom_config no 1194 udp Edit Delete 0 Start Edit Delete sample_server no 1194 udp sample_client no Start 1194 udp Edit Delete Client configuration for an ethernet 🔹 🔛 Add 🕴 Reset Save Save & Apply

DRAFT

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.

Home Servic	ces Status	Syste	m VPN	Network Users	i Statistics	Logout						
Diagnostics	Interfaces	Wifi	VLAN Switch	DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
iagnostics												
Network U	tilities											
dev.openwrt.org)			dev.op	enwrt.org			[dev.open	wrt.org		
IPv4 🗘 🛄 F	ing			🛄 Tra	ceroute				Nsioo	kup		
				Instal	l iputils-tracer	oute6 for IPv6 tr	aceroute					

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**).

DRAFT

orfacor		
endes		
nterface Overview		
Network	Status	Actions
WAN6	Uptime: 0h 0m 0s	
Øwan	RX: 8.32 MB (90902 Pkts.) TX: 929.69 KB (7386 Pkts.)	👸 Connect. 🥘 Stop 🛛 🔏 Edit 💌 Delet
CAP	Uptime: 14h 18m 33s	
Æ	RX: 81.55 KB (884 Pkts.)	🦉 Connect 🥘 Stop 📝 Edit 💌 Delet
tun0	TX: 365.31 KB (1016 Pkts.) IPv4: 10.1.5.1/24	
BIZ	Uptime: 14h 19m 6s	
	RX: 0.00 B (0 Pkts.)	🖉 Connect 🙆 Stop 📝 Edit 💌 Delet
eth3	TX: 0.00 B (0 Pkts.) IPv4: 192.168.11.1/24	
	Uptime: 14h 19m 6s	
LAN	MAC-Address: F4:90:EA:00:01:56 RX: 156.73 KB (1105 Pkts.)	
br-lan	TX: 391.21 KB (1092 Pkts.) IPv4: 192.168.10.254/24 IPv6: fd49:4e9d:af71::1/60	ing Connect 🥥 stop 😰 Eait 🔀 Delet
PPP	Uptime: 14h 12m 28s	
0qqq	FX: 40.19 KB (615 Pkts.) TX: 49.72 KB (881 Pkts.) IPv4: 10.247.113.122/32	🤔 Connect 🏼 🥮 Stap 🛛 🛣 Edit 💌 Delet
РРТР	MAC-Address:	
ppp11+	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	🖉 Connect 🥘 Stop 🛛 Edit 💌 Delet
WAN	Uptime: 14h 18m 56s	
Æ	RX: 8.32 MB (90902 Pkts.)	🤔 Connect 🥘 Stop 📝 Edit 💌 Delet
eth0	TX: 929.69 KB (7386 Pkts.) IPv4: 192.168.0.79/24	
WAN2	Uptime: 0h 0m 0s	
E.	MAC-Address: F4:90:EA:00:01:55 RX: 0.00 B (0 Pkts.)	🔗 Connect 🧔 Stop 📝 Edit 💌 Delet
eth1	TX : 0.00 B (0 Pkts.)	
Add new interface		
lobal network options		
Pv6 ULA-Prefix	fd49:4e9d;af71::/48	

- **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

RecPort Stop Edit Delete

- 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.

lame of the new interface	The allowed characters are: A-Z, a-z, 0-9 and _
lote: Interface name length	Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe-etc.)
rotocol of the new interface	Static address ÷
reate a bridge over multiple interfaces	
Cover the following interface	Ethernet Adapter: '@wan' (wan6) Ethernet Adapter: 'eth0' (wan, wan6) VLAN Interface: 'eth0.11" Ethernet Adapter: 'eth1' (wan2) VLAN Interface: 'eth2' (lan) VLAN Interface: 'eth2' (lan) VLAN Interface: 'eth2'.11" Ethernet Adapter: 'eth3'' (wext) Ethernet Adapter: 'gretap0" Ethernet Adapter: 'teq10" Ethernet Adapter: 'teq0" Ethernet Adapter: 'teq0" Ethernet Adapter: 'teq0" Wireless Network: Master "wXa-524-0154-2.4GHz" (lan) Wireless Network: Master "wXa-524-0154-5GHz" (lan)

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.

Home	Servi	ices Statu	5	Syste	n	VPN	Netwo	k Users	Statistics	Logout						
Diagnos	stics	Interfaces	W	lífi	VLAN	Switch	DHC	P and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
PPTP	WAN	WAN2	PPP	LAI	4 (CAP	WEXT	WAN6								

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



Common Configu	ration			
General Setup Ad	dvanced 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.

ome Services Status System VPN Network Use	ers Statistics Logout
agnostics Interfaces Wifi VLAN Switch DHCP and DM	S Hostnames Static Routes Firewall Packet Capture PPP SQM QoS DSCP QoS Failover/Load Balancing
AN2 WAN BIZ PPTP LAN CAP PPP WAN6	
erfaces - BIZ	
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
ces. You can also use VLAN notation INTERFACE.VLANNR (e.g	;; eth0.1).
General Setun	Finguist Sattinge
Status	Intime: 14b 24m 45c
	Image: Second
Protocol	(Static address +
IPv4 address	192.168.11.1
IPv4 n <mark>etmask</mark>	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	Dublic apply south to this douise for distribution to cliente
	Public prenx routes to this service for distribution to clients.
HCP Server	
General Setup Advanced Settings IPv6 Settings	
Ignore interface	Oisable DHCP for this interface.
Start	100
Limit	150 Ø Maximum number of leased addresses.
Leasetime	12h Expiry time of leased addresses, minimum is 2 minutes (2m).
ack to Overview 🙆 Reset	Save & A

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.

RedPort

erfaces - BIZ	44 										
his page you can xes. You can also	configure the netwo use VLAN notation II	rk interfaces. You ca NTERFACE.VLANNR (e	n bridge several .q.: eth0.1).	interfaces by tic	king the "bridge	interfaces" field a	nd enter the na	imes of sever	al network interfaces separated		
ommon Config	guration										
Seneral Setup	Advanced Settings	Physical Settings	Firewall Settin	gs							
Bring up on boot			9	2							
Jse builtin IPv6-n	nanagement		1	2							
override MAC add	Iress		I	F4190/EA100101157							
Override MTU			I	1500							
Jse gateway met	ric			0							
HCP Server General Setup	Advanced Settings	IPv6 Settings		Disable DH	CP for this interface	2.					
Start				100 Lowest leased	address as offset f	rom the network a	ddress.				
Limit				150 a Maximum number of leased addresses.							
			I	12h Expiry time of	leased addresses,	minimum is 2 min	utes (2m).				

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.

AN2 WAN BIZ PPTP LAN CAP PPP 1	WAN6
erfaces - BIZ	
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 separate
ommon Configuration	
Seneral Setup Advanced Settings Physical Set	tings Firewail Settings
Bridge interfaces	@ creates a bridge over specified interface(s)
nterface	<pre>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: "gretap0" Ethernet Adapter: "teql0" Ethernet Adapter: "wwan0" Wireless Network: Master "wXa-524-0154-2.4GHz" (lan) Vireless Network: Master "wXa-524-0154-5GHz" (lan) Custom Interface: []]</pre>
HCP Server	
General Setup Advanced Settings IPv6 Setting	5
	U Usable DHCP for this interface.
	 Lowest leased address as offset from the network address.
lmit	150 Maximum number of leased addresses.
easetime	12h

DRAFT

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.

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.VLANNA (e.g.: eth0.1). **Common Configuration** General Setup Advanced Settings Physical Settings Firewall Settings Create / Assign firewall-zone 🔿 cap: cap: 🛃 lan: lan: 🖉 👳 💇 biz: 🧝 0 🔿 ppp: ppp: 💼 🔿 vpn: pptp: 🛃 🔿 wan: wan: 🧾 wan2: 🧾 unspecified -or- create: Ochoose 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 100 Lowest leased address as offset from the network address. 150 Limit Maximum number of leased addresses. 12h Expiry time of leased addresses, minimum is 2 minutes (2#) Leasetime 🖻 Back to Overview 🧐 Reset Save 🛄 Save & Apply

DRAFT

9.2.3.5. DHCP Server - General Setup

General Secup Advanced Securitys 1946 Securitys	
Ignore interface	Disable DHCP for this interface.
Start	100
	Uncomest leased address as offset from the network address.
Limit k	150
	Maximum number of leased addresses.
Leasetime	12h
	Expiry time of leased addresses, minimum is 2 minutes (2m).

9.2.3.6. DHCP Server Advanced

RedPort

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.
Pv4-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.

9.2.3.7. DHCP Server IPv6 Settings

outer Advertisement-Service	disabled	*)	
HCPv6-Service	disabled	•	
DP-Proxy	disabled	*)	
nnounced DNS servers		1	
nnounced DNS domains			

9.3. WiFi

Requires "superadmin" login.

