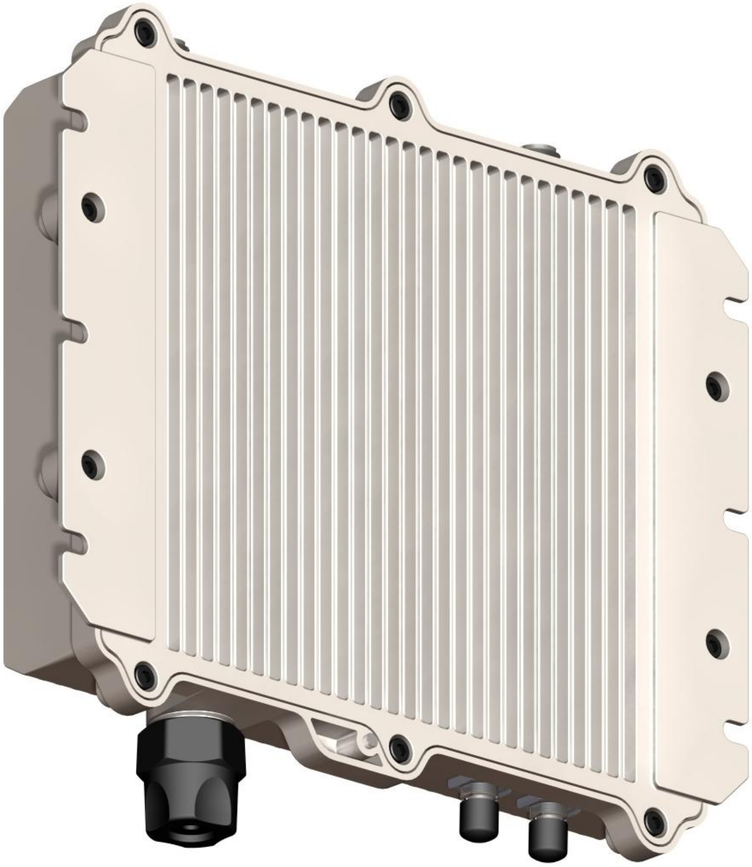
RDL-3000

Broadband Wireless Radio Platform



User Manual

Copyright Information

Disclaimer

The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Additionally, Redline makes no representations or warranties, either expressed or implied, regarding the contents of this product. Redline Communications shall not be liable for any misuse regarding this product. The information in this document is subject to change without notice. No part of this document shall be deemed to be part of any warranty or contract unless specifically referenced to be part of such warranty or contract within this document.

Software Versions

This manual describes operation using software release v1.xx. This document may include references to features that are different or unavailable in previous software releases. Refer to the product Release Notes for information about specific software releases.

CONTENTS SUMMARY

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

1 Important Notices

1.1 Service & Safety

1.1.1 Safety Warnings

1. ⚠ PoE power adapter caution:

> ***Warning to Service Personnel**: 48 VDC*
>
> Customer equipment including personal computers, routers, etc., must be connected only to the INPUT (DATA) port on the PoE unit.
>
> Only the outdoors Ethernet interface cable connecting to the unit can be safely connected to the OUTPUT (DATA & POWER) connector. Connecting customer premises Ethernet equipment directly to the OUTPUT (DATA & POWER) connector on the Power-over-Ethernet power adapter may damage customer equipment.

2. Installation of the system must be contracted to a professional installer.
3. Read this manual and follow all operating and safety instructions.
4. Keep all product information for future reference.
5. The power requirements are indicated on the product-marking label. Do not exceed the described limits.
6. Disconnect the power before cleaning, or when the unit is not be in-use for an extended period.
7. The unit must not be located near power lines or other electrical power circuits.
8. The system must be properly grounded to protect against power surges and accumulated static electricity. It is the user's responsibility to install this device in accordance with the local electrical codes: correct installation procedures for grounding the unit, mast, lead-in wire and discharge unit, location of discharge unit, size of grounding conductors and connection requirements for grounding electrodes.

1.1.2 Warning Symbols

These symbols may be encountered during installation or troubleshooting. These warning symbols mean danger. Bodily injury may result if you are not aware of the safety hazards involved in working with electrical equipment and radio transmitters. Familiarize yourself with standard safety practices before continuing.

Electro-Magnetic Radiation

High Voltage

1.1.3 Lightning/Surge Protection

WARNING: The information provide in this user manual consists of general recommendations for installation the system equipment. The wireless equipment must be installed by a qualified professional installer who is knowledgeable of the requirements of installing outdoor radio equipment and follows local and national codes for electrical grounding and safety. Failure to meet safety requirements and/or use of non-standard practices and procedures may result in personal injury and/or damage to equipment.

The system must be properly grounded to protect against power surges and accumulated static electricity. It is the user's responsibility to install this device in accordance with the local electrical codes: correct installation procedures for grounding the unit, mast, lead-in wire and discharge unit, location of discharge unit, size of grounding conductors and connection requirements for grounding electrodes.

All outdoor wireless equipment is susceptible to surge damage from a direct hit or current induced from a near strike. A direct lightning strike may cause serious damage even if recommended guidelines are followed. Installing surge protection and following grounding practices detailed in local and national electrical codes can minimize equipment damage, service outages, and chance of serious injury.

The major reasons for surge damage can be summarized as:

- Poorly grounded antenna sites
- Improperly installed surge protection equipment

A lighting protection system provides a means by which the energy may enter earth without passing through and causing damage to parts of a structure. A good grounding system disperses most of the surge energy from a lightning strike away from the building and equipment. Improperly grounded connections are a source of noise that can cause malfunctions in sensitive equipment. The remaining energy on the Ethernet cable shield and conductors can be directed safely to ground by installing a surge arrestor in series with the cable. A surge protection system does not prevent lightning strikes, but protects equipment by providing a low resistance path for the discharge of energy safely to ground. If you have determined that surge protection is required for your system, the following general industry practices are provided as a guideline only:

1. The AC wall outlet ground for the indoor POE adapter should be connected to the building grounding system.
2. Install a surge arrestor in series with the Ethernet cable at the point of entry to the building. The grounding wire should be connected to the same termination point used for the tower or mast.
3. Provide direct grounding connections from the RDL-3000, the mounting bracket, and the antenna to the common building ground bus. Use the grounding screws provided for terminating the ground wires.

1.2 Regulatory Notices

1.2.1 FCC & IC Notices: Deployment in USA and Canada

Read the following notices about deployment in the USA and Canada:

1. The Model RDL-3000 and its antenna must be professionally installed.
2. ⚠WARNING -- FCC & IC RF Exposure Warnings

   To satisfy FCC and IC RF exposure requirements for RF transmitting devices, the following distances should be maintained between the antenna of this device and persons during device operation:

Table 1: **Notices - FCC & IC RF Recommended Safe Separation Distances**

Frequency (GHz)	Deployment	Separation Distance
4.9 - 5.3	PTP or PMP	270 cm (107 in) or more
5.8	PMP	20 cm (8 in) or more
	PTP	270 cm (107 in) or more

   To ensure compliance, operation at closer than these distances is not recommended. The antenna used for this transmitter must not be collocated in conjunction with any other antenna or transmitter.

3. FCC Information to Users @ FCC 15.105:

   NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

   This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

   - Reorient or relocate the receiving antenna.
   - Increase the separation between the equipment and receiver.
   - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
   - Consult the dealer or an experienced radio/TV technician for help.

   Where DFS is required by regional regulations, this function is permanently enabled at the factory and can not be disabled by the installer or end-user.

4. FCC Information to Users @ FCC 15.21:

   Warning: Changes or modifications not expressly approved by Redline Communications could void the user’s authority to operate the equipment.

1.2.2 Avis de la FCC et IC: Déploiement aux Etats-Unis et le Canada

Lisez les mentions suivantes sur le déploiement aux Etats-Unis et le Canada:

1. Le modèle RDL-3000 et son antenne doivent être installés par un professionnel.
2. ⚠ AVERTISSEMENT - FCC et IC avertissements d'exposition RF

   Pour satisfaire les exigences d'IC et du FCC en ce qui a trait aux expositions aux RF pour RF dispositifs de transmission, les distances suivantes doit être maintenue entre l'antenne de ce dispositif et des personnes pendant le fonctionnement du dispositif:

Table 2: **Notices - FCC & IC RF Distances de séparation sécuritaire recommandées**

Fréquence (GHz)	Déploiement	Distance de Séparation
4.9 - 5.3	PTP ou PMP	270 cm (107 in) ou plus
5.8	PMP	20 cm (8 in) ou plus
	PTP	270 cm (107 in) ou plus

   Pour assurer la conformité , l'operation à une distance moindre que celles-ci n'est pas recommandé. L'antenne utilisée pour ce transmetteur ne doit pas être co-localisé avec une autre antenne ou transmetteur.

3. Informations de la FCC aux utilisateurs @ FCC 15.105:

   NOTE: Cet équipement a été testé et démontré conforme aux exigences pour un dispositif numérique de classe B, conformément à la partie 15 des règles FCC. Ces exigences sont conçues pour fournir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle.

   Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément aux instructions, peut causer des interférences nuisibles aux communications radio. Toutefois, il n'existe aucune garantie que des interférences ne se produiront pas dans une installation particulière. Si cet équipement provoque des interférences nuisibles à la réception radio ou télévision, ce qui peut être déterminé en mettant l'équipement hors tension, l'utilisateur est encouragé à essayer de corriger l'interférence par un ou plusieurs des mesures suivantes:

   - Réorienter ou déplacer l'antenne de réception.
   - Augmenter la distance entre l'équipement et le récepteur.
   - Alimenter l'équipement par un circuit différent de celui du récepteur.
   - Consulter le revendeur ou un technicien radio / TV pour assistance.
   -

   Lorsque DFS est requis par les règlements régionaux, cette fonction est activée en permanence à l'usine et ne peut pas être désactivé par l'installateur ou l'utilisateur final.

4. Informations de la FCC aux utilisateurs @ FCC 15.21:

   Avertissement: Les changements ou modifications non expressément approuvées par Redline Communications peut annuler l'autorisation de l'utilisateur à utiliser cet équipement.

1.2.3 UL Information

1. The suitability of the supplied Ethernet cable is subject to the approval of Authority Having Jurisdiction and must comply with the local electrical code.
2. The equipment must be properly grounded according with NEC and other local safety code and building code requirements
3. To meet the over-voltage safety requirements on the telecommunications cables, a minimum 26 AWG telecommunication line cord must be used.

   Pour être en conformance avec les exigences finies de sûreté de sur-tension sur les câbles de télécommunications un fil de télécommunication ayant un calibre minimum de 26 AWG doit être utilisé.
4. Reminder to all the BWA system installers: Attention to Section 820-40 of the NEC which provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as is practical.
5. RDL-3000 must be installed in compliance with relevant articles in National Electrical Code-NEC (and equivalent Canadian Code-CEC) including referenced articles 725, 800 and 810 in NEC.
6. RF coaxial cable connecting an antenna to the RDL-3000 must comply with the local electrical code.

1.2.4 WEEE Product Return Process

In accordance with the WEEE (Waste from Electrical and Electronic Equipment) directive, 2002/96/EC, Redline Communications equipment is marked with the logo shown above. The WEEE directive seeks to increase recycling and re-use of electrical and electronic equipment. This symbol indicates that this product should not be disposed of as part of the local municipal waste program. Contact your local sales representative for additional information.

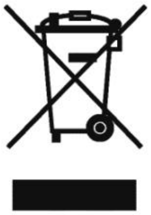


Fig. 1: Notices - WEEE Logo

1.2.5 Service & Warranty Information

1. Refer all repairs to qualified Service personnel. Do not remove the cover panel or modify any part of this device, as this action will void the warranty.
2. Locate the serial numbers and record these for future reference. Use the space below to affix serial number stickers. Also, record the MAC address identified on the unit product label.
3. Redline does not endorse or support the use of outdoor cable assemblies: i) not supplied by Redline, ii) third-party products that do not meet Redline's cable and connector assembly specifications, or iii) cables not installed and weatherproofed as specified in the RDL-3000 Installation Guidelines manual. Refer to the Redline Limited Standard Warranty and RedCare Service agreements.