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

dio0: M	aster "wXa-524-0154-2,4GHz	r" radio1: Master "wXa-524	-0154-5GHz"										
reles	s Overview												
R	Generic MAC80211 80 Channel: 6 (2.437 GHz) B	02.11abgn (radio0) litrate: ? Mbit/s								a	Scan		Add
	SSID: wXa-524-0154-7 0% BSSID: F4:90:EA:00:0	2.4GHz Mode: Master 11:56 Encryption: None						١	Disable		Edit		Remove
<u>@</u>	Generic MAC80211 80 Channel: 36 (5.180 GHz)	D2.11abgn (radio1) Bitrate: 144.4 Nbit/s								Q	Scan		Add
	SSID: wXa-524-0154 100% BSSID: F4:90:EA:00	I-5GHz Mode: Master :01:56 Encryption: None						0	Disable		Edit		Remove
ocia	ted Stations												
	SSID	MAC-Address	IPv4-Addres	s Signal	Noise		RX R	ate			TX R	ate	
	wXa-524-0154-5GHz	EC:35:86:3B:80:84	?	-32 dBn	n 0 dBm	130.0 M	1bit/s, M	CS 15, 20MHz	z	144.4	Mbit/s, M	CS 15, 2	OMHz

RedPort



- 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.

dio0: M	laster "wXa-524-0154-2.4GH	z" radio1: Master "wXa-524	4-0154-5GHz"			 -			-		-	-
reles						 						
	Generic MAC80211 8 Channel: 6 (2.437 GHz)	D2.11abgn (radio0) Bitrate: ? Mbit/s							a	Scan	1	Add
	SSID: wXa-524-0154- 0% BSSID: F4:90:EA:00:0	2.4GHz Mode: Master 01:56 Encryption: None						Disable		Edit		Remov
<u>®</u>	Generic MAC80211 8 Channel: 36 (5.180 GHz)	02.11abgn (radio1) Bitrate: 144.4 Nbit/s							Q	Scan		Add
	SSID: wXa-524-0154 100% BSSID: F4:90:EA:00	1-5GHz Mode: Master :01:56 Encryption: None						Disable		Edit		Remov
ocia	ted Stations											
	SSID	MAC-Address	IPv4-Addre	ss Signal	Noise	 RX R	ate			TX R	ate	
							No. of Concession, Name					

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: ☑ lan: ☑ ppp:	

- 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.

iagnosti	cs Interfaces Wifi V	LAN Switch DHCP and DN	S Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failo	ver/Load B	Balancing	9
adio0: M	laster "wXa-524-0154-2,4GH	radio1: Master "wXa-52	4-0154-5GHz"										
ireles	s Overview												
	Generic MAC80211 8(Channel: 6 (2.437 GHz) E)2.11abgn (radio0) litrate: ? Mbit/s								Q	Scan		Add
	<pre>ssiD: wXa-524-0154-3 0% BSSID: F4:90:EA:00:0</pre>	2.4GHz Mode: Master 11:55 Encryption: None						.0	Disable		Edit		Remov
®	Generic MAC80211 80 Channel: 36 (5.180 GHz)	02.11abgn (radio1) Bitrate: 144.4 Mbit/s								۵	Scan		Add
	SSID: wXa-524-0154 100% BSSID: F4:90:EA:00	I-5GHz Mode: Master :01:56 Encryption: None							Disable		Edit		Remov
socia	ted Stations												
	SSID	MAC-Address	IPv4-Addr	ess Signal	Noise		RX R	ate			TX R	ate	
	wXa-524-0154-5GHz	EC:35:86:3B:80:84	?	-32 dBn	0 dBm	130.0 M	bit/s, M	CS 15, 20MHz	2	144.4	Mbit/s, M	CS 15, 3	20MHz

Locate the wXa WiFi network and click <Edit>.

Interface Configuration		
General Setup Wireless Security MAC-Filter		5
Encryption	No Encryption 🗘	
Carlo M M SANCARI M		

- 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.

Home	Services	Status	System	VPN	Network	Users	Statistics	Logout						
Diagnos	tics Int	erfaces	Wifi VLA	N Switch	DHCP a	nd DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
Switch	1													
The netw segment	vork ports s. Often t	on this de here is by (vice can be default one	combine Uplink p	ed to sever ort for a co	al VLANs	in which cor to the next	nputers can com greater network	municate d like the int	lirectly with each ernet and other p	other. V orts for	LANs are off	ten used to s vork.	eparate different network
Swite	ch "eth0													
VLAN	ls on "et	h0"												
				v	LAN ID									
11 Made	i								off				\$	× Delete
Swite	h "eth1													
VLAN	ls on "et	h1"												
				v	LAN ID									
11	1								off				\$	× Delete
Swite	ch "eth2													
VLAN	ls on "el	h2"												
				v	LAN ID									
11									off				\$	Delete
Add	1													
Reset	_													Save Save Save & Apply

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.

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 **DHCP and DNS** Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls Server Settings General Settings Resolv and Hosts Files TFTP Settings Advanced Settings Domain required 🕑 🧐 Don't forward DNS-Requests without DNS-Name Authoritative This is the only DHCP in the local network Local server Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only Local domain Local domain suffix appended to DHCP names and hosts file entries Log queries Write received DNS requests to syslog DNS forwardings /e: List of DNS servers to forward requests to Rebind protection Discard upstream RFC1918 responses Active DHCP Leases Hostname IPv4-Address MAC-Address Leasetime remaining There are no active leases. Active DHCPv6 Leases IPv6-Address DUID Leasetime remaining Hostname There are no active leases. Static Leases Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the Add Button to add a new lease entry. The MAC-Address indentifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host. Hostname MAC-Address IPv4-Address IPv6-Suffix (hex) This section contains no values yet Add Reset Save Save & Apply

DRAFT

9.6. Hostnames

Requires "superadmin" login.

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

	Wifi VLAN Switch	DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/L	oad Balancing
tnames											
lost entries											
	Hostname					IP address					
			C							•	and Chalanta
Optimizer			127.0.0.1							÷.	Delete

9.6.1. Add Hostname

RedPort

agnostics Interfaces Wifi VLAN Switch DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/L	oad Balancing
names									
Hostname				IP address					
)ptimizer	127.0.0.1							\$	Delete
lewHostName	*							•	Delete
- Acid	192.168.0.1 (00:0d:b9:29:68:10) - 192.168.0.254 (00:0d:b9:24:5a:34) custom								
Reset									Save Save

- 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.

agnostics Interfaces Wifi VL	AN Switch DHCP and DNS Hostn	ames Static Routes Firewall Packet Co	apture PPP SQM QoS DSCP	QoS Failover/Load Balancing
utes				
tes specify over which interface an	nd gateway a certain host or network	can be reached.		
tatic IPv4 Routes				
Interface 📄	Target	IPv4-Netmask	IPv4-Gateway	Metric MTU
	Host-IP or Network	if target is a network		
		This section contains no values yet		
Add				
tatic IPv6 Routes				
Interface 🖭	Та	rget	IPv6-Gateway	Metric MTU
	IPv6-Address o	Network (CIDR)		
		This section contains no values yet		
Add				

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.

neral Settings Port Forwards Firewall Rules IPset I	P Proxy					
rewall - Zone Settings						
e firewall creates zones over your network interfaces to contr General Settings	ol network traffic fi	ow.				
Enable SYN-flood protection						
Drop invalid packets						
Input	rejec	it	\$)			
Output	acce	pt	;)			
Forward	rejec	t	*)			
Zones						
Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
ppp: ppp: 📷 → REJECT	reject	<pre>\$) accept</pre>	reject	• 🛛	0	Edit Delete
cap: cep: 🖉 ⇒ ACCEP7	accept	¢ accept	accept	•) 🛛	0	Edit Delete
lan: lan: 🚂 🙊 👷 biz: 🚑 → ppp wan	reject	¢) accept	reject	•	0	ZEdit Delete
wan: wan: 🛃 wan2: 🛃 ⇒ REJECT	accept	<pre>\$) accept</pre>	(reject)	•	0	Edit Delete
vpn: pptp: 🖉 🔿 ACCEPT	accept	¢) accept	¢) accept	•	0	Edit Delete
An and a second s						

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	eject 🗘 🔽 🖾 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:	Eaît MDelete
---------------	--------------

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.



lan: lan: 🛃 👷 👰	⇒ p	pp v	wan	reject	•)(accept \$	reject 🛟) 🛛	Edit Delete

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.

wan: wan: 🖉 wan2: 🖉 wext: 🖉 → REJECT	accept \$)(accept \$)(reject \$)	Edit Delete

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.

vpn: pptp: 🧾 → ACCEPT	accept 🛟	accept \$	accept \$		Edit 💌 Delete

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.

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
ppp: ppp:	(reject 🛟	accept \$	reject 🛟			Edit Delete
cap: cap: D → ACCEPT	(accept \$	(accept \$	accept 🛟			Edit Delete
lan: lan: 🛃 🙊 🙊 🔿 ppp 🛛 wan	(reject \$	(accept \$	(reject 🛟			ZEdit Delete
wan: wan: 🦉 wan2: 🛃 wext: 🛃 ⇒ REJECT	accept \$	(accept \$)	reject 🛟		0	ZEdit Delet
vpn: pptp: 🛃 → ACCEPT	accept \$	(accept \$	accept 🛟			ZEdit Delet
newzone: (empty) = REJECT	(reject \$	(accept \$)	reject 🛟			Edit Delet

Home Services Status System VPN Networ	k Users Statistics Logout
Diagnostics Interfaces Win VLAN Switch DHCP	and DNS Hostnames Static Routes Firewall Packet Capture PPP SQM Qos DSCP Qos Failover/Load Balancing
reneral settings Fort forwards Firewark Kules IP	SEL IP PLOXY
rewall - Zone Settings - Zone "newzone	3"
Zone "newzone"	
This section defines common properties of "newzone". The orwarded traffic between different networks within the zon	input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for i.e. Covered networks specifies which available networks are members of this zone.
General Settings Advanced Settings	
Name	newzone
Input	(reject 🛟
Output	accept \$
Forward	(reject 🗘
Masquerading	
MSS clamping	0
Covered networks	Cap: 🛃
	🗋 Ian: 🚂 🙊 🙊
	D ppp: 2
	pptp: e
	🗋 wan: 🚂
	🗋 wan2: 🗾
	🗋 wan6: 🖉
	🗆 wext: 📜
	create:
Inter-Zone Forwarding he options below control the forwarding policies between t orwarded traffic from other zones targeted at "newzone	this zone (newzone) and other zones. <i>Destination zones</i> cover forwarded traffic originating from "newzone" . <i>Source zones</i> match ". The forwarding rule is <i>unidirectional</i> , e.g. a forward from Ian to wan does <i>not</i> imply a permission to forward from wan to Ian as well.
Allow forward to destination zones:	Cap: 2ap: 2
	🗆 lan: 🗾 🧶 🙊
	D ppp: ppp: 2
	D vpn: pptp: 🖉
	wan: wan: wan2: www.t:
Allow forward from source zones:	Cap: Cap: J
	🗆 lan: 🚂 🙊 🙊
	ppp: ppp:
	🗆 vpn: pptp: 🖉
	wan: wan2: wext:
Back to Overview 🥹 Reset	Save 🛽 Save & Ap

DRAFT

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.