Chapter 2

2 System Features

2.1 RDL-3000 Overview

The RDL-3000 system is designed and manufactured by Redline Communications -- a world leader in design and production of Broadband Fixed Wireless (BFW) systems.

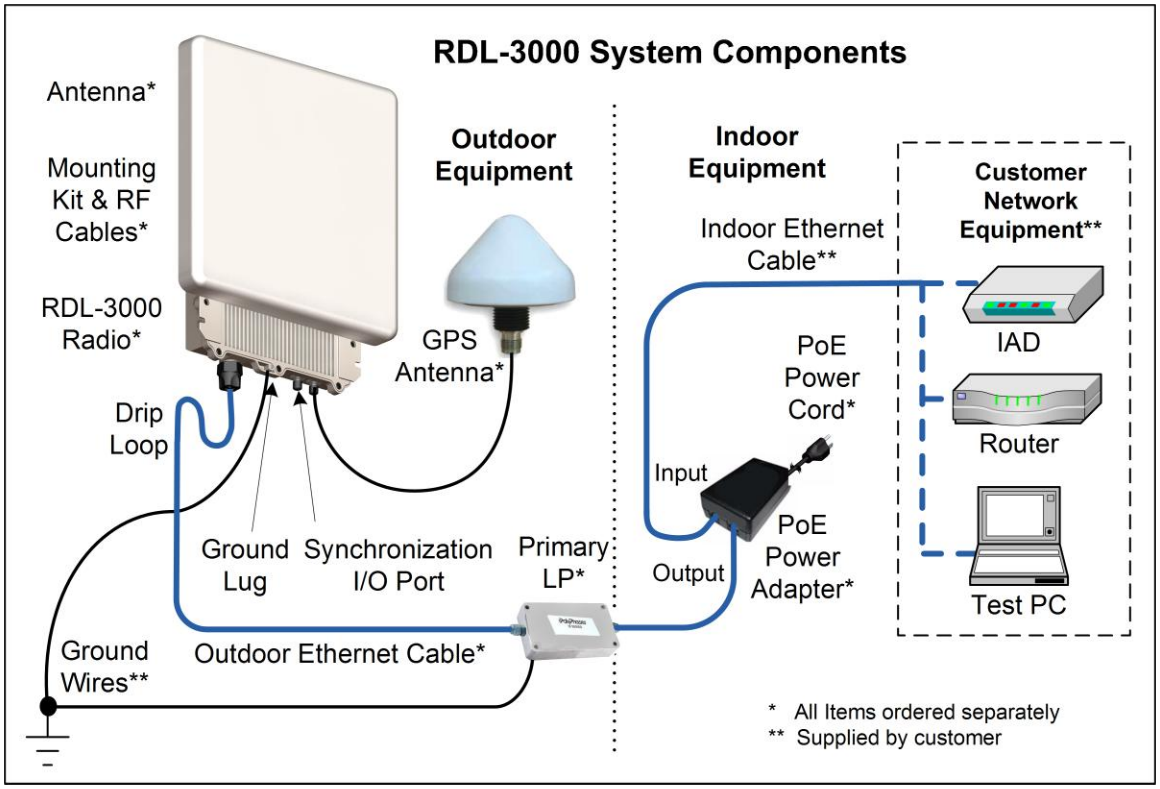


Fig. 2: Site Survey: RDL-3000 System Components

- Software configured common radio platform:
  - PTP and PMP applications
  - 4.9 to 5.8 GHz operation
- All outdoor configuration with IEEE 802.3at PoE
- Highest capacity system in the industry
- Up to 100 Mbps Ethernet throughput
- Lowest end-to-end latency
- Long-range capabilities
- QoS controls to manage traffic groups
- Software controlled speed and channel size selection
- Per-link dynamic TDD, ARQ & adaptive modulation/coding
- Synchronization option for collocated units (internal or GPS)
- Operates as a sector controller for AN-80i PMP subscribers

2.2 Ethernet Port

The Ethernet port (RJ-45 / F connector) receives DC power and provides Ethernet connectivity with the local network. The Ethernet port connects to the PoE adapter using a weatherproof CAT-5e Ethernet cable.

Note: The maximum total length of the Ethernet cable is 100 m (328 ft). For example, 95 m from the RDL-3000 to the PoE and 5 m from the PoE to the local network equipment.

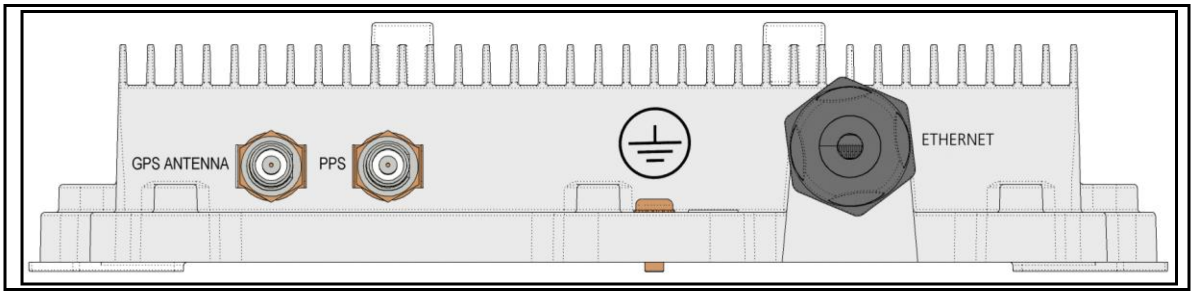


Fig. 3: **Features - RDL-3000 - Ethernet and Sync Ports (Bottom View of Radio)**

2.3 Synchronization I/O Port (PPS)

The PPS port (TNC / F connector) is provided to synchronize the RF transmission cycles of collocated sector controllers. This feature minimizes inter-sector interference by synchronizing the transmit cycles of collocated RDL-3000 sector controllers.

This port is software configurable: mode = input, output, or disabled, impedance = 50 ohms, 75 ohms, or high impedance. Multiple RDL-3000 units can be synchronized by using up to 46 m (~150 ft).of interconnecting synchronization cable.

Important: The synchronization feature must be used at any site where two or more sector controllers are deployed.

A factory-installed protective weatherproof plastic cap is installed on the PPS port. If this cap is removed to install a synchronization cable or TNC Tee connector, the port must be adequately weatherproofed. Refer to the RDL-3000 Installation guidelines for detailed instructions.

2.4 GPS Antenna Port (GPS ANTENNA)

The GPS antenna port (TNC / F connector) conducts RF signals between the RDL-3000 and the antenna system (ordered separately). This port is provided only on units factory-equipped with GPS hardware. The GPS antenna can be located remotely from the RDL-3000 unit by using up to 46 m (~150 ft) of high quality antenna cable. The GPS module does not set the RDL-3000 internal date/time clock.

Important: A GPS receiver must be provided at each sector controller site comprising a network of geographically collocated cells.

A factory-installed protective weatherproof plastic cap is installed on the GPS antenna port. If this cap is removed to install an antenna cable, the port must be adequately weatherproofed. Refer to the RDL-3000 Installation.

2.5 RF Ports

The two RF ports (N-type / F connectors) conduct RF signals between the RDL-3000 and the antenna system (ordered separately). The RDL-3000 can be operated using a SISO (single antenna) or MIMO (multiple antenna) system.

Important: Version 1.xx operation is limited to port RF-1. Port RF-2 must be electrically terminated (connect antenna or RF terminating device) and must be weatherproofed.

Important: A factory-installed protective weatherproof plastic cap is installed on the RF ports. When a cap is removed to install an antenna cable, the port must be adequately weatherproofed. Refer to the RDL-3000 Installation guidelines for detailed instructions.

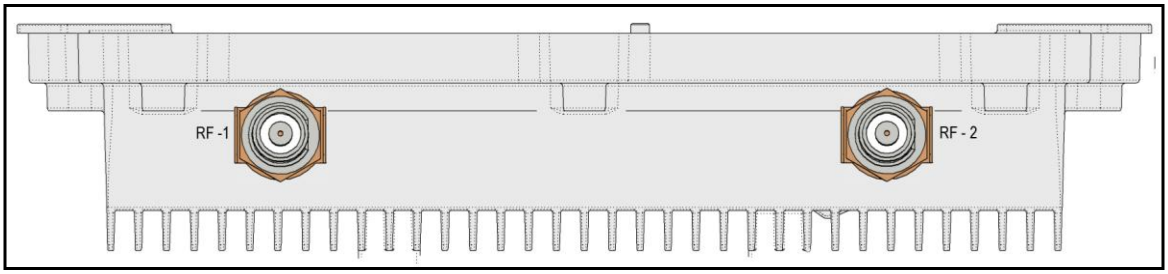


Fig. 4: Features - RDL-3000 RF Ports (Top View of Radio)

2.6 RF Jumper Cables

Two RF jumper cables are provided with each RDL-3000 mounting kit. The RF cables conduct RF signals between the RDL-3000 and the antenna system. The cable length supplied (230 mm or 400 mm) is based on the type of mounting kit.

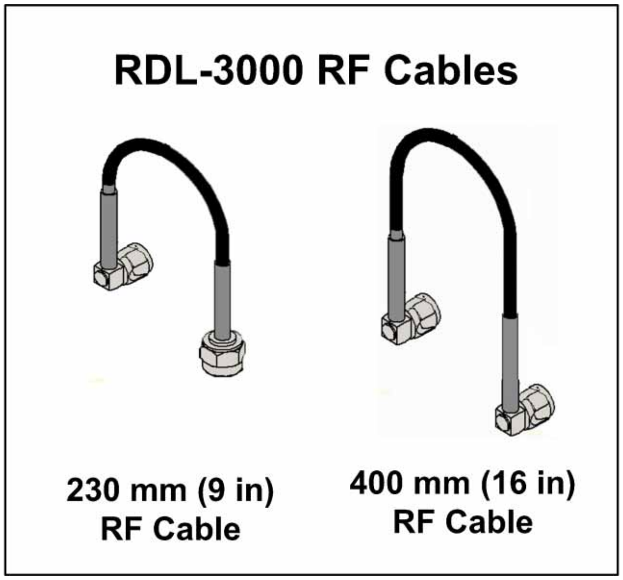


Fig. 5: Features - RDL-3000 - RF Jumper Cables

2.7 Ground Lug

A ground-lug ⏚ is provided on the RDL-3000 chassis. Use this connection to terminate a grounding wire. All RDL-3000 systems must be properly grounded to protect against power surges and accumulated static electricity.

2.8 Audible Alignment Tool

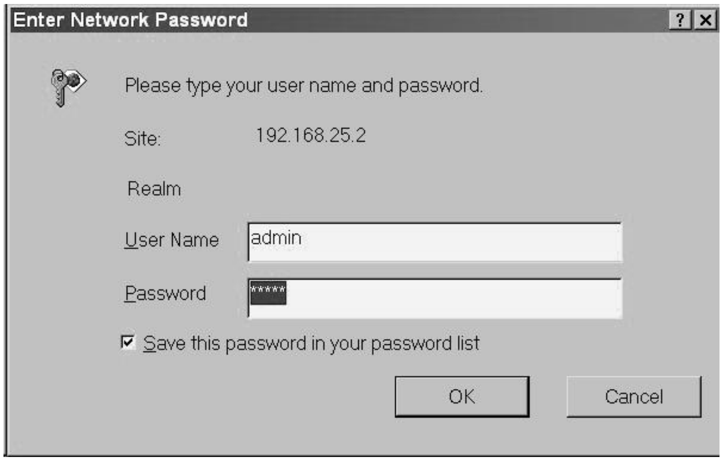
The audible alignment tool is provided to assist the installer to perform basic antenna alignment. When enabled, the audible alignment signal 'chirps' slowly when a low signal level is detected, and faster when stronger signals are detected. The tool is enabled and disabled using the Web or CLI interface.

2.9 Management Interfaces

The operator can use a standard Web browser or Telnet client to access all settings and statistics necessary to configure and monitor the operation of the RDL-3000. The unit can also be configured monitored using the SNMP-based Redline ClearView NMS .

2.9.1 Web Browser (HTTP)

To monitor and configure the RDL-3000 using HTTP, open a Web browser (Internet Explorer 6 or higher recommended) and enter the unit IP address. For new systems, the default IP address is 192.168.25.2. The following login dialog should be displayed:



Please type your user name and password.

Site: 192.168.25.2

Realm

User Name: admin

Password: *****

☑ Save this password in your password list

Fig. 6: **Features - Web Login to the RDL-3000**

The default username is 'admin' and the default password is 'admin'.

Note: There is no logout command on the Web interface.

2.9.2 Telnet (CLI)

To monitor and configure the RDL-3000 using CLI, open a Telnet session using the unit IP address. When the command prompt screen appears, login to the RDL-3000. The default username is 'admin' and the default password is 'admin'. The RDL-3000 supports two concurrent Telnet sessions. One session with full read/write capabilities (administrator) and a second concurrent session with read-only access.

The Telnet session is logged out automatically when no commands are received (idle) for a period of ten minutes. Use the following command to exit immediately from the CLI:

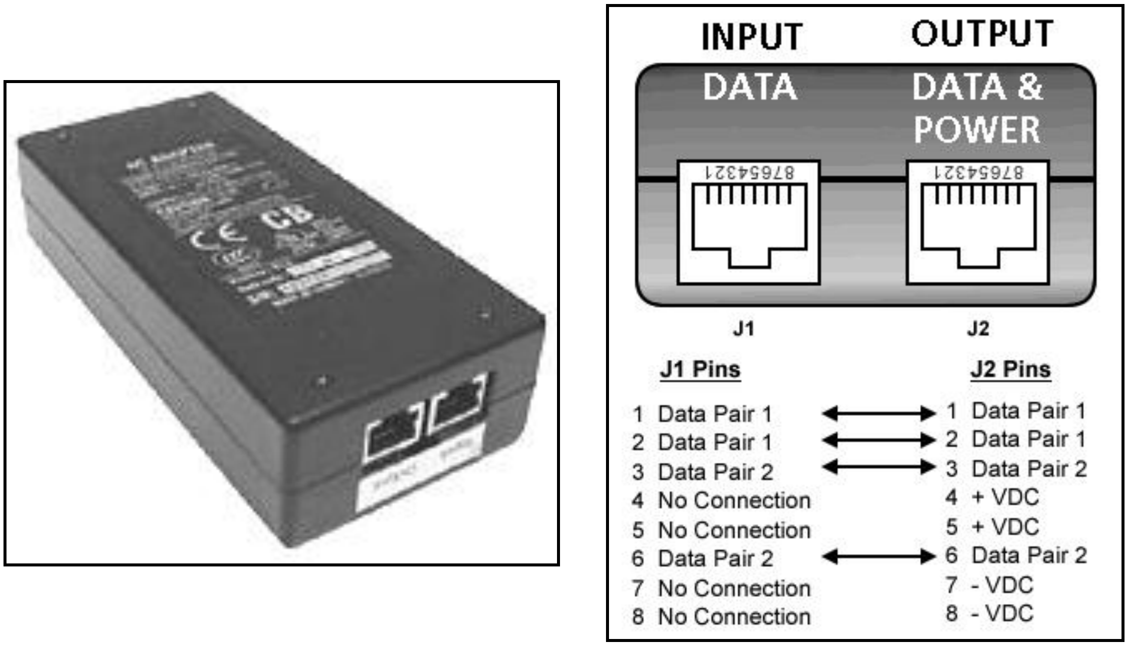
```
logout [ENTER]
```

2.9.3 ClearView NMS Application

The Redline Management Suite is a set of applications designed to assist provisioning, monitoring and administration of the Redline components deployed in Radio Access Networks (RANs). Contact your Redline representative or visit the Redline website for further information about the Redline ClearView NMS application.

2.10 PoE Power Adapter

The PoE power adapter (Standard IEEE 802.3at PoE, 25 W max.) supplies operational power (48 VDC) to the RDL 3000. Power is injected using four reserved wires in the Ethernet cable. The RJ-45 / F connectors allow for easy mid-span installation without opening the Ethernet cables. The power adapter AC input is auto-sensing 110/220/240 VAC 50/60 Hz. Cables are available with NA, EU, or UK plugs.



J1 Pins		J2 Pins
1 Data Pair 1	↔	1 Data Pair 1
2 Data Pair 1	↔	2 Data Pair 1
3 Data Pair 2	↔	3 Data Pair 2
4 No Connection		4 + VDC
5 No Connection		5 + VDC
6 Data Pair 2	↔	6 Data Pair 2
7 No Connection		7 - VDC
8 No Connection		8 - VDC

Fig. 7: **Features - Indoor Power-over-Ethernet (PoE) Module - AC Model**

Note: The PoE does not amplify the Ethernet signal. The maximum total length of the Ethernet cable is 91.5 m (300 ft). For example, 90 m (295 ft) from the RDL-3000 to the PoE and 1.5 m (5 ft) from the PoE to the local network equipment.

Warning to Service Personnel**: **48 VDC

Customer equipment including personal computers, routers, etc., must be connected only to the INPUT (DATA) port on the PoE unit. Only the outdoors Ethernet interface cable connecting to the RDL-3000 can be safely connected to the OUTPUT (DATA & POWER) connector. Connecting customer premises Ethernet equipment directly to the OUTPUT (DATA & POWER) connector on the Power-over-Ethernet power adapter may damage customer equipment.

Chapter 3

3 Functional Description

3.1 Operational Modes

The RDL-3000 operates on a common software base controlled by options keys. Each key (a string of numbers, letters, and dashes) enables modes of operation (PTP/PMP), modulation, RF frequency, available channel sizes, etc. When no options key is installed (factory default), the RDL-3000 has very restricted operating parameters. The operator must obtain and enter a permanent options key for each RDL-3000 unit before deploying units in a production network. Refer to the following sections for operation in PMP mode. Refer to section 3.3: PTP Mode on page 35 for operation in PTP mode.

3.2 PMP Mode

This section describes the parameters required to configure PMP support and an overview of VLAN functions.

The RDL-3000 PMP firmware provides the following main features:

- IEEE 802.1Q/1p standards compliance
- Multiple Virtual Local Area Network (VLAN) services per subscriber
- Individual Committed Information Rate (CIR) and Peak Information Rate (PIR) setting per service
- VLAN Service Groups (broadcast/multicast) span subscribers
- VLAN tagged management traffic
- Multiple Transparent LAN Services (TLS) transport based on VLAN ID classification
- VLAN trunking with tag insert/delete/re-map

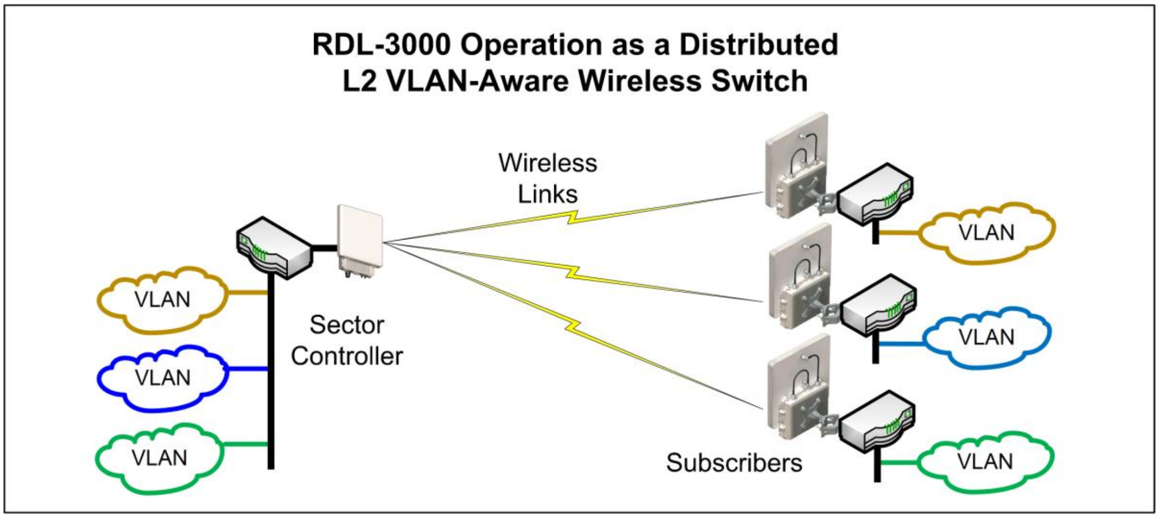

RDL-3000 Operation as a Distributed
L2 VLAN-Aware Wireless Switch
Wireless
Links
VLAN
VLAN
VLAN
Sector
Controller
VLAN
VLAN
VLAN
Subscribers

Fig. 8: PMP - RDL-3000 Distributed L2 VLAN-Aware Wireless Switch

The RDL-3000 can operate as a point-to-multipoint (PMP) VLAN-aware wireless L2 switch, with traffic being classified and forwarded based on the packet VID. Each classification includes CIR/PIR settings to guarantee required bandwidth. The RDL-3000 also provides a 'Pass through' classification to forward traffic not matched to any defined VID, or to generally forward all traffic received on a port.

Operation in PMP mode is controlled by the options keys. Enter PMP-enabled options keys before deploying and configuring the RDL-3000 units. The options keys enable specific PMP options, including the total number of subscribers. A specific range of RF power settings are provided for PMP operation.

Ethernet data traffic can not be transmitted over the wireless interface until at least one **Link**, **Service Group**, and **Service** have been provisioned. All provisioning is performed on the sector controller:

> **Link**: Enable a wireless connection between the sector controller and a subscriber and set the uplink and downlink rates uncoded burst rates (UBR). Rates are set individually for each link.
>
> **Service Group**: Define packet filtering at the sector controller Ethernet port and set parameters for broadcast/multicast groups.
>
> **Service**: Define packet filtering at the subscriber Ethernet port and set parameters for subscriber (unicast) traffic.

3.2.1 Wireless Links

A Link enables a wireless connection from the sector controller to the subscriber and sets the uplink and downlink rates (UBR). The sector controller will only communicate with registered subscribers. Each link is uniquely identified with a name and the MAC address of the subscriber.

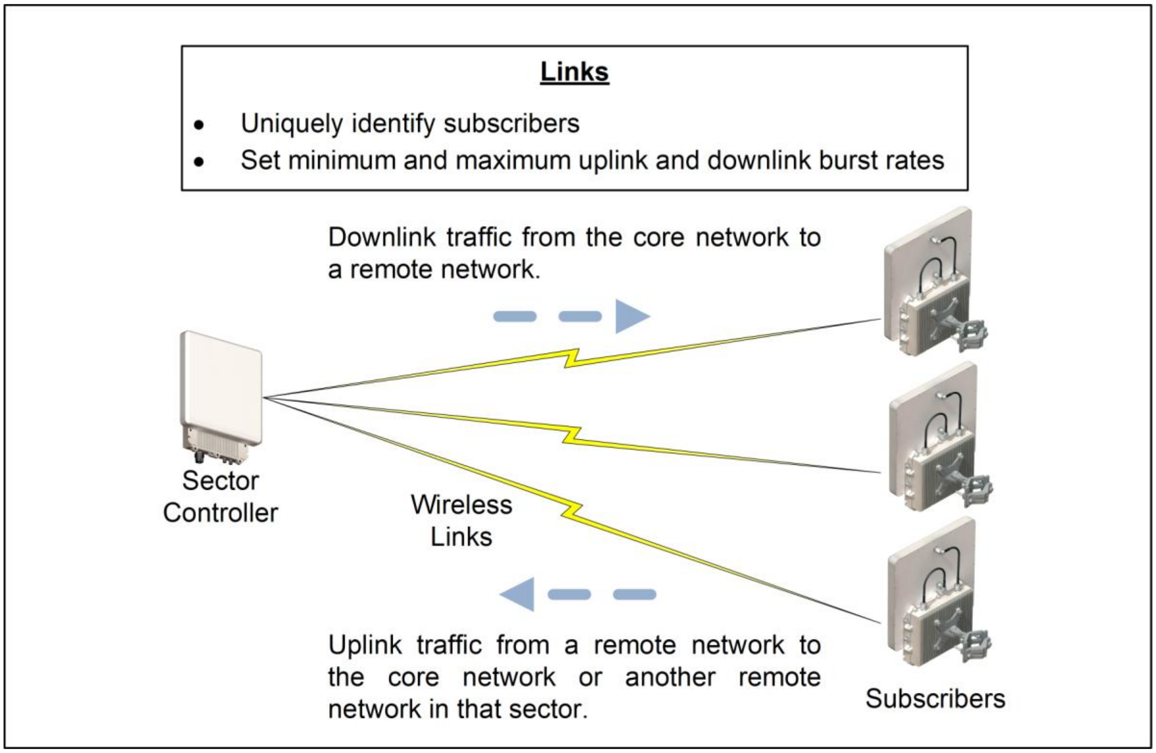

Links
• Uniquely identify subscribers
• Set minimum and maximum uplink and downlink burst rates
Downlink traffic from the core network to a remote network.
Sector Controller
Wireless Links
Uplink traffic from a remote network to the core network or another remote network in that sector.
Subscribers

Fig. 9: PMP - Wireless Subscriber Links

3.2.2 Services and Service Groups

The RDL-3000 operates as a VLAN-aware wireless L2 switch, classifying and forwarding traffic based on the packet VID. Ethernet ingress packets containing a VLAN (802.1Q) field are first compared to the tagged-type Service Groups (sector controller) or Services (subscriber) associated with that port.