RedPort



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.

againmenter and the	es Witi VLAN Switch DHCP and DNS	Hostnames Static Routes Firew	rall Packet Capture PPP	SQM QoS DSCP Qo	S Failover/Load Balancing
neral Settings P	rt Forwards Firewall Rules IPset I	Proxy			
ewall - Port F	orwards				
t forwarding allows	remote computers on the Internet to con	nect to a specific computer or service v	vithin the private LAN.		
Port Forwards					
Name	Match			Forward to	Enable Sort
		This section contains no v	alues vet		
	New	v port forward:			
INDITIC			A meriar port	The sea	
New over Tenuerd		[cap ¥] [ACO	

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.

Aller and a second		viton DicPan	a DNS HO	istnames Stat	IC ROUTES	irewall	Packet Capture	PPP	SQM QOS	DSCP Q05	Fallover	r/Load Balancing
neral Settings Po	ort Forwards Firew	all Rules IPse	t IP Proxy	<u>(</u>								
ewall - Port F	orwards											
				_								
forwarding allows	remote computers of	n the Internet to	o connect to	a specific com	puter or servi	ice within	the private LAN.					
ort Forwards								0.000.000				
Name		Match					Forward to			Enable	Sort	
		TPV4-TCP UDP										
New-		From any host in cap					any host in cap				4 4	Edit Delet
of the tware		Via any router IP										
			New port	forward:								
Name	Protocol	External zone	External po	ort Internal zo	ne Internal II	Paddress	Internal port					
						•		1 (***).				
New port-torward				Cab	•	•)		P	400			

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.

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 General Settings Port Forwards Firewall Rules IPset IP Proxy Firewall - Traffic Rules Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router. Traffic Rules Action Enable Sort Name Match Any traffic BLOCK WAN 📄 🔮 🦉 Edit 🐮 Delete From any host in wan Discard input DO_NOT_MODIFY To any router IP on this device Any traffic ALL 🗧 🖣 🔣 Edit 💌 Delete From any host in any zone Accent forward DO_NOT_MODIFY To any host in any zone Any UDP PASS DNS 🔮 🤚 🌌 Edit 💌 Delete From any host in any zone Accept forward DO_NOT_MODIFY To any host, port 53 in any zone Any UDP DNS From any host in any zone Accept input 🖻 🤚 🔣 Edit 🐮 Delete DO_NOT_MODIFY To any router IP at port 53 on this device Any TCP HTTP From any host in any zone Accept forward 🔮 🤮 📶 Edit 🗶 Delete DO_NOT_MODIFY To any host, port 80 in any com Any TCP HTTPS 🕈 🤚 🖉 Edit 🗶 Delete From any host in any zone Accept forward DO NOT MODIFY To any host, port 443 in any zone Any TCP FTF 🔮 🔮 🔣 Edit 🗶 Delete Accept forward From any host in any zone DO_NOT_MODIFY To any host, ports 30-21 in any zor Open ports on router: Name Protocol External port New input rule TCP+UDP \$ Add New forward rule: Name Source zone Destination zone lan \$) (wan + Add and edit... New forward rule. Source NAT Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets. Name Match Action Enable Sort This section contains no values yet New source NAT: Name Source zone Destination zone To source IP To source port + -- Please choo: + Do not rewrite Add and edit... (wan) New SNAT rule lan Save Save & Apply Reset

DRAFT

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

New forward rule:			
Name	Source zone	Destination zone	
New forward rule] (lan 🛟	(wan 🛟	Add and edit

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

This is standard firewall convention. Once the rule is created, 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.

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

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.

eneral Settings	Port Forwards	VLAN Switch Firewall Rules	DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
Sets											
ck, Allow, or De h priority rules	fine groups of a apply before us	lomains to be u er defined firev	sed by the firewa	ll and/or the v priority rule	oad balancer. s apply after.						
IPset Name	Action	Priority					Domains				
	Filtering Action	Filter Priority				Don	ain(s) to Filter				
Unique Name											

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.

alivera suggests	ifi VLAN Switch	DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
eneral Settings Port Forwa	rds Firewall Rules	IPset IP P	oxy							
Proxy										
vide IP forwarding.										
Local Port Remote Host	Remote Port									
				This section cont	ains no value	es yet				
*										

9.9. Packet Capture

Requires "superadmin" login.

greates manages min rear	Switch DHCP and DNS Hostnames Static Routes Firew	vall Packet Capture PPP SQM QoS DSCP QoS	Failover/Load Balancing
art network capture			
Interface	seconds, packets	Filter	Actions
[lo 🛟	0 seconds \$	google pap-filter(7) manual for syntax or leave blank	Start capture
utput capture in progress			
Output o capture in progress Capture links			
Output o capture in progress Capture links Capture file	Modification date	Capture size	Actions

DRAFT

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.

nostics Interfaces Wifi	VLAN Switch	DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
tus Settings Log							_			
Status and Tools										
Connection Status			Co	nnected						
				Connect						
			(8)	Disconnect						

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.

RedPort

gnostics Interfaces Wifi	VLAN Switch DHCP ar	d DNS Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
tus Settings Log			_	_	_		_	_	
and Modem Settings									
ngs which control the dialup b	ehavior of USB connecte	ed satellite phones.							
letwork PPP GSM Sigr	nal Pionitor								
letwork			GSM satellite or	dialun netv	+)	Note th	at for CSM th	APN under P	PD parameters must be set
			Enable on rou	ter startup.	Implies demand o	ption.			
napie									

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

-	None Selected	
V	GSM	
	Iridium	
	Globalstar	
	Isatphone	
	Thuraya	

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:

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 Status Settings Log PPP and Modem Settings Settings which control the dialup behavior of USB connected satellite phones. Network PPP GSM Signal Monitor Modem Interface USB2 + Select COM port assigned to modem. Modem Speed 921600 4 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 Time in seconds between reconnection attempts. Maximum Fail 0 Maximum reconnection fail attemtps 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. Save Save & Apply Reset

DRAFT

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:

RedPort

Demand	Initiate the link only on demand, i.e. when data traffic is present. Implies Persist.
Hold Off Timeout	30 30 Ime in seconds between reconnection attempts.
Maximum Fail	0 Maximum reconnection fail attemtps 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.

tus Settings Log	Switch DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QOS	DSCP QoS	Failover/Load Balancing
and Modern Settings									
ings which control the dialup behavio	or of USB connected sate	lite phones.							
Network PPP GSM Signal Me	onitor								
Network		G	SM	r dialun nat	÷)	Note th	at for CCM th	A DNI under F	D as manatam must be set
		- <u> </u>	GSM, satelate, o	r dialup net	work to connect to	. Note th	at for GSM tr	ie APN under P	PP parameters must be set.
Foable			Enable on rou	dar ekselves	Implies demand a	milimin			

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

DRAFT

	None Selected
V	GSM
	Iridium
	Globalstar
	Isatphone
	Thuraya

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:

Diagnostics Interfaces Wifi VLAN Switch DHCP and D	IS Hostnames Static Routes Firewall Packet Capture PPP SQM QoS DSCP QoS Failover/Load Balancing
itatus Settings Log	
P and Modem Settings	
ttings which control the dialup behavior of USB connected s	atellite phones.
Network PPP GSM Signal Monitor	
	APN Wizard
APN	Broadband
Username	Blank Entry Ø Value set under PPP settings and displayed here for convenience.
Password	Blank Entry Ø Value set under PPP settings and displayed here for convenience.
Pincode	SIM card pin. Leave blank if none required.

Before you can configure the Optimizer for 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:

RedPort

Home Services Status System VPN Retwork	Users Statistics Logout		-	<u>.</u>		
iagnostics Interfaces Wifi VLAN Switch DHCP a	nd DNS Hostnames Static Routes	Firewall Packet Capt	re PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
Status Settings Log						
PN Wizard						
is assistant helps you easily set up a mobile broadband	connection to a cellular network. Se	lect your country or regio	n and hit N	ext.		
Country	✓ None Selected					
	Alganistan					
	Algeria					
	Andorra					
	Angola					
	Argentina					
	Armenia					
	Australia					
	Austria					
	Azerbaijan					

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

ies Wifi VLAN Switch Log u easily set up a mobile bri	DHCP and DNS Hostnames	Static Routes Firewall	Packet Capture PP	P SQM QoS	DSCP QoS	Failover/Load Balancing
Log u easily set up a mobile bri					-	
u easily set up a mobile br						
u easily set up a mobile bro						
u easily set up a mobile bro						
	padband connection to a cellula	r network. Select your pro	ovider and hit Next.			
	Vone 🗸 None	Selected	•)			
	Voda	rone				
		Voda Voda	V None Selected Vodafone	Vodafone	Vodafone	Vodafone

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

tus Sattings Log	ondrana Diva nosciantes Static Rouces	Pirewaii Packet Capture Pi	- SQITQUS DSCFQU	5 Pallove / Load Balancing
us Settings Log				
Wizard				
assistant helps you easily set up a mobile bro	adband connection to a cellular network. Select	t your plan and hit Next.		
ning: Selecting an incorrect plan may result in	n billing issues for your broadband account or r	may prevent connectivity. If yo	u are unsure of your plan (lease ask your provier for
plan's APN.				
an	✓ None Selected	÷)		
	TWA	F		
	Vodafone Web			

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

RedPort

tus Settings Log					
and Modem Settings					
ngs which control the dialup behavior of USB connect	ed satellite phones.				
SM Network PPP Signal Monitor You must hit Save & Apply to record new APN.					
	APN Wizard Select APN by Cou	untry, Provider, and Plan.			
PN	Twa	e.			
sername	Blank Entry Ø Value set under Pf	PP settings and displayed	here for conv	enience.	
assword	Blank Entry Image: State of the set of the se	PP settings and displayed	here for conv	enience.	
incode	I SIM card pin. Leav	ve blank if none required			