When a VID is matched, the packet is processed according to the settings for that Service Group or Service. Packets with a unicast address are forwarded based on destination address. Packets with a multicast/broadcast address, and unicast addresses with unknown destinations, are forwarded to all Service Group members.

A Service Group or Service set to 'Pass through' mode forwards (unmodified) packets not matched to any tagged Service Group or Service (e.g., unmatched VID or packet without 802.1Q tag).

Table 3: Web - Operation - Traffic Classification

Type	Function	Settings
Service Group	Classify and forward ingress and egress traffic at the sector controller Ethernet port.	Tagging Mode (VLAN/Pass through) VLAN ID (tag) Default Priority
Service	Classify and forward ingress and egress traffic at the subscriber Ethernet port.	Tagging Mode (VLAN/Pass through) VLAN ID (tag) Default Priority

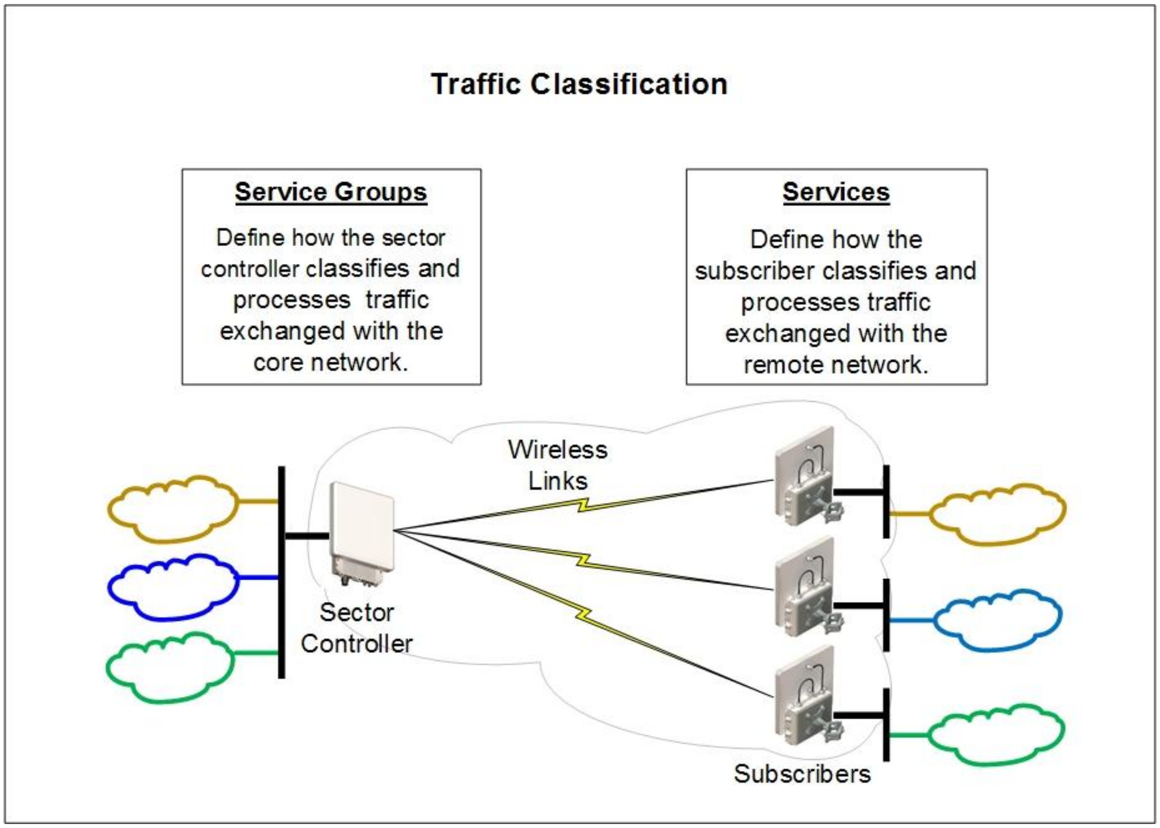

Traffic Classification
Service Groups
Define how the sector controller classifies and processes traffic exchanged with the core network.
Services
Define how the subscriber classifies and processes traffic exchanged with the remote network.
Wireless Links
Sector Controller
Subscribers

Fig. 10: PMP - Services and Service Groups

Services

Services define classification (filtering) for ingress and egress packets at the subscriber Ethernet port, and set the uplink and downlink rates (per Service definition) for unicast traffic transmitted across the wireless interface. Service settings include VLAN ID (tag), default priority, parent Link, and parent Service Group (see 3.2.3: Setting Wireless Rates on page 26).

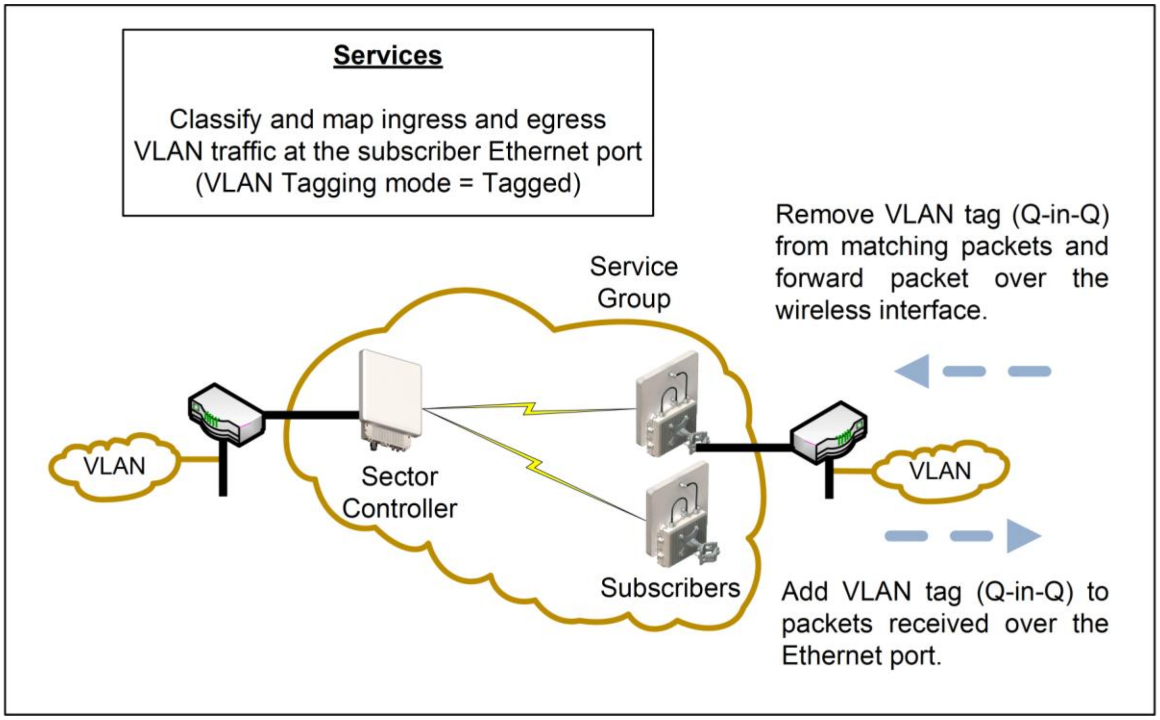

Services
Classify and map ingress and egress VLAN traffic at the subscriber Ethernet port (VLAN Tagging mode = Tagged)
Remove VLAN tag (Q-in-Q) from matching packets and forward packet over the wireless interface.
Service Group
VLAN
Sector Controller
VLAN
Subscribers
Add VLAN tag (Q-in-Q) to packets received over the Ethernet port.

Fig. 11: PMP - Services (Subscriber)

Notes:

1. Ethernet port ingress packets with VLAN tags matching a Service definition have the VLAN tag removed (Q-in-Q), and are forwarded over the wireless interface. Forwarding is based on the packet address:
2. Unicast packets addressed to a known address, and the host is a member of this Service Group, are forwarded only to the host sector controller or subscriber (hairpinning).
3. Broadcast, multicast, and unknown unicast packets are forwarded to all Service Group members.
4. Ingress packets that do not match any classification are discarded.
5. Ethernet port egress packets (received over the wireless interface) have the associated VLAN tag added (Q-in-Q) and are forwarded on the Ethernet segment.
6. Each Service must belong to a Service Group and a Link.
7. Packet priority is preserved. Default priority may be specified when priority was not specified in the original packet.

Service Groups

Services Groups define classification for ingress and egress packets at the sector controller Ethernet port, and set the uplink and downlink rates (per Service Group) for broadcast and multicast traffic transmitted across the wireless interface. Service Group settings include VLAN ID (tag), default priority, and broadcast rates (see 3.2.3: Setting Wireless Rates on page 26).

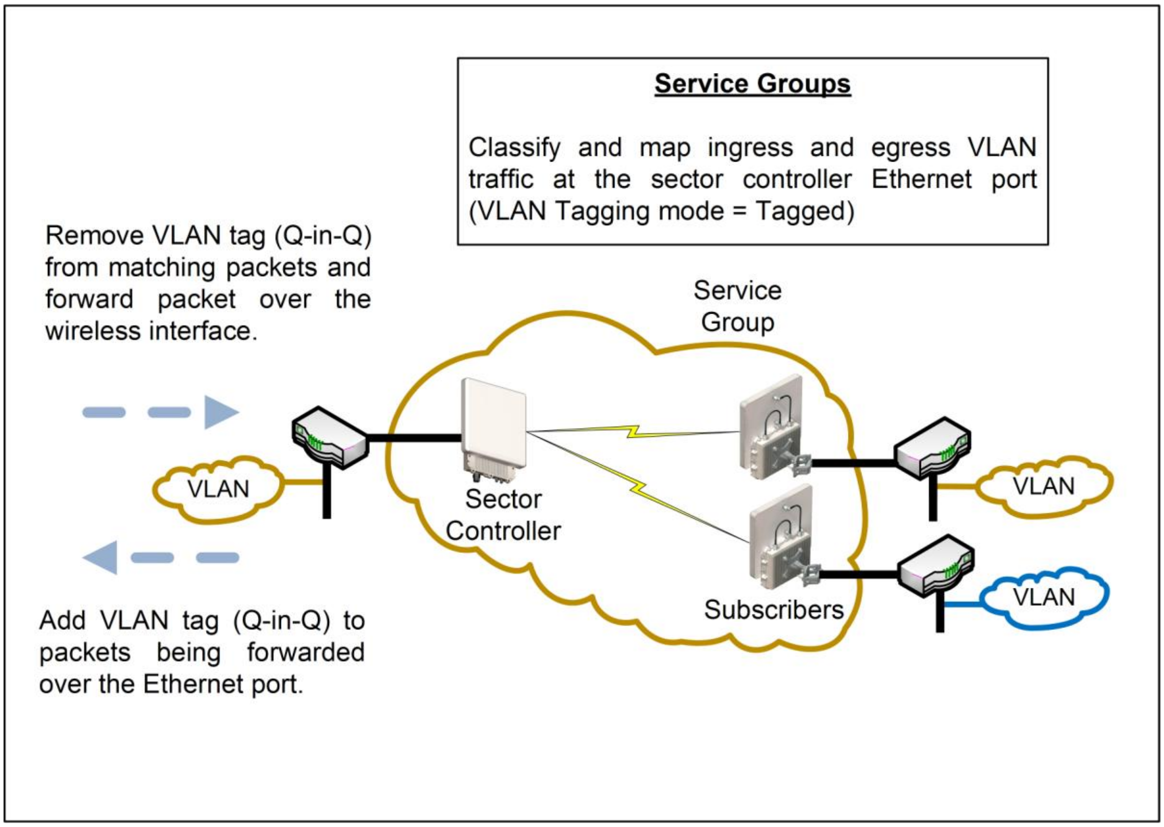

Service Groups
Classify and map ingress and egress VLAN traffic at the sector controller Ethernet port (VLAN Tagging mode = Tagged)
Remove VLAN tag (Q-in-Q) from matching packets and forward packet over the wireless interface.
Service Group
VLAN
Sector Controller
VLAN
VLAN
Subscribers
Add VLAN tag (Q-in-Q) to packets being forwarded over the Ethernet port.