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

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.

gnosues interfaces will veally switch	DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
tus Settings Log									
Status and Tools									
		F - 1		4 m					
onnection Status		No	PPP network se	lected					
		10	Connect						
		1							
		C	Disconnect						

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

RedPort

me Services Status System VPN Network Use	rs Statistics Logout			
agnostics Interfaces Wifi VLAN Switch DHCP and DNS	Hostnames Static Routes Fire	vall Packet Capture PPP	SQM QoS DSCP QoS	Fallover/Load Balancing
itus Settings Log				
and Modem Settings				
ngs which control the dialup behavior of USB connected satelli	e phones.			
etwork PPP GSM Signal Monitor				
letwork	None Selected GSM, satellite, or dialup	network to connect to. Note that	for GSM the APN under PPP p	parameters must be set.
inable	📄 🥝 Enable on router sta	tup. Implies demand option.		
00000000000000000000000000000000000000				
				100 100

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

	None Selected	
V	GSM	
	Iridium	
	Globalstar	
	Isatphone	
	Thuraya	

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:
ngs which control the dialup behavior of USB conne	cted satellite phones.
etwork PPP GSM Signal Monitor	
leset LTE Modem	 Reset LTE Modem Reset modem to factory defaults. This takes 60 seconds to execute.
lodem Interface	System Default Select COM port assigned to modem.
todem Speed	System Default Baud rate for modem serial interface.
Isername	Leave blank if none required.
assword	Leave blank if none required.
hone Number	Phone number to dial. Leave blank for system default.
dle 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.
ersist	🗷 🞯 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.
lold Off Timeout	30 Ime in seconds between reconnection attempts.
laximum Fail	0 Maximum reconnection fail attemtps before giving up. set to 0 for infinite retries.
xtra Init	Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before dialing.
πυ	Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.
ebug	Write PPP connection debugging information to the system log.

- 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:

RedPort

Cattlenes	
settings Log	
nd Modem Settings	
s which control the dialup behavior of USB connected satellite pho	nes.
vork PPP GSM Signal Monitor	
	APN Wizard
	Broadband Coss Point Name.
Delay	2 2
	Some modems (such as the sierra wireless mc7455) require a delay (in seconds) between setting the APN and dialing.
mame	Blank Entry
	Value set under PPP settings and displayed here for convenience.
sword	Blank Entry Walue set under PPP settings and displayed here for convenience.
ode	
	SIM card pin. Leave blank if none required.

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

iagnostics Interfaces Wifi VLAN Switch	DHCP and DNS	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
tatus Settings Log									
N Winord									
N WIZARO									
s assistant helps you easily set up a mobile broa	adband connection	on to a cellula	ar network. Sele	ect your cou	untry or region a	nd hit N	ext.		
						•••••••			
Country		✓ Non	a Selected						
		Afgh	anistan						
		Alba	nia		-				
		Alge And	na						
		Ang	ola						
		Arge	ntina						
		Arm	enia						
		Aust	ralia						
		Aust	ria						

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

ome Services Status System VPN Network Users Stat	listics Logout	5				
iagnostics Interfaces Wifi VLAN Switch DHCP and DNS Hostn	ames Static Routes	Firewall Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
Status Settings Log				_	_	
PN Winned						
is assistant helps you easily set up a mobile broadband connection to a ce	llular network. Select y	your provider and hit Next.				
<u>балаат (27) (27) (27)</u>	(5			200000000000000000000000000000000000000	
Provider	V None Selected	Ð				
Provider	✓ None Selected AT&T BendBroadband	Ð				
Provider	✓ None Selected AT&T BendBroadband Cincinnati Bell Wirel Lycamobile	less				
Provider	✓ None Selected AT&T BendBroadband Cincinnati Bell Wirel Lycamobile MTPCS (Cellular On	less no)				
Provider	✓ None Selected AT&T BendBroadband Cincinnati Bell Wirel Lycamobile MTPCS (Cellular On Streight Talk T_Mobile	iess re)				

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

RedPort

agnostics Interfaces Wifi VLAN Switch	DHCP and DNS H	Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
Status Settings Log		_	_	_	_		_	_	
NI 118									
'N WIZARD									
PN WIZARD is assistant helps you easily set up a mobile bro arning: Selecting an incorrect plan may result	padband connection to in billing issues for you	a cellular ne ur broadband	twork. Select yo account or may	our plan and prevent co	l hit <i>Next.</i> nnectivity. If you	are uns	ure of your p	lan please ask	your provier for your plan's AP
Is assistant helps you easily set up a mobile bra arning: Selecting an incorrect plan may result	oadband connection to in billing issues for you	a cellular ne ur broadband	twork. Select yo account or may	our plan and v prevent co	hit Next. nnectivity. If you	are uns	ure of your p	lan please as	v your provier for your plan's AP

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

Home Services Status System VPN Network Users Statist Diagnostics Interfaces Wifi VLAN Switch DHCP and DNS Hostnarr	ics Logout mes Static Routes Firewall Packet Capture PPP SQM QoS DSCP QoS Fallover/Load Balancing
Status Settings Log	
PP and Modem Settings	
ettings which control the dialup behavior of USB connected satellite phones.	
Network PPP GSM Signal Monitor	
	APN Wizard Select APN by Country, Provider, and Plan.
APN	Broadband
APN Delay	Construction of the number Some moderns (such as the sierra wireless mc7455) require a delay (in seconds) between setting the APN and dialing.
Username	Blank Entry Value set under PPP settings and displayed here for convenience.
Password	Blank Entry Slank Entry Slank Entry Blank Entry Blank E
Pincode	SIM card pin. Leave blank if none required.
Reset	🥥 Save 🛄 Save & App

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:

RedPort

nostics Interfaces Wifi VLAN Sv	vitch DHCP and DN	S Hostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancing
Js Settings Log									
Status and Tools									
nnection Status		C	onnected						
			Connect						
			Disconnect						

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.

and the Interfere			DUICE and	DAID	Usabasanas	Charle Daubar	Circum II	Paulut Cashura		CON 0-C	0000 0-0	Falley and Balanaire
ignostics Interface	es with VL	AN SWITCH	UNCP and	DIVS	nostnames	Static Routes	Firewall	Packet Capture	PPP	SQM QOS	DSCP QOS	Fallover/Load Balancing
tus Settings	Log											
D and Modern (ottings											
r and modern s	berrings											
ings which control t	he dialup beha	vior of USI	3 connected	d satellit	e phones.							
									anna as an a			
intuinels DDD	Cianal	Monitor										
Network PPP 0	Signal	Monitor				-						
Network PPP (Signal	Monitor				Enable/Disal	ble signal mo	nitoring during co	nnections			
Network PPP (Enable Level	Signal	Monitor			2	Enable/Disal	ble signal mo	onitoring during co	nnections	.		กับและที่ พี่เหล่าก็เหลากับวิวณณติ ก็เหลากับวิจ
Network PPP (Enable Level	Signal	Monitor			ی ۱۵] ۱۵]	Enable/Disal Allow satellite c	ble signal mo	onitoring during co	nnections al streng	i. th is larger th	an this value.	วัดอาวี ตัวออร์ และที่เว็บอาติเว็บออร์ กังเร
Network PPP 1 Enable Level	35M Signal	Monitor			<mark>ک</mark> آور ا	Enable/Disal Allow satellite of	ble signal mo	onitoring during con ections only if signa	nnections al streng	i. th Is larger th	ian this value.	Transferier Transferier Transferier
Network PPP I Enable Level	Signal	Monitor			2 3 3 3 3	Enable/Disal Allow satellite c	ble signal mo	ections only if sign	nnections al streng	i. th Is larger th	an this value.	

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.

art Queue management							
SQM you can enable traffic shaping, better mixing (Fair Queueing), acti	ve queue length m	anagement	(AQM) and prio	ritisation	on one netv	ork interface	•
ueues							
Basic Settings Queue Discipline Link Layer Adaptation							× Dele
nable this SQM instance.	0						
nterface name	eth1		÷)				
Download speed (kbit/s) (ingress) set to 0 to selectively disable ingress	85000		1.				
haping:							
Ipload speed (kbit/s) (egress) set to 0 to selectively disable egress	10000						
haping:							
create log file for this SQM instance under							
var/run/sqm/\${Inerface_name}.debug.log. Make sure to delete log files							
renosity of SOM's output into the system log	(into (default)		•]				
erbosity of Sight's output into the system log.	(Into (default)		•)				

9.12. DSCP QoS

Requires "superadmin" login.