Fig. 12: PMP - Service Groups (Sector Controller)

Notes:

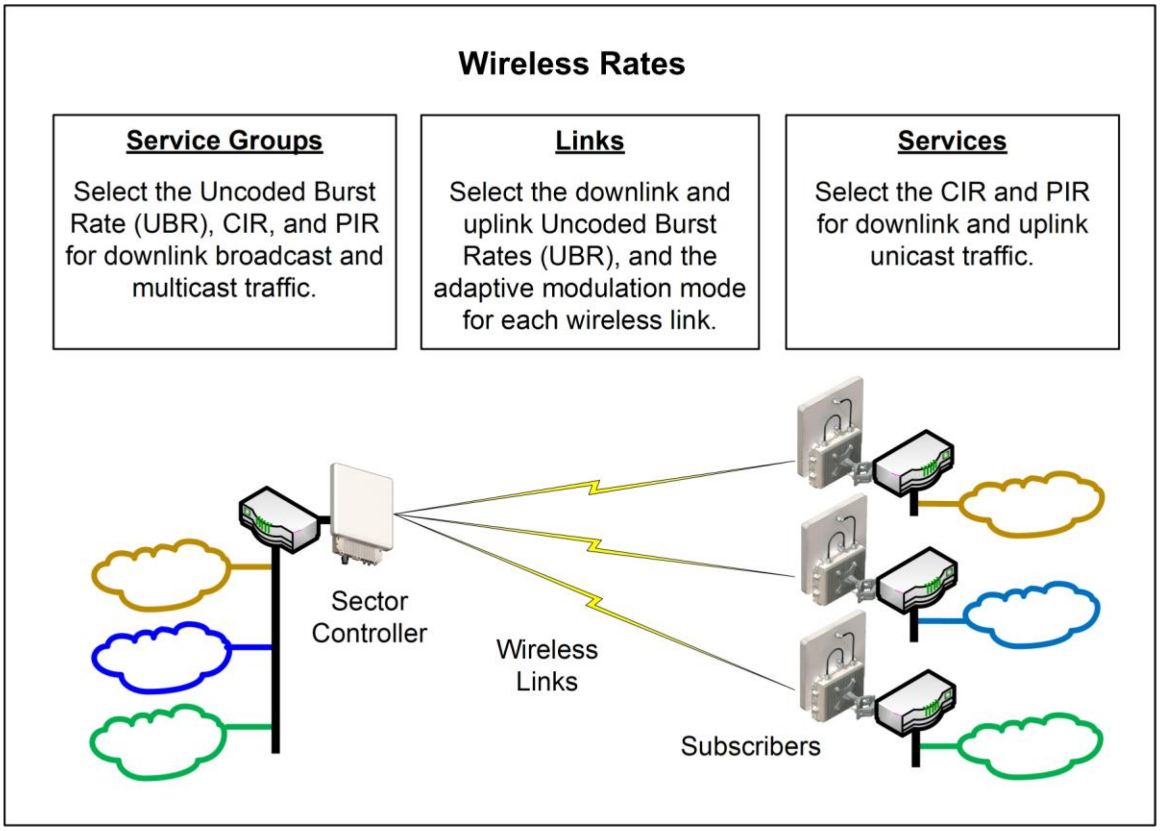
1. Ethernet port ingress packets with VLAN tags matching a Service definition have the VLAN tag removed (Q-in-Q), and are forwarded over the wireless interface. Forwarding is based on the packet address:
   a. Unicast packets addressed to a known address, where the host is a member of this Service Group, are forwarded only to the host subscriber.
   b. Broadcast, multicast, and unknown unicast packets are forwarded to all Service Group members.
2. Ingress packets that do not match any classification are discarded.
3. Ethernet port egress packets (received over the wireless interface) have the associated VLAN tag added (Q-in-Q) and are forwarded on the Ethernet segment.
4. Packet priority is preserved. Default priority may be specified when priority was not specified in the original packet.

3.2.3 Setting Wireless Rates

The wireless bandwidth is shared between all subscribers in a sector. Use the following settings to control traffic rates over the wireless interface.

Table 4: Web - Operation - Wireless Rates

Type	Function	Wireless Settings
Link	Set the Uncoded Burst Rates (UBR) for uplink and downlink traffic to/from this subscriber. This rate is shared across all Services and Service Groups.	• Downlink UBR • Uplink UBR • Adaptive modulation mode
Service	Set the uplink and downlink rates (per Service) for unicast traffic to/from this subscriber.	• Downlink CIR / PIR • Uplink CIR / PIR
Service Group	Set the downlink rates (per Service Group) for multicast and broadcast traffic sent to members of this group.	• Downlink Burst rate • Downlink CIR / PIR



Wireless Rates

Service Groups

Select the Uncoded Burst Rate (UBR), CIR, and PIR for downlink broadcast and multicast traffic.

Links

Select the downlink and uplink Uncoded Burst Rates (UBR), and the adaptive modulation mode for each wireless link.

Services

Select the CIR and PIR for downlink and uplink unicast traffic.

Fig. 13: PMP - Wireless Rates

Notes:

1. Unicast traffic with an unknown destination (all RDL-3000 units maintain a forwarding table) is transmitted two modulation steps below the lowest rate currently in-use across all active Services.

3.2.4 Pass through Mode

A Service Group or Service set to 'Pass through' mode forwards (unmodified) packets not matched to any tagged Service Group or Service (e.g., unmatched VID or packet without 802.1Q tag).

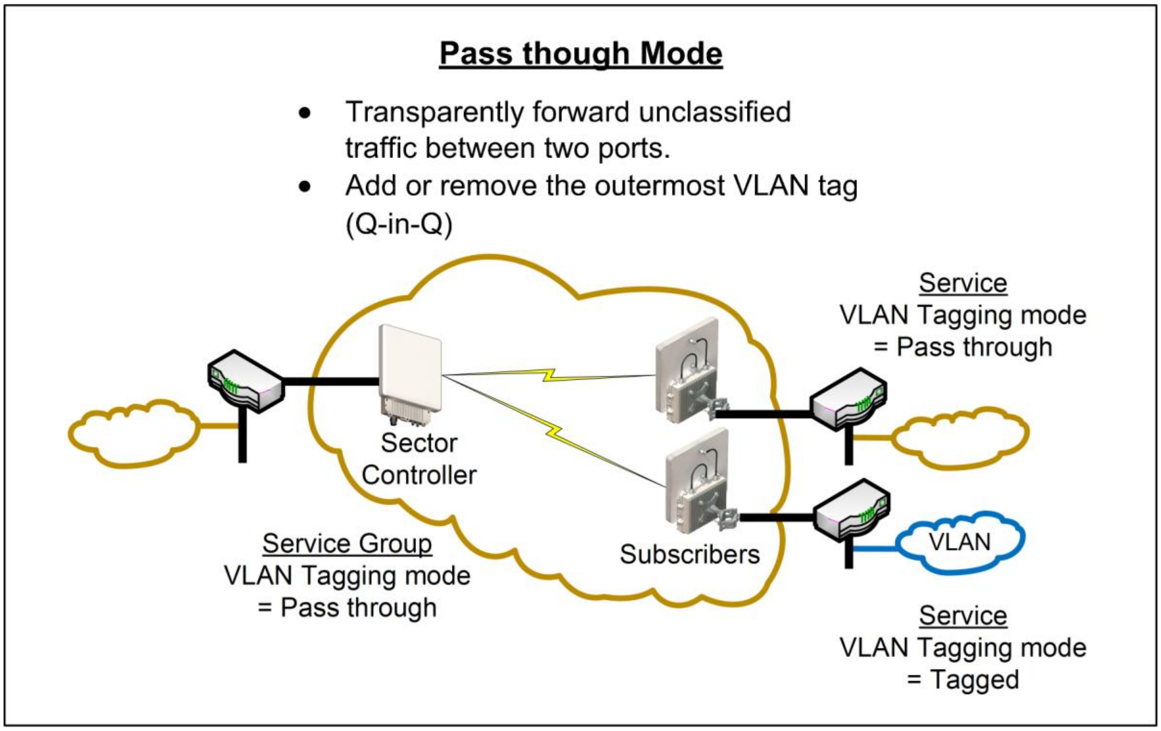
Examples of 'Pass through' mode:

- Forward traffic transparently between two ports.

  For example, both ports set to 'Pass though'.

- Add or remove outermost VLAN tag (Q-in-Q) based on the traffic to/from an Ethernet network segment.

  For example, one port is 'tagged' and the other port is 'Pass though'.



Pass though Mode

- Transparently forward unclassified traffic between two ports.
- Add or remove the outermost VLAN tag (Q-in-Q)

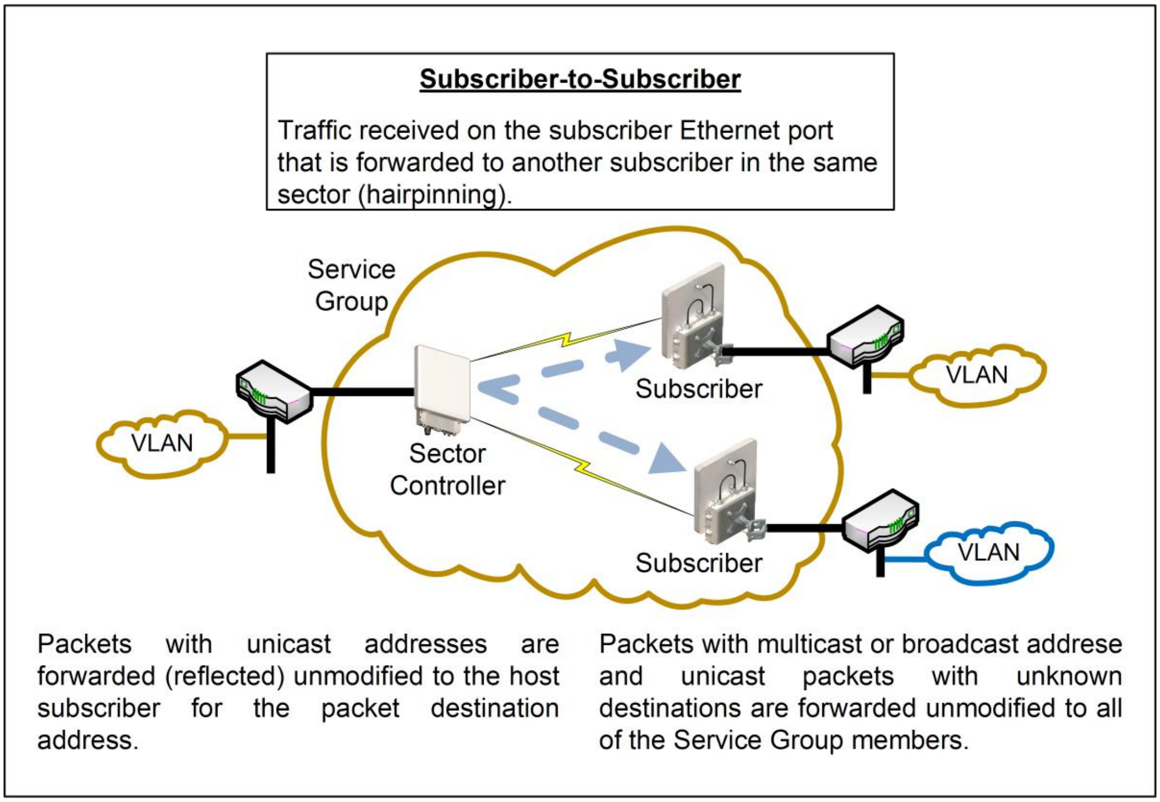
Fig. 14: PMP - 'Pass through' Mode

Notes:

1. Only one Service Group (sector controller) may be set to 'Pass though' mode.
2. Only one Service on each subscriber may be set to 'Pass though' mode.
3. Unmatched packets are discarded when no 'Pass through' filter is defined.

3.2.5 Subscriber-to-Subscriber Traffic

Subscriber-to-subscriber traffic (hairpinning) refers to forwarding a packet received on the subscriber Ethernet port to another subscriber in the same sector. Subscribers do not communicate directly, and packets are forwarded to the sector controller and re-transmitted (unmodified) over the wireless interface to the destination subscriber. Wireless data rates are based to the Service Group and member Services.



Subscriber-to-Subscriber

Traffic received on the subscriber Ethernet port that is forwarded to another subscriber in the same sector (hairpinning).

Packets with unicast addresses are forwarded (reflected) unmodified to the host subscriber for the packet destination address.

Packets with multicast or broadcast addrese and unicast packets with unknown destinations are forwarded unmodified to all of the Service Group members.

Fig. 15: PMP - Subscriber-to-Subscriber Unicast Traffic

Notes:

1. Subscriber-to-subscriber broadcast and multicast traffic may optionally be blocked.

3.2.6 VLAN Tagged Management

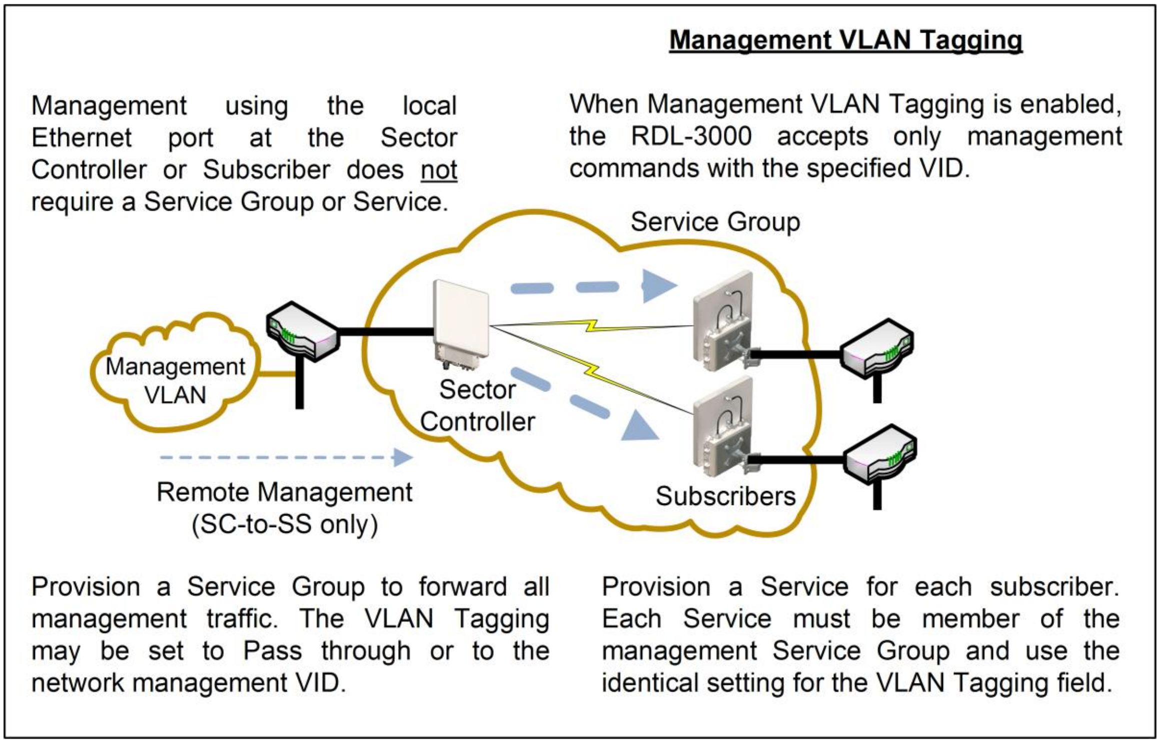
When the Management VLAN Tagging feature is enabled, the RDL-3000 recognizes only management commands received in VLAN packets with the specified VID.

Remote Management

Use of remote management (over the wireless interface) requires creating a Service Group and adding a Service for each managed subscriber. The CIR and priority settings must provide sufficient bandwidth and priority to perform administrative tasks.

Local Management

A Service Group and Services are not required for local access to the RDL-3000 using the Ethernet port. Ingress packets received on the Ethernet port are checked for a VLAN tag with the management VID before performing classification, and matching packets are forwarded directly to the management application.



Management VLAN Tagging

Management using the local Ethernet port at the Sector Controller or Subscriber does not require a Service Group or Service.

When Management VLAN Tagging is enabled, the RDL-3000 accepts only management commands with the specified VID.

Provision a Service Group to forward all management traffic. The VLAN Tagging may be set to Pass through or to the network management VID.

Provision a Service for each subscriber. Each Service must be member of the management Service Group and use the identical setting for the VLAN Tagging field.

Fig. 16: PMP - VLAN Tagged Management

Notes:

1. For initial installation and setup, it is recommended to use 'Pass through' mode for the management Service Group and member Services. Connectivity issues with VLAN services may cause the RDL-3000 management function to be unreachable and require a site visit and/or long reset operation to recover control of the unit.
2. The remote unit can be managed over the air only via the sector controller (SC)Ethernet port (security restriction).

3.2.7 PMP Configurations

This section describes basic configurations for an RDL-3000 PMP system.

VLAN Services

Default Groups and Services

In this example, all voice traffic is separated from data traffic, allowing specific CIR and PIR value to be set for this traffic. All traffic not classified to the Voice Service Group is processed by the Data Group (Pass through mode).

The Voice Group and member Services are configured for tagged traffic. The VLAN tag (VID=3) is removed from packets received from the wired network and restored when the packet is forwarded on the remote wired network (both directions). The Data Group and Services are configured for Pass-through mode and packets are forwarded unmodified to the destination port.

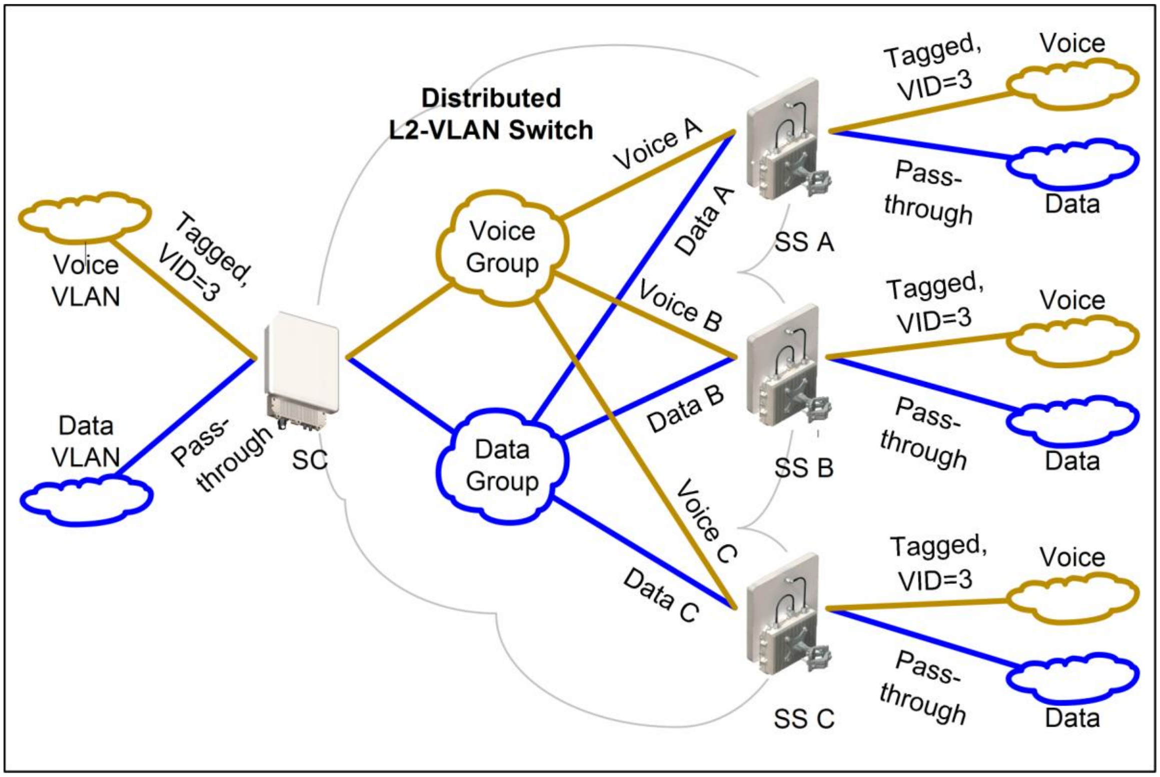


Fig. 17: PMP - Operation - VLAN Services - Default Groups and Services

Notes:

1. This configuration does not enforce a Service Group to have a Service on every subscriber.
2. The sector controller Ethernet port may be disable to support a private network.

VLAN Mapping

In this example, the RDL-3000 performs VLAN mapping between selected ports. This function is comparable to Label Switch Router (LSR) in Multi-protocol Label Switching (MPLS). VLAN tagging is assigned independently for each Service Group (sector controller port) and Service (subscriber port).

Ingress packets with VID=3 received on the sector controller Ethernet port are classified to the 'Voice Group' and forwarded over the wireless interface based on packet destination address. Packets forwarded by subscriber A and B are re-tagged with VID=3, while packets forwarded by subscriber C are tagged with VID=777. The process is

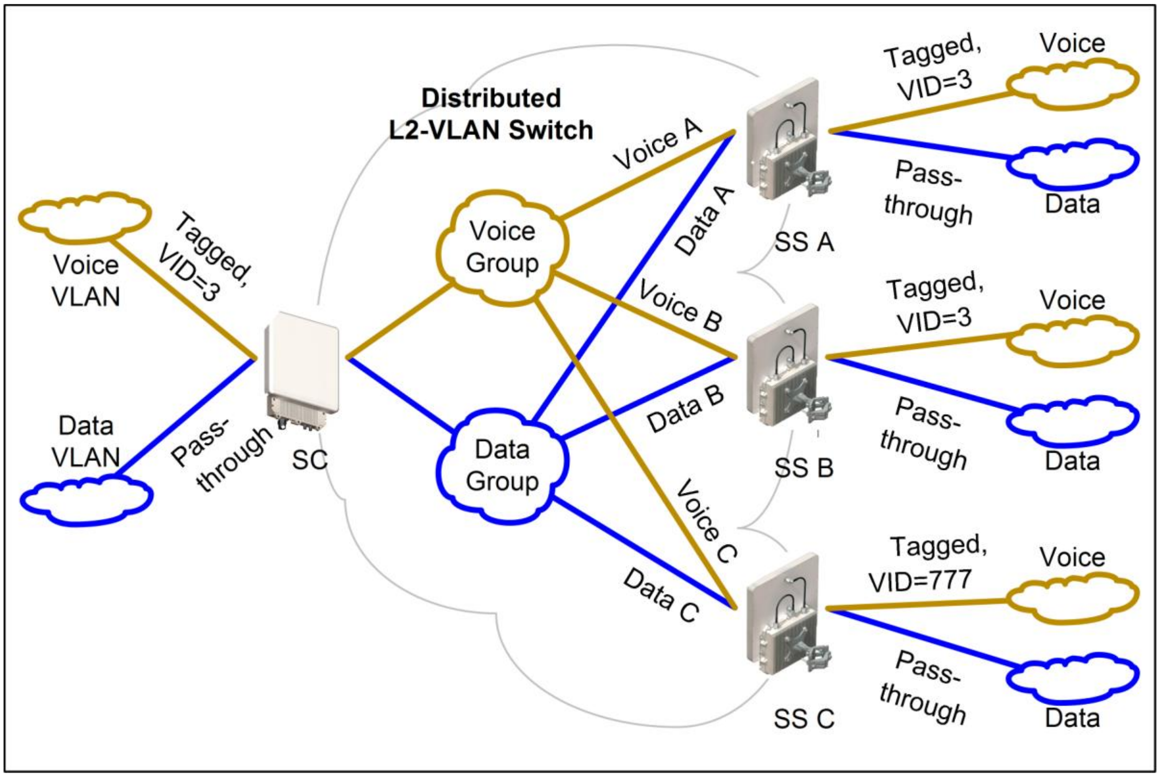


Fig. 18: PMP - Operation - VLAN Services - VLAN Mapping

Strict VLAN Tagging

In this example, only identified VLAN traffic is forwarded across the wireless interface. By not specifying a pass though Service Group, all unclassified packets are discarded.