gnostics interraces	WIII VLAN SWITCH	Unce and Divs Ho	stratic Koules	FireWall	Packet Capture	PPP	SQM Q0S	DSCP QOS	Fallovery Load Baland
P Rules									
entiated services or Dil	fServ is a compute	er networking architectur	re that specifies a simple	and scalab	le mechanism for	classif	ying and ma	inaging netwo	ork traffic and providi
e best-effort service to	non-critical service	es such as web traffic or	file transfers.	iow-idtency	to chical netwo	K u anno	c such ds Vu	ice of screening	ing media wille prov
ss can be either a netw	vork name, a hostr	ame, a network IP addr	ress (with /mask), or a pi	lain IP addr	ess. Hostnames v	vill be r	esolved onc	e only, before	the rule is submitted
ernel. Please note that	specifying any nam	he to be resolved with a	remote query such as DI	NS is a real	ly bad idea. The I	mask ca	in he either	a network ma	sk or a plain number
fuine the number of 1's	at the left side of	the network mack. Thus	a mack of 24 is equival	lant to 255	255 255 0 A "I"	aroumo	int before th	a network ina	cification invorts the
fying the number of 1's address.	at the left side of	the network mask. Thus	s, a mask of 24 is equival	lent to 255.	255.255.0. A "!"	argume	nt before th	e address spe	ecification inverts the
fying the number of 1's e address. es can be either addres	at the left side of ses or ports separa	the network mask. Thus ated by '-' or ':'	, a mask of 24 is equival	lent to 255.	255.255.0. A "I"	argume	nt before th	e address spe	ecification inverts the
fying the number of 1's e address. es can be either addres DSCP Value	at the left side of ses or ports separa	sted by '-' or ':'	s, a mask of 24 is equival	lent to 255.	255.255.0. A "!" Dest IP	argume	Dest F	Port	Comment
fying the number of 1's e address. es can be either addres DSCP Value	Proto	sted by '-' or ':' Source IP IP/Net/Range	s, a mask of 24 is equival Source Port Port/Range	lent to 255.	255.255.0. A "!" Dest IP IP/Net/Range	argume	Dest F Port/Ra	e address spe	Comment
fying the number of 1's e address. es can be either addres DSCP Value	et the left side of sees or ports separa Proto	sted by '-' or ':' Source IP IP/Net/Range	s, a mask of 24 is equival Source Port Port/Range This section contains	no values ye	255.255.0. A "!" Dest IP IP/Net/Range	argume	Dest F	Port	Comment
fying the number of 1's e address. les can be either addres DSCP Value	at the left side of ses or ports separa Proto	sted by '-' or ':' Source IP IP/Net/Range	s, a mask of 24 is equival Source Port Port/Range This section contains	lent to 255. no values ye	255.255.0. A "!" Dest IP IP/Net/Range	argume	Dest F Port/Ra	Port	Comment
fying the number of 1's e address. es can be either addres DSCP Value	at the left side of ses or ports separa Proto	the network mask. Thus ated by '-' or ':' Source IP IP/Net/Range	s, a mask of 24 is equival Source Port Port/Range This section contains	lent to 255. no values ye	255.255.0. A "!" Dest IP IP/Net/Range et	argume	Dest F Port/Ra	Port	Comment

9.13. Failover/Load Balancing

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

RedPort



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

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

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

	Pland DNS Hostnames Stat	c Routes Firewall	Packet Capture P	PP SQM QoS	DSCP QoS	Failover/Load Balancin
erview Configuration Advanced				_	_	
erface Status Detailed Status						
MWAN Interface Live Status						
wan (eth0)	wan2 (eth1)		ppp (ppp0)			
Online (tracking active)	Offline		Offline			
wext (eth3) Offline						
MWAN Interface Systemion						
HWAN Intellace Systemog						
No MWAN systemlog history found						

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

RedPort

gnostics erview (Interfaces V Configuration	Vifi VLAN S	Switch	DHCP a	and DNS	Hostna	ames	Static Routes	Firewall	Packet Capture	PPP	SQM QoS	DSCP QoS	Failover/Load Balancin
rview	Configuration	Advanced												
face Stati		THE FOLLOW	_	_			_				_			
	us Detailed	Status												
	Detailed Cha													
MWANI	Detailed Stat	lus												
Inter	face status:													
inter	rface wan is	online (tr	acking	down)										
inter	rface ppp is	offline (t	racki	ng down)	,									
inter	rface wext is	s offline (track:	ing down	1)									
Folicy	y balanced:													
wan	(100%)													
Policy	y gsm sat sat	2:												
wan ((100%)													
Policy	y sat2 only:													
unrea	achable													
Folicy	y sat2 sat:													
wan	(100%)													
Policy	y sat only:													
wan	(100%)													
Policy	y sat_sat2:													
wan	(100%)													
Policy	y wi gsm:													
unrea	achable													
Folicy	y wi_gsm_sat_	sat2:												
wan ((100%)													
Known	networks:													
10.1.	.5.0/24													
192.1	0.0.0/8													
192.3	168.0.79													
192.1	168.90.0													
10.1.	.5.1													
10.1.	.5.0													
192.1	168.0.255													
192.3	168,10,255													
127.0	0.0.1 168.0.0													
192.1	168.0.0/24													
127.0	0.0.0													
192.1	168.0.254													
224.0	0.0.0/3													
192.1	255.255.255													
10.1	.5.255													
192.1	168.10.0/24													
Active	e rules:													
504	38880 - wi_q	[sm_sat_sat	2 all	L 1	• 3	*	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.

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

9.13.2.1. Interfaces

Requires "superadmin" login.

lover /1 -	ad Balanci	ine										
over/Loa	au baianci	ing	,									
rview	Configura	tion Advanced		_					_	_		
erfaces	Members	s Policies Ru	iles						_	_	_	
AN INCO	errace	onfiguratio	n									
are cu	rrently 3	of 250 support	ted interfaces config	gured								
NING: S	ome inte	rfaces have no	default route in the	e main routi	ng table!							
NING: 5	ome inte	rfaces have no	metric configured i	n /etc/conf	ig/network!							
terface	-											
AN suppo AN requir nes must	s rts up to 2 res that all match the	50 physical and/o interfaces have a interface name fo	r logical interfaces unique metric configure und in /etc/config/netw	d in /etc/confi ork (see advar	g/network nced tab)							
AN suppo AN requir nes must nes may o erfaces ma terface	s res that all match the contain cha ay not shar Enabled	50 physical and/o interfaces have a interface name fo racters A-Z, a-z, (re the same name Tracking IP	r logical interfaces unique metric configure und in /etc/config/netw 0-9, and no spaces as configured members Tracking reliability	d in /etc/config ork (see advar s, policies or ru Ping count	g/network nced tab) iles Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort	
AN suppo AN requir nes must nes may o rfaces ma iterface	es that all match the contain cha ay not shar Enabled Yes	50 physical and/o interfaces have a interface name fo racters A-Z, a-z, (re the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.222.220 8.8.4.4	rlogical interfaces unique metric configure und in /etc/config/netw 0-9,and no spaces as configured members Tracking reliability 1	d in /etc/config ork (see advar s, policies or ru Ping count 1	g/network inced tab) Ping timeout 2s	Ping interval	Interface down	Interface up	Metric 10	Errors	Sort	Edit 🛪 Delet
AN suppo AN require nes must nes may o rrfaces ma tterface wan wan	rts up to 2 es that all match the contain cha ay not shar Enabled Yes Yes	50 physical and/o interfaces have a interface name for iracters A-Z, a-z, (re the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4 8.8.8.8 8.8.4.4 208.67.220.220	r logical interfaces unique metric configure und in /etc/config/netw 0-9,and no spaces as configured members Tracking reliability 1	id in /etc/confii ork (see advar s, policies or ru Ping count 1	g/network inced tab) illes Ping timeout 2s 2s	Ping interval 5s 10s	Interface down	Interface up 3 3	Metric 10 20	Errors	Sort	ZEdit * Delet
AN suppo AN requir nes must nes may c erfaces ma iterface wan wan2	rts up to 2 es that all match the contain cha ay not shar Enabled Yes Yes Yes	50 physical and/o interfaces have a interface name fo interface name fo racters A-2, a-2, (re the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.222.222 208.67.222.220 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220	r logical interfaces unique metric configure und in /etc/config/netw 0-9 ₉ _ and no spaces as configured members Tracking reliability 1 1 1	d in /etc/confi ork (see advar s, policies or ru Ping count 1 1 1	g/network need tab) Ping timeout 2s 2s 2s	Ping interval 5s 10s 5s	Interface down 3 3 3 3	Interface up 3 3 3	Metric 10 20	Errors ©	Sort	Edit × Deleta
AN support AN requir nes must mes must erfaces must sterface wan wan2	rts up to 2 es that all match the contain cha ay not shar Enabled Yes Yes Yes	50 physical and/o interfaces have a interface name fo interface name fo racters A-2, a-2, (re the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.222.220 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220	r logical interfaces unique metric configure und in /etc/config/netw 0-9and no spaces as configured members Tracking reliability 1 1 1	nd in /etc/confii ork (see advar s, policies or ru Ping count 1 1 1	g/network need tab) Ping timeout 2s 2s 2s	Ping interval 5s 10s 5s	Interface down 3 3 3 3	Interface up 3 3 3	Metric 10 20	Errors ©	Sort	Edit Deleta

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>.

NewAD1	Add

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

RedPort

Configuration Advanced	and only inscribing state notes. Filewall Facker capture, Frr. SQM Qus, DSCF Qus, Pallover/Load Balancin
Verview Configuration Advanced	
iterraces members Policies Rules	
VAN Interface Configuration - NewAD1	
RNING: this interface has no default route in th	he main routing table!
RNING: this interface is configured incorrectly	or not at all in /etc/config/network!
RNING: this interface has no metric configured	l in /etc/config/network!
ina and a second se	
Enabled	(Yes 🗘
Tracking IP	
	This IP address will be pinged to dermine if the link is up or down. Leave blank to assume interface is always online
Tracking reliability	
	Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up
Ping count	(1 *)
Ping timeout	2 seconds
Ping interval	5 seconds +
Interface down	3
	Interface will be deemed down after this many failed ping tests
Interface up	(3 ÷)
Interface up	3 ↔ ② Downed interface will be deemed up after this many successful ping tests
Interface up Metric	Owned interface will be deemed up after this many successful ping tests
Interface up Metric	3 Obvious Downed interface will be deemed up after this many successful ping tests
Interface up Metric	3 € Owned interface will be deemed up after this many successful ping tests This displays the metric assigned to this interface in /etc/config/network

- 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 the 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:

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

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.