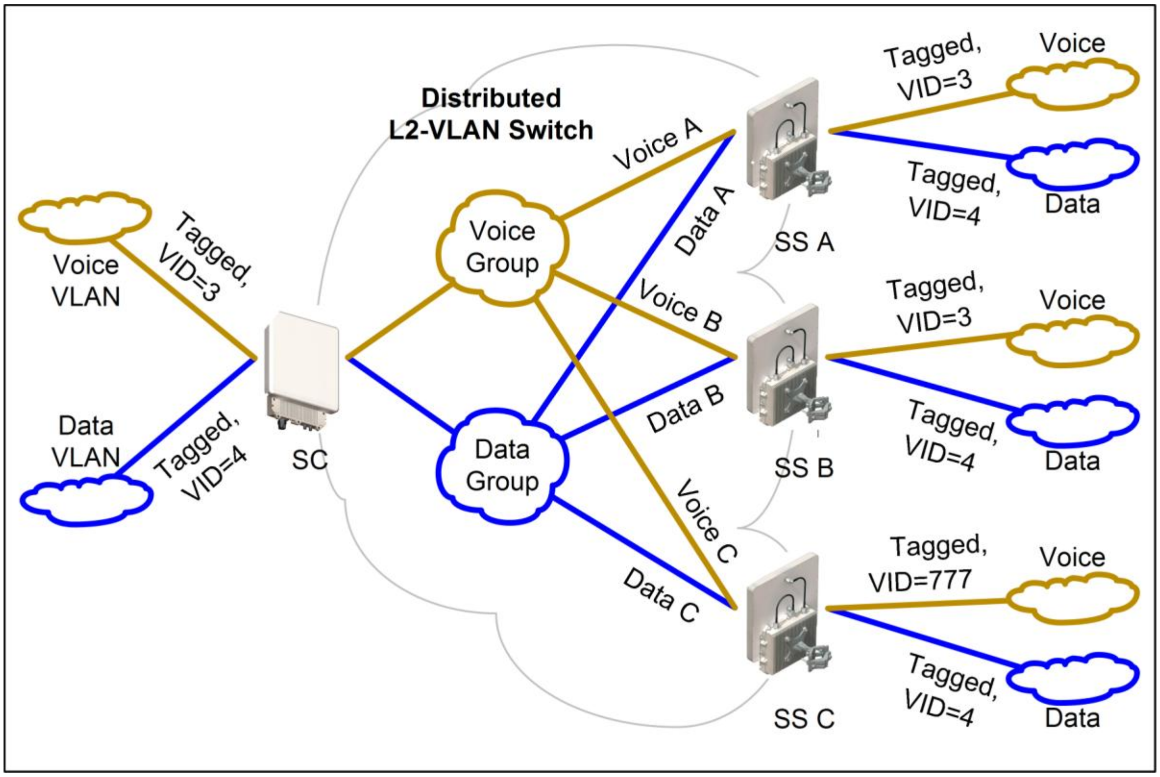


Fig. 19: PMP - Operation - Strict VLAN Tagging

TLS (Transparent LAN Services)

Extended TLS and Double Tagging

In this example, TLS traffic is extended across the wireless interface to remote locations. The TLS packets are segregated from other traffic by specifying a reserved VID for this traffic.

This solution allows unmodified traffic to be exchanged between Network B and Network C. Tagged traffic from Network B or Network C addressed to the TLS Network will be double-tagged (Q-in-Q) when forwarded to the TLS Network. Double-tagged packets from the TLS network addressed to Network B or Network C have the outer tag removed when the packet is forwarded to Network B or Network C.

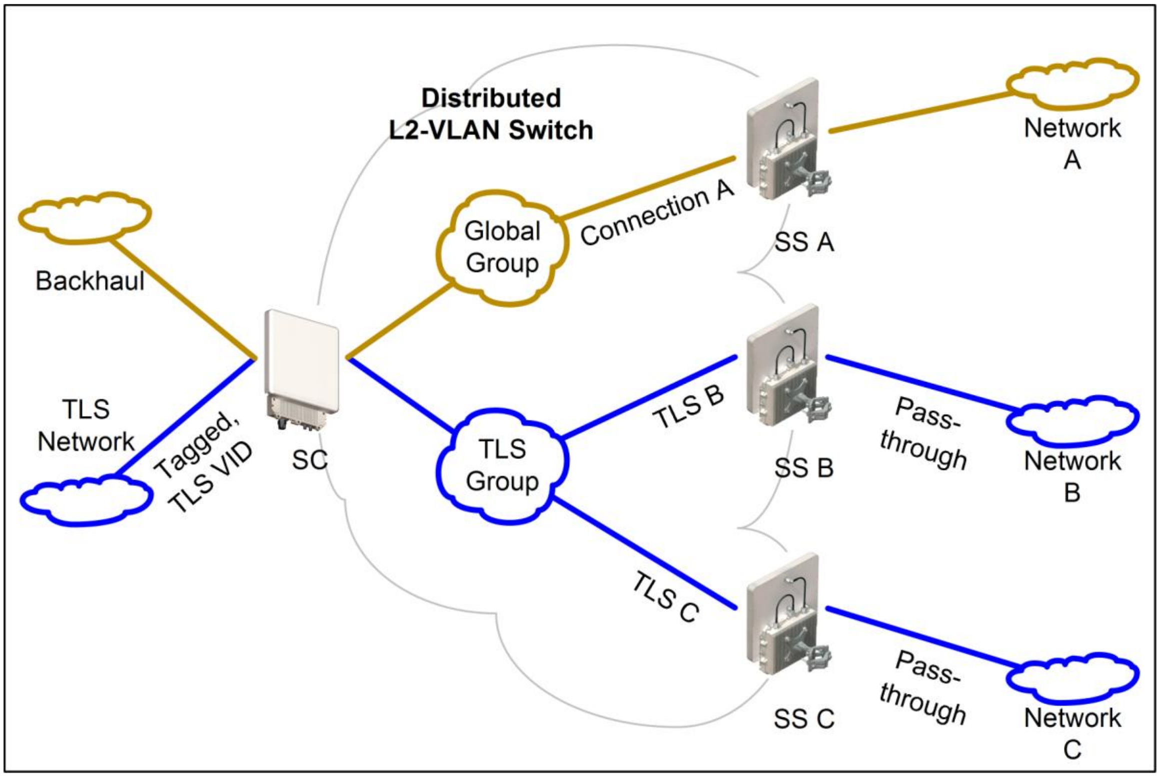


Fig. 20: PMP - Operation - TLS - Extended TLS and Double Tagging

Port-by-Port Tagging

In this example, the sector controller port accepts only tagged traffic and all subscriber ports are set to Pass though mode. A new Service Group is defined for every VLAN supported at the sector controller, with each Service Group having exactly one connection on the required link.

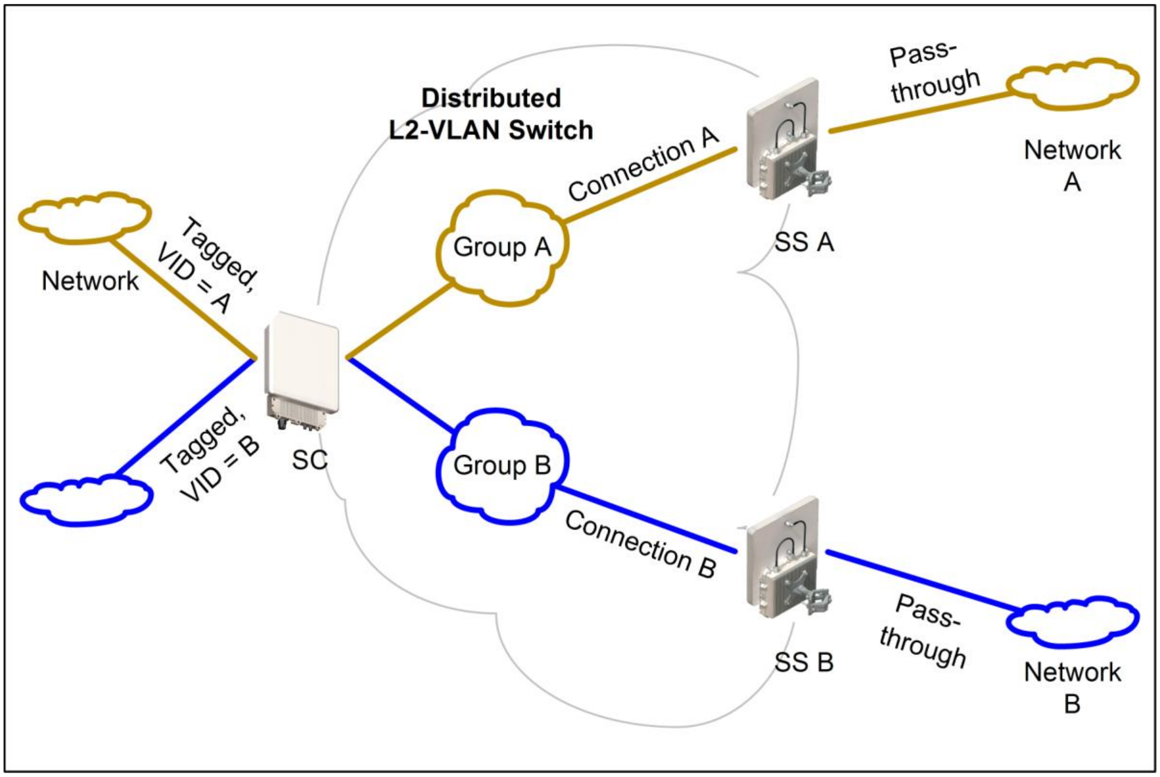


Fig. 21: PMP - Operation - Tagged Traffic - Port-by-Port Tagging

Notes:

1. The tagged port may be on the sector controller or subscriber.
2. Tagged traffic entering one of the subscribers exits the sector controller port double-tagged.

3.3 PTP Mode

The RDL-3000 can operate as a point-to-point (PTP) VLAN-aware wireless L2 switch, with traffic being classified and forwarded based on the packet VID. Each classification includes CIR/PIR settings to guarantee required bandwidth. The RDL-3000 also provides a 'Pass through' classification to forward traffic not matched to any defined VID, or to generally forward all traffic received on a port.

PTP mode is enabled by the options key. Enter a PTP-enabled options key before deploying and configuring the RDL-3000 units. The options key enables specific PTP options, including restricting operation to a single remote subscriber and a PTP-specific range of RF power settings.