DRAFT

for a start of the	The second	14/101 1/1 0.01	C ALL DUCK - I D	ALC: DESCRIPTION	Photo Photo Photo	the second se	Burghan Burghan	DDD DOM O-	c	0.0.0			And the second second
agnostics	Interface	s With VLAN	Switch DHCP and D	NS Hostnan	nes Static Rou	ites Firewall	Packet Capture	PPP SQM Qo	s bsc	P QoS	Failov	er/Load Bal	lancin
verview	Configura	tion Advanced							_	_	_		
nterfaces	Members	Policies Ru	les										
VAN Int	erface (Configuration	n										
ere are cu	rrently 5	of 250 support	ed interfaces config	ured									
RNING: :	some inte	rfaces have no	default route in the	main routir	g table!								
	come inte	rfaces are conf	igured incorrectly o	r not at all i	n /etc/config/	networki							
DUTNC: S	some inte	faces have	mateix applications		a (notwork)	INCOVOTRS							
RHING: S	some inte	naces have no	metric configured i	n /etc/conn	g/ network!								
WAN SUDDO	erts up to 2	50 physical and/or	logical interfaces	_									
WAN requi	res that all	interfaces have a	unique metric configured	d in /etc/config	/network								
ames must	t match the	interface name for	und in /etc/config/netwo	ork (see advan	ced tab)								
ames may	contain cha	racters A-Z, a-z, C)-9. and no spaces										
lames may nterfaces m	contain cha ay not shar	racters A-Z, a-z, C re the same name)-9, and no spaces as configured members	, policies or ru	les								
lames may nterfaces m Interface	contain cha ay not shar Enabled	racters A-Z, a-z, C te the same name Tracking IP	0-9, _ and no spaces as configured members Tracking reliability	, policies or rul Pin <mark>g count</mark>	les Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort		
ames may nterfaces m Interface wan	contain cha nay not shar Enabled Yes	racters A-Z, a-z, C te the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4)-9, _ and no spaces as configured members Tracking reliability 1	, policies or rul Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric 10	Errors	Sort	ZEdit 🗙	Delete
ames may nterfaces m Interface wan wan2	contain cha hay not shar Enabled Yes Yes	racters A-Z, a-z, C e the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4 8.8.8.8 8.8.4.4 208.67.220.220	9-9,and no spaces as configured members Tracking reliability 1 1	i, policies or rul Ping count 1	Ping timeout 2s 2s	Ping interval 5s 10s	Interface down 3 3	Interface up 3 3	Metric 10 20	Errors	Sort	ZEdit 💌	Delete
lames may nterfaces m Interface wan wan2 ppp	contain cha nay not shar Enabled Yes Yes	racters A-Z, a-z, C re the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4 8.8.8.8 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220)-9,and no spaces as configured members Tracking reliability 1 1	, policies or rul Ping count 1 1	Ping timeout 2s 2s 2s	Ping interval 5s 10s 5s	Interface down	Interface up 3 3 3	Metric 10 20	Errors ©	Sort	Edit X	Delete Delete
lames may nterfaces m Interface wan wan2 ppp wext	contain cha hay not shar Enabled Yes Yes Yes	racters A-Z, a-z, C ee the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220)-9,and no spaces as configured members Tracking reliability 1 1 1 1	, policies or rul Ping count 1 1 1	Ping timeout 2s 2s 2s 2s	Ping interval 5s 10s 5s 5s	Interface down	Interface up 3 3 3 3	Metric 10 20 -	errors ©	Sort	Edit X	Delete Delete Delete
lames may nterfaces m Interface wan wan2 ppp wext NewAD1	contain cha hay not shar Enabled Yes Yes Yes Yes	racters A-Z, a-z, C e the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.220.220 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.222.222 208.67.220.220	9-9,and no spaces as configured members Tracking reliability	, policies or rul Ping count 1 1 1 1 1	Ping timeout 2s 2s 2s 2s 2s	Ping interval 5s 10s 5s 5s -	Interface down	Interface up 3 3 3 3 -	Metric 10 20 5	Errors ම ම	Sort 	Edin X	Delete Delete Delete
lames may interfaces m Interface wan wan2 ppp wext NewAD1	contain cha hay not shar Enabled Yes Yes Yes Yes	racters A-Z, a-z, C re the same name Tracking IP 8.8.8.8 208.67.222.222 208.67.220.222 08.67.220.220 8.8.8.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220 8.8.8.8 8.8.4.4 208.67.220.220	9-9,and no spaces as configured members Tracking reliability 1 1 1 1 1 1 1 2 3 4 1	, policies or rul Ping count 1 1 1 1 1 1	Ping timeout 2s 2s 2s 2s 2s	Ping interval 5s 10s 5s 5s -	Interface down	Interface up 3 3 3 3 3	Metric 10 20 - 5 -	Errors ©	Sort	<pre>ZEdit ★</pre>	Delete Delete Delete

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.

Status System VPN Network Users Statistics Logout Home Services Interfaces Wifi VLAN Switch DHCP and DNS Static Routes DSCP QoS Failover/Load Balancing Diagnostics Hostnames Firewall Packet Capture PPP SQM QoS Overview Configuration Advanced Interfaces Members Policies Rule MWAN Member Configuration Members Members are profiles attaching a metric and weight to an MWAN interface Names may contain characters A-Z, a-z, 0-9, _ and no spaces Members may not share the same name as configured interfaces, policies or rules Weight Member Interface Metric Sort 4 4 sat_m1_w1 Edit Delete war 1 1 + 5 sat_m1_w2 wan 1 2 Edit Delete 3 . 1 Edit Delete sat m1_w3 wan 2 4 4 sat_m2_w1 1 Edit Delete wan sat_m2_w2 2 2 4 4 Edit Delete wan 2 4 5 3 Edit MDelete sat m2 w3 wan * * 3 sat_m3_w1 1 Edit Delete wan sat_m3_w2 war 3 2 4 4 Edit Delete sat_m3_w3 wan 3 3 ZEdit Delete + 5 1 Edit Delete set2 m1 w1 1 wan2 * * sat2_m1_w2 wan2 1 2 Edit MDelete sat2_m1_w3 1 3 4 4 Edit Delete wan2 2 4 4 sat2_m2_w1 wan2 1 Edit Delete 4 5 2 2 Edit Delete sat2 m2 w2 wan2

DRAFT

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>.

NewMbrAD1_M1_W1	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).

Member used	✓ sat_m1_w1) <u>1</u>
Last resort	sat_m1_w2 sat_m1_w3 sat_m2_w1	ne use this behavior for matched traffic
Currently Configured Members	sat_m2_w2 sat_m2_w3 sat_m3_w1	
	sat_m3_w2 sat_m3_w3 sat2_m1_w1 sat2_m1_w2	

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

ember used	sat_m1_w1	•	
ast resort	✓ unraachable (reject) blackhole (drop) default (use main routing table)	ne use this behavior for matched traffic	

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:

rview Configuration Advanced					
rfaces Members Policies Rule	es				
AN Policy Configuration					
licies					
cies are profiles grouping one or more hber interfaces with lower metrics are i d-balanced member interfaces distribut nes may contain characters A-Z, a-Z, 0 cies may not share the same name as	members controlling how MWAN distributes used first. Interfaces with the same metric te more traffic out those with higher weight 9, _ and no spaces. Names must be 15 ch configured interfaces, members or rules	s traffic load-balance is aracters or less			
Policy	Members assigned	Last resort	Errors	Sort	
sat_only	sat_m1_w1	unreachable (reject)		• •	Edit Delete
sat2_only	sat2_m1_w1	unreachable (reject)		4 4	Edit Delete
sat_sat2	sat_m1_w1 sat2_m2_w1	unreachable (reject)			Edit Delete
sat2_sat	sat2_m1_w1 sat_m2_w1	unreachable (reject)			Edit Delete
balanced	sat_m1_w1 sat2_m1_w1	unreachable (reject)			Edit Delete
gsm_sat_sat2	ppp_m1_w1 sat_m2_w1 sat2_m3_w1	unreachable (reject)			Edit Delete
wi_gsm_sat_sat2	wext_m1_w1 ppp_m2_w1 sat_m3_w1 sat2_m4_w1	unreachable (reject)			ZEdit ZDelete
wi_gsm	wext_m1_w1 ppp_m2_w1	unreachable (reject)			Edit XDelete
NewMbrAD1_M1_W1	sat_m1_w1	unreachable (reject)		•	Edit Delete
	Add				

DRAFT

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)	•	Edit Delete

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)	9	Edit Delete
gsm_sat_sat2	ppp_m1_w1 sat_m2_w1 sat2_m3_w1	unreachable (reject)		Edit X Delete

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>.

wan_AD1	bbA

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>.

Home Services Status System VPN Network Use	rs Statistics Logout			
Diagnostics Interfaces Wifi VLAN Switch DHCP and DNS	Hostnames Static Routes Fire	wall Packet Capture PP	P SQM QoS DSCP QoS	Failover/Load Balancing
Overview Configuration Advanced				
Interfaces Members Policies Rules				
MWAN Policy Configuration - wan_AD1				
Member used	(sat_m1_w1	• <u>)</u> *1		
Last resort	unreachable (reject)	are offline use this behavior	for matched traffic	
Currently Configured Members				
	sat_m1_w1			
	sat_m1_w2			
	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.

wan_AD1 sat_m1_w1 unreachable (reject)	wan_AD1	sat_m1_w1	unreachable (reject)	•	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:

RedPort

and the second sec		2 0					- Contraction and Provide	a contrate o		17		
rview Co	onfiguration Ac	dvanced				_		_			_	
rfaces M	Members Policies	Rules										
	Configuratio	'n										
affic Rule	es											
affic Rule	es											
affic Rule as specify w	es which traffic will use	a particular M	WAN policy based on IP	address, port or prote	col							
affic Rule as specify w as are mate	es which traffic will use ched from top to bo	a particular M ttom. Rules bel	WAN policy based on IP of which was a matching rule are	address, port or proto ignored. Traffic not m	ocol atching any	rule is re	outed using the ma	ain routir	ng table		_	
affic Rule es specify w es are mato ffic destined	es which traffic will use ched from top to be d for known (other t	a particular M ttom. Rules bel than default) ne	WAN policy based on IP ow a matching rule are etworks is handled by th	address, port or proto ignored. Traffic not m e main routing table.	ocol atching any Traffic mate	rule is ro hing a ru	uted using the ma le, but all WAN int	ain routir terfaces	ng table for that policy a	re down will	be black	holed
affic Rule es specify w es are mato fic destined nes may co	es which traffic will use ched from top to bo d for known (other to ontain characters A-	a particular Mi ttom. Rules bel than default) ne Z, a-z, 0-9, _ a	WAN policy based on IP ow a matching rule are atworks is handled by th and no spaces	address, port or proto gnored. Traffic not m e main routing table.	ocol atching any Traffic mate	rule is ro ching a ru	uted using the ma le, but all WAN int	ain routir terfaces	ng table for that policy a	re down will	be black	holed
es specify w es are matc ffic destined mes may co es may not	es which traffic will use ched from top to bol d for known (other t ontain characters A- share the same nar	a particular Mi ttom. Rules bel than default) ne Z, a-z, 0-9, _ a me as configure	WAN policy based on IP ow a matching rule are i etworks is handled by th ind no spaces ed interfaces, members	address, port or proto ignored. Traffic not m e main routing table. or policies	ocol atching any Traffic mate	rule is re ching a ru	outed using the ma le, but all WAN int	ain routir terfaces	ng table for that policy a	re down will	be black	holed
es specify w es are mato ffic destined nes may co es may not Rule	es which traffic will use ched from top to bold d for known (other to ontain characters A- share the same nar Source address	a particular Mi ttom. Rules bel than default) ne Z, a-z, 0-9, _ a me as configure Source port	WAN policy based on IP ow a matching rule are etworks is handled by th and no spaces ed interfaces, members Destination address	address, port or proto gnored. Traffic not m e main routing table. or policies Destination port	ocol atching any Traffic mato Protocol	rule is ro ching a ru Sticky	uted using the ma ile, but all WAN int Sticky timeout	ain routin terfaces IPset	ng table for that policy a Policy assig r	re down will e d Errors	be black Sort	holed
affic Ruli es specify w es are matc ffic destinec mes may co es may not Rule	es which traffic will use ched from top to bol d for known (other t ontain characters A-, share the same nar Source address	a particular M ttom. Rules bel than default) ne Z, a-z, 0-9, _ a me as configure Source port	WAN policy based on IP ow a matching rule are etworks is handled by th nd no spaces ed interfaces, members Destination address 0.0.0.0/0	address, port or proto ignored. Traffic not m e main routing table. or policies Destination port	ocol atching any Traffic mato Protocol all	rule is ro ching a ru Sticky No	uted using the ma le, but all WAN int Sticky timeout	ain routin terfaces IPset —	ng table for that policy a Policy assig r wi_gsm_sat_s	re down will ed Errors	be black Sort	holed
affic Rule es specify w es are matc ffic destinec mes may co es may not Rule	es which traffic will use ched from top to be d for known (other t nitain characters A- share the same nai Source address	a particular Mi ttom. Rules bel than default) no Z, a-z, 0-9, _ a me as configure Source port 	WAN policy based on IP ow a matching rule are etworks is handled by th nd no spaces ad interfaces, members Destination address 0.0.0.0/0	address, port or proto ignored. Traffic not m e main routing table. or policies Destination port	ratching any Traffic mato Protocol all	rule is ro ching a ru Sticky No	uted using the ma le, but all WAN int Sticky timeout	ain routin terfaces IPset —	ng table for that policy a Policy assig r wi_gsm_sat_s	re down will ed Errors	be black	holed
affic Rule es specify v es are matc fic destinec nes may co es may not Rule fault_rule	es which traffic will use ched from top to beid d for known (other t ontain characters A- share the same nai Source address	a particular MI ttom. Rules bel than default) ne Z, a-z, 0-9, _ a me as configure Source port	WAN policy based on IP ow a matching rule are etworks is handled by th nd no spaces ed interfaces, members Destination address 0.0.0.0/0	address, port or proto ignored. Traffic not m e main routing table. or policies Destination port	ocol atching any Traffic mato Protocol all	rule is ro ching a ru Sticky No	uted using the ma le, but all WAN int Sticky timeout	in routin terfaces IPset	ng table for that policy a Policy assig r wi_gsm_sat_s	re down will ed Errors	be black Sort	holed

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 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 "wan" interface, if it is up. If the "wan" 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 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.

Member used	(wext_m1_w1 \$)x
	(ppp_m2_w1 +
	(sat_m3_w1 ♥) 💌
	(sat2_m4_w1 ♥)
ast resort	unreachable (reject)
	When all policy members are offline use this behavior for matched traffic

AD_rule	Add

System VPN Network Users Statistics Logout Status Services Diagnostics Interfaces Wifi VLAN Switch DHCP and DNS Hostnames Static Routes Firewall Packet Capture PPP SQM QoS DSCP QoS Failover/Load Balancing Overview Configuration Advanced Interfaces Members Policies Rules 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 \$ al View the contents of /etc/protocols for protocol descriptions Sticky (No \$ Iraffic 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**

DRAFT

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	-	all	No	-	-	wi_gsm_sat_sat2		•	Edit Delete
AD_rule	-	-	-		all	No	-	8 — 3	-		•	Edit Delete
		Add										

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.

OE Advanced, v1.0

© 2018 RedPort Global Powered by Global Marine Networks, LLC.



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.

California and Companya and California	*Dert	Switch Drive and I	JNS I	tostnames	Static Routes	rirewan	Facket Capture	PPP	50M 005	Dacr Qua	Fallover/ Load Balanci
verview Configuration Adv	anced		_					_			
agnostics											
MWAN Interface Diag	nostic	S									
wan		<u>•</u>)									
Ping default gateway		Ping tracking IP		Check IP	ules 🛄	Check ro	uting table		Hotplug ifup		
Hotplug ifdown											
MWAN Service Contro	[
	-		diam'								
Restart MWAN		Stop MWAN		Start MW	/AN						

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:

affic Routing	
Routing Mode	
Routing Mode	Automatic Manual
Real time WAN usage	
	(wan/eth0): RX bytes:14235226 (13.5 MiB) TX bytes:3510323 (3.3 MiB)
	(wan2/eth1): RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
	DISB Cell of Diago (ppp/ppp0): Off-line

Automatic Failover (default setting) requires no intervention; if a MWAN interface is unavailable, traffic will automatically by 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

© 2018 RedPort Global Powered by Global Marine Networks, LLC.

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.



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: <u>http://10.1.5.1:4990/www/login.chi</u>.

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.

Users		
s		
erface Overvie	W	
Users	Status	Actions
ADMIN	Group: users	
2	Date Added: Wed Jan 17 16:37:15 2018 Last Entry: Wed Jan 17 16:37:15 2018	Edit Delete

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

MIN			
er Configuration Options			
Enable Vpn Menus	6		
Enable Network Menus	0		
Enable Services Menus	٥		
Enable Status Menus			
 ✓ Firewall ✓ Routes ✓ System_Log ✓ Kernel_Log ✓ Realtime_Graphs ✓ Load ✓ Traffic ✓ Wireless ✓ Connections 			
Enable Statistics Menus			
Enable Home Menus	0		

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

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

dit Users	Sus Statem I'll Interior Carls Statistics Eugent	
sers		
Interface Overvie	w	
Users	Status	Actions
ADHIN	Group: users	
2	Date Added: Wed Jan 17 16:37:15 2018 Last Entry: Wed Jan 17 16:37:15 2018	Edit 🕷 Delete

Click <Add New User...>

in a	Network Users Statistics Logout	
it Users		
d New User		
r Configuration		
ana ana amin'ny tanàna mandritra dia kaominina dia kaominina dia kaominina dia kaominina dia kaominina dia kaomi Ny faritr'ora dia kaominina d		unur
Jser Name		
Enable Vpn Menus		
Inable Network Menus	<u>S</u>	
IP_Proxy Wifi Interfaces Firewall General_Settings Port_Forwards Failover/Load_Balancing Configuration Members Policies Rules Advanced SQM_QoS PPP Settings Log DSCP_QoS Packet_Capture		
Enable Services Menus		
Enable Status Menus	0	
Enable Statistics Menus		
Enable Home Menus	0	

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

RedPort

me	Services	Status	System	VPN	Network	Users	Statistics	Logout				
lit Use	ers								_	_		
MIN												
S												
terf	face Over	view										
			U	sers			St	atus		Act	tions	
NETWORK ASSISTANT												
		Co	Collecting data	🔣 Edit 💌 Delete								
				7								
			AD	MIN								
			1	2			Co	llecting data	Edit Delete			
				?								
Add I	New User											

11. Statistics

Requires "superadmin" login.

Home	Services	Status	System	VPN	Network	Users	Statistics		Logout	ut											
Graphs	Setup	Bandwid	thd						2		_	_	_	_	_	_	_	_	_	_	
Statisti	ics																				
The statis	stics packa	ge uses	Collectd to	gather d	ata and F	RDtool to	render diag	jram ir	nages.												
You can ir	nstall addit	ional col	ectd-mod	-* plugins	s to enab	le more s	tatistics.														

11.1. Graphs

Requires "superadmin" login.

Home Services	Status System VPN Network Users Statistics Logout						
Graphs Setup	Bandwidthd						
Interfaces Wirele	less System Load Memory Processes Uptime						
Statistics							
The statistics package uses <u>Collectd</u> to gather data and <u>RRDtool</u> to render diagram images.							
You can install additional collectd-mod-* plugins to enable more statistics.							

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

OE Advanced, v1.0

DRAFT

Requires "superadmin" login.

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

General plugins Network plugins Output plugins		
allectd Settings		
llectd is a small daemon for collecting data from various source	s through different plugins. On this page you can change general settings for the collectd daemon	÷.
Base Directory	/ver/run/soliectd	
Directory for sub-configurations	/etc/collectd/conf.d	
Directory for collectd plugins	/usr/lib/collectd	
Used PID file	/var/run/collectd.pid	
Datasets definition file	/usr/share/collectd/types.db	
Data collection interval	30 a Seconds	
Number of threads for data collection	2	
Try to lookup fully qualified hostname	D	
Additional Field 🛟 🎦 Add		

11.3. Bandwidth

Requires "superadmin" login.

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

Home Services Status System VPN Network	rs Statistics Logout	
Graphs Setup Bandwidthd		
Bandwidthd		
Bandwidthd		
C		
2	View Stats]
Settings		
Listen interface	(any +)	
Subnets	0.0.0.0/0	
Reset	() Sa	ve 🔲 Save & App

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

RedPort Tue Sep 11 19:55:06 2018

DRAFT



Programmed by David Hinkle, Commissioned by DerbyTech wireless networking.

- Daily -- Weekly -- Monthly -- Yearly -

Pick a Subnet: - <u>Top20</u> -- <u>0.0.0.0</u> -

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	32.9М	3.7M
199.48.130.178	2.6G	28.0M	2.6G	0	2.6G	0	2.6G	0	0
<u>10.1.5.4</u>	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.OM	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.OM	0	54.9M	0	55.3M	4.9M	1.0M
10.1.5.15	32.1M	29.4M	2.7M	0	30.5M	0	31.7м	342.6K	2.4K

RedPort

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

Home Services Status System	VPN Network Users Statistics Logout
Tasks Traffic Routing MWAN Overv	iew
Welcome	
Crew Internet Services	
Captive Portal URLs: Login - http://10.1.5.1:4990/www/lo Status - http://10.1.5.1:4990/www/! Logout - http://logout	gin.chi tatus.chi
	Generate pincodes
	Create users
	E Generate pincode usage reports (CDRs)
	(View/Manage pincodes
Email Accore	
WEB - <u>http://10.1.5.1/webmail</u> POP - 10.1.5.1:10 SMTP - 10.1.5.1:25 with no connect	on or authentication security
	Co to webmail
l	
Email Management	
	Create and manage crew email accounts
	Retrieve, delete, or drop large emails (BigMail) quarantined on the server
	Perform common email tasks
	View email logs
System Status	
	USystem status overview
	Realtime bandwidth usage over satellite link
	Historic bandwidth usage over satellite link
	C System message log
Local WiFi setup	
CETD and Security	
	© Change hotspot name and/or add security and set password
Remote Support	
	Inside remote support Inside 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.

Remote Support	
Remote access urls: http://remote.redportglobal.com:56503 ssh://remote.redportglobal.com:56502	
	e Remote Support nate remote support

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

Remote Access	and Filtering RedPort Email	GPS tracking	Remote Access	5M5	GPS/INMEA Repeater	VOICE PBX	Network Share
ptions							
mote access urls:							
Enable Remote Access	rur	Open up a tunne ming.	l to remote.redportglo	bal.com a	llowing remote access to	the router and	keep it
	rur	ining.					

Click "Enable Remote Support"

When remote support is enabled Remote Access URLs are displayed.

Options					
emote access urls: http://remote.redportglobal.com:57443 ssh://remote.redportglobal.com:57442					
Enable Remote Access	🗹 😨 Open up a tunn running.	el to remote.redportglobal.com	allowing remote access to	the router and keep it	
Access Port	7442				

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



		Optimizer Er	nterprise Guidelines
The router is shipped	d ir	n the following Default State: (Legend: E=Er	nabled, D=Disabled, O=Open)
Captive Portal		E	
Transparent Proxy	8	E	
Firewall	- 1	0	
DNS		0	
Web Compression		D	
RedPort Email	-8	D	
SMS	1	E	
GPS Tracking	-	D	
Voice		D	
RedPort VolP	8	D	
Automatic Failover			
The list below is desi Secure Your Router	ign b	ed as a general guideline for customizing th efore you begin.	e router to meet your needs. Be sure to read Chapter ??? "How to
Contrue Restal Lise	-	Actions	Location in the Of
Captive Portal Use	4	Change Copting Postal Admin Personand	Sanulana - Crow Internet Assess - Tools
	0	Add upper approvat	Services > Grew Internet Access > Tools
6 20	4	Add to Allowed Heats table	Services > Crew Internet Access > Osers
2	3	Add to Allowed Hosts table	Services > Grew Internet Access > Settings > Allowed Hosts
	4	Set Content Filtering Sceme	Services > web Compression and Filtering > Content Filtering
	0	Add and uner appoints	Network > Firewail > Firewail Roles
0	0	Add end user accounts	Services > Crew Internet Access > Osers
Web Commencies (/	Create Pincodes for Users	Services > Grew Internet Access > Pincodes
web Compression (Pre	emium Service - tees may apply)	
	-	Fates Lines ID and Decouverd	Services > Web Compression and Filtering > Settings > Compression
6 2	2	Enter User ID and Password	Services > Web Compression and Filtering > Settings > Compression
2	3	Set Compression Level	Services > Web Compression and Filtering > Settings > Compression
	4	Set Content Pittering Scheme	Services > Web Compression and Filtering > Content Filtering
	0	Establish Domain and Path Filters	Network > Firewall > Firewall > Litewall > L
Red Port Empil (Prom	O .	r Ponuice foco may apphi)	Network > Firewaii > Firewaii Rules
Neuron Email (rien	1	Must be enabled	Services > BadPort Email > Ceneral > Ceneral Settings
	2	Enter Main Identify Login Info	Services > RedPort Email > General > General > Settings
	2	Select Satellite connection method	Services > RedPort Email > Connection
9	4	Set Inhound Email Filter Size	Services > RedPort Email > Connection
2 6	5	Set Outbound Email Eiter Size	Services > RedPort Email > Filtere
	6	Enter Primany Accounts Purchased	Services > RedPort Email > Primary Accounts
	7	Add Crew/Sub Accounts	Services > RedPort Email > Crew Accounts
SMS	1.	Add Orew Sub Accounts	Services > Hear of Centair > Orew Accounts
onto	1	Set Satellite Device	Services > SMS > Settings
	2	Configure Extensions	Services > Voice PRX > Extensions
GPS Tracking via SM	19		
OF O TRUCKING VIE OV	1	Configure Tracking Parameters	Services > GPS Tracking > Tracking Via SMS
	1	comigure macking ratameters	our need a contracting a macking via owne

GPS Tracking via	Red	Port (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 VolP (Pr	emiu	n Service - fees may apply)	
0	1	Must be activated	Services > Voice PBX > RedPort VoIP
	2	Configure Extensions	Services > Voice PBX > Extensions
Failover / Load B	alanc	ing	
х	1	Configure PPP/GSM, if needed	Network > PPP > Settings
0	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
2 2	5	Create MWAN Traffic Rule(s), if needed	Network > Failover/Load Balancing > Configuration > Rules
Firewall (See Adv	ance	d User Guide before attempting modifcations	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

RedPort

14. Appendix B

		Access to Op	timizer Enterprise Us	er Interface (UI) Based or	Login Credentia	ls			10
SUPERADMIN ACCESS		Services Tab continued		Network Tab continued			Users Tab Continued		
Home Tab		SNMP)	Interfaces continued			_		Interfaces
Tasks			General		WEXT				Wireless
Traffic Routing		5	Community		WAN6			Output plugins	
MWAN Overview			Com2Sec	Wife		(Network
Services	Tab		Group	VLAN Switch					RRDTool
Crew Internet Access			View	DHCP and DNS			Bandwidthd		
	Settings		Access	Hostnames		:		Bandwidthd	6
	Users		Log	Static Routes				Lopout Tab	
	Pass-through MAC	Network Shares		Firewall	j.	j j	4	DMIN ACCES	s
Pincodes		Status Tab			General Settings		Statu	s Tah	
	CDRs	Overview			Port Forwards	÷3	Overview		
-	Toois	Frewall	č –	1997 - 19	Fireal Rules		Firewall		-
Web Compression and Filteri	ng	Routes			IPset		Routes		
	Settings	System Loo			IP Proxy		System Log		c
	Content Filtering	Kernel Log		Packet Capture		e – 2	Kernel I on	8	15
-	Cache Management	Realtime Graphs	()	PPP	2		Realtime Graphs		-
	Traffic Management	Contant	Tab	-	Status			Load	
	Access Control	System	140		Settings	-	-	Traffic	
-	Loss	Administration		0	Lon	s		Wireless	
	Logs	Profiles	· · · · ·	0010-0	LOG		-	Connections	17 · · · ·
DadDart Email	nep	Proties	Dusting	Dech Ove			-	CONNECTIONS	
negrori cinali	(Conserved)	-	Track	Colored and Onlanding		2	Descured	Admin Options Ta	lb
	General	0.1.15.15	10015	Fallover/Load Balancing	0	s	Massword		
-	Connection	Backup / Hash Hirmware			Overview	-	-	Logout Tab	r
	Filters	Heboot			Configuration		-		-
	Primary Accounts	VPN T	ab	(<u> </u>		Interfaces	-		i
	Crew Accounts	PPTP				Members	-		
	File Transfer		Settings			Policies		1	
	Spool	-	Users		n Managana	Rules	-		
	Tools	IPSec		L	Isers Tab		-		
	BigMail		IPSec Configuration	Edit Users					
	Logs		Connections	Graphs					
Remote Access		_	Phase 1 proposais		Interfaces		_		
r	Remote Access		Phase 2 proposals		Wreless		-		
SMS			Tunnels		System Load		_		
	Settings		IPSec Logs		Memory				
	Management	OpenConnect VPN			Processes		_		
GPS Tracking	2	_	Server Settings			asterisk			
	Tracking		User Settings			chilli			
Dynamic DNS	0	OpenVPN				radiusd			
GPS/NMEA Repeater		Network	Tab		_	xgate			
	GPS/NMEA Repeater	Diagnostics			Uptime		_		
Voice PBX		Interfaces		Setup					
	Settings		PPTP		General plugins	i i			
	Extensions		WAN			System Load			
	Voicemail		WAN2			Memory	_		
	Logs		PPP			Processes			
·	Sat SIP Trunk		LAN	÷		Uptime		5	
	RedPort VolP		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