One unit must be configured as a sector controller (PMP SC) and the second unit as a remote (PMP SS).

Note: Refer to the RDL-3000 installation Guidelines for additional information about installing and operating the RDL-3000 in PTP mode.

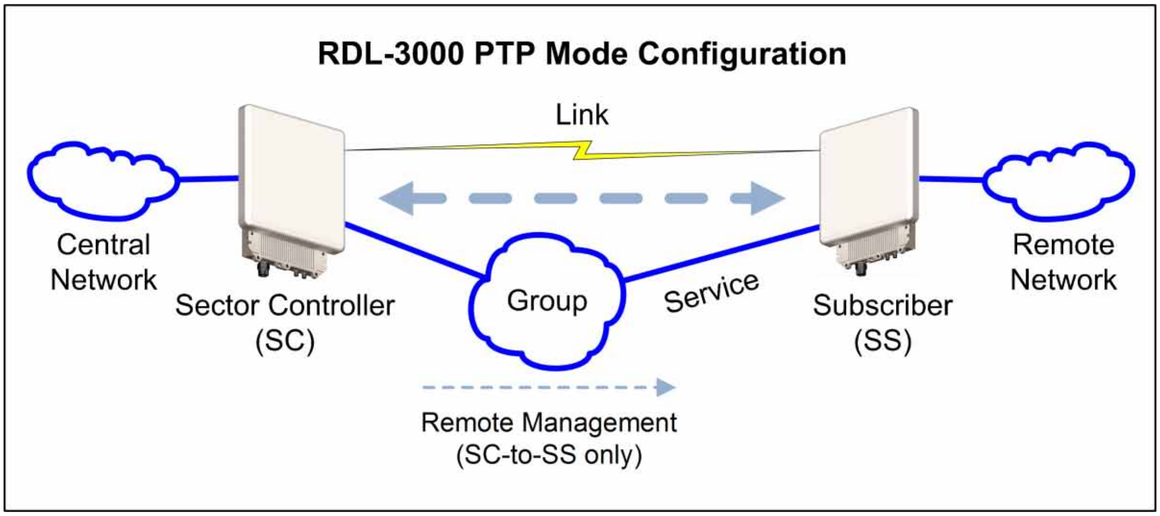


Fig. 22: PTP - RDL-3000 PTP Mode Configuration

Notes:

1. Service Group and Service settings should be set for the maximum throughput.
2. The remote unit can be managed over the air only via the sector controller (SC) Ethernet port (security restriction).

4 Web Interface

4.1 Network Connection to RDL-3000

The RDL-3000 can be configured and monitored using a PC equipped with a standard Ethernet port and a Web browser (Internet Explorer 6.0 or higher) or Telnet client. Refer to the following diagram for basic connections.

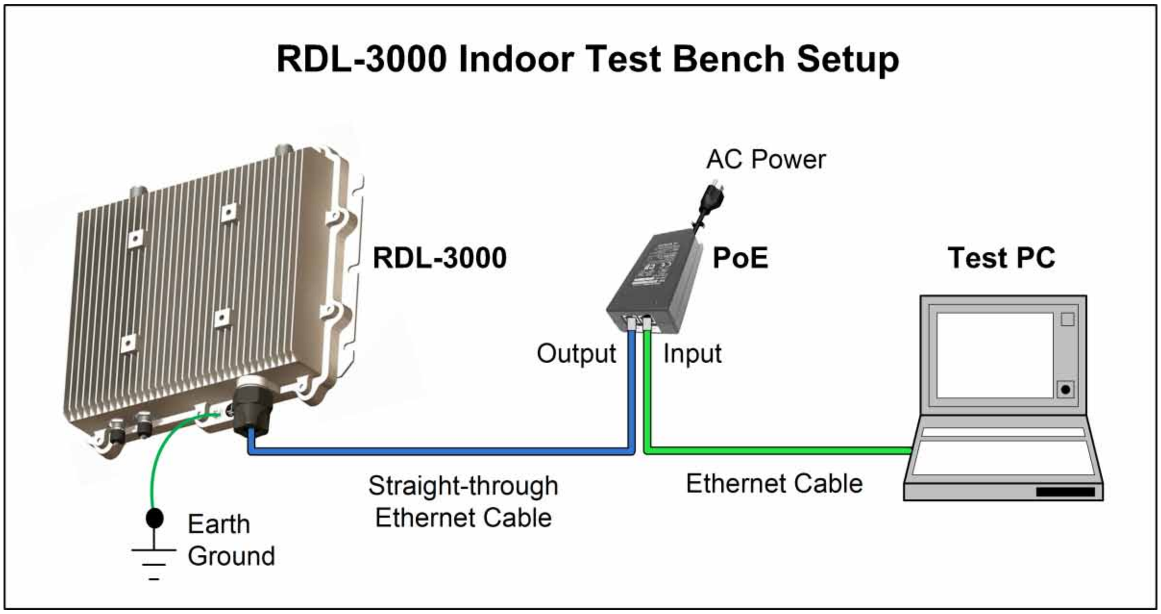

RDL-3000 Indoor Test Bench Setup
AC Power
RDL-3000
PoE
Test PC
Output
Input
Straight-through Ethernet Cable
Ethernet Cable
Earth Ground

Fig. 23: Web - Connecting a PC to the RDL-3000

Notes:

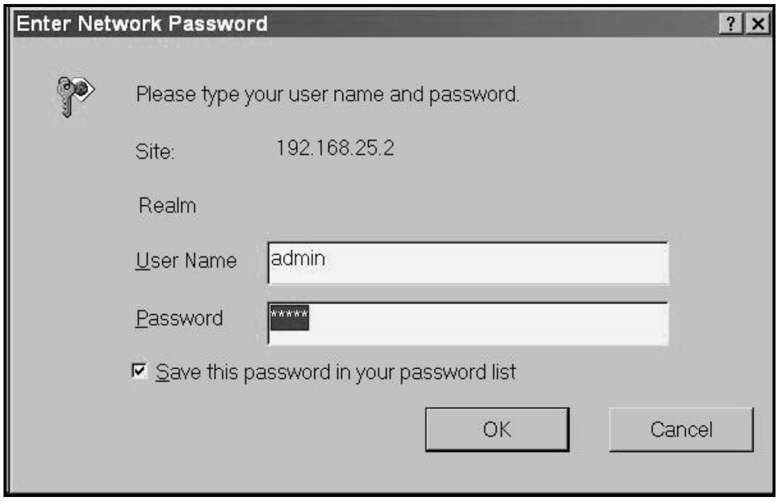
1. This diagram does not illustrate the surge protection required for outdoors installation of the RDL-3000 equipment. The system must be properly grounded to protect against power surges and accumulated static electricity. Refer to the RDL-3000 Installation Guidelines manual.
2. When configuring the RDL-3000 in sector controller mode (PMP SC), the RF ports must be properly terminated to an RF load device, or the radio must be disabled (Radio Enable = off).

Use the following steps to establish a Web session with the RDL-3000.

1. The IP address and subnet mask of the PC must be on the same subnet as the RDL-3000. For example:

	Test PC	RDL-3000 (default)
IP Address:	192.168.25.11	192.168.25.2
Net Mask:	255.255.255.0	255.255.255.0

2. On the test PC, open a browser and enter the unit RDL-3000 IP address.
3. When the dialog screen is displayed, enter the username and password to login. The factory default username is 'admin', and the default password is 'admin'.



Enter Network Password

Please type your user name and password.

Site: 192.168.25.2

Realm

User Name: admin

Password: *****

☑ Save this password in your password list

Fig. 24: Web - Login Screen

4. If the login was successful, the General Information screen is displayed in the Web browser.

4.2 System Menus and Access Permissions

4.2.1 Main Menus

The main menu items are different for the sector controller and subscriber functions.

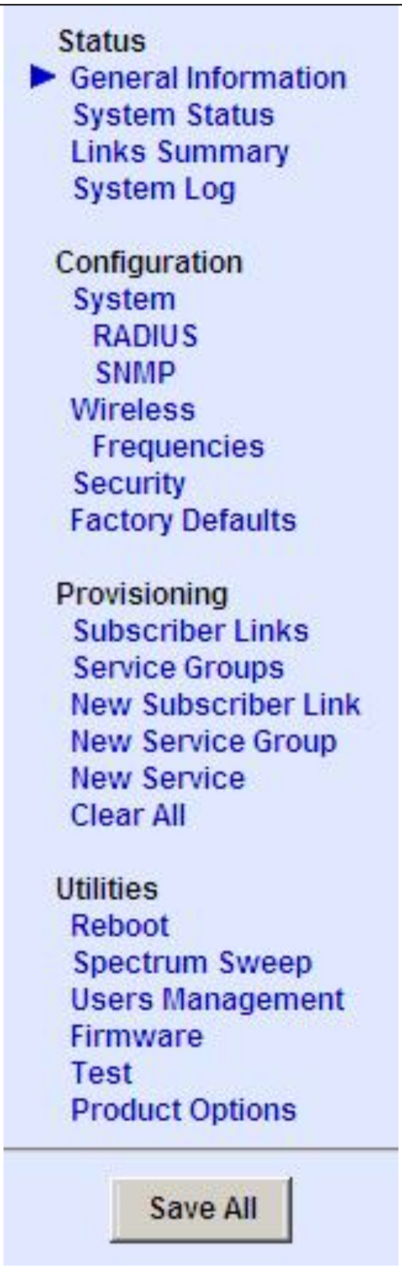
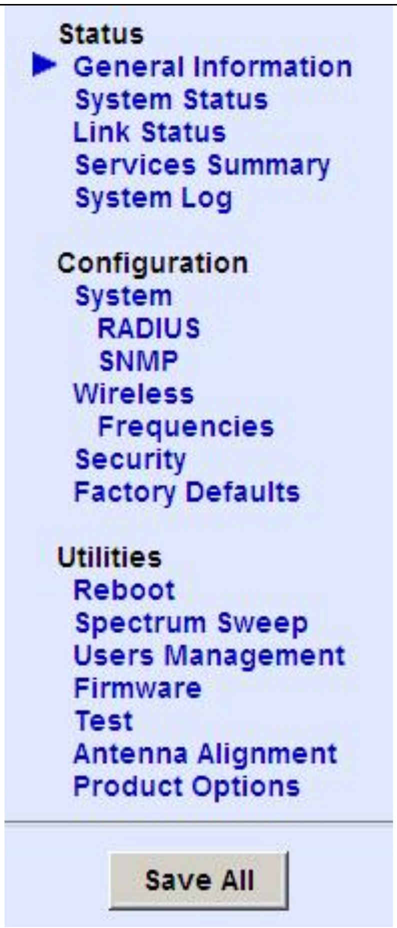
Sector Controller Menu	Subscriber Menu
	

Fig. 25: **Web - Main Menus for Sector Controller and Subscriber**

Notes:

1. Identical menus are used for PMP and PTP operation.

4.2.2 Access Permissions

The following table lists all menu commands, the associated Web GUI screens, and the required access permissions.

Table 5: Web - Screens and User Access

Menu Command	Screen Title	Admin		User		Description
		SC	SS	SC	SS	
Status						
General Information	General Information	✓	✓	✓	✓	View general identification and configuration.
System Status	System Status	✓	✓	✓	✓	View system, Ethernet, and wireless statistics.
Links Summary	Subscriber Links Summary	✓	N/A	✓	N/A	View all wireless links.
Services Summary	Subscriber Services Summary	N/A	✓	N/A	✓	View all wireless links.
System Log	System Events	✓	✓	✓	✓	View system status messages.
Configuration						
System	System Configuration	✓	✓	X	X	View and adjust system, and network settings.
-> RADIUS [1]	RADIUS Configuration	✓	✓	X	X	View and adjust RADIUS server settings.
-> SNMP [1]	SNMP Configuration	✓	✓	X	X	View and adjust SNMP settings.
Wireless	Wireless Configuration	✓	✓	X	X	View and adjust RF settings.
-> Frequencies [1]	Frequency Management	✓	✓	X	X	View and adjust RF scanning lists.
Security	Security Configuration	✓	✓	X	X	View and adjust security settings.
Factory Defaults [2]	N/A	✓	✓	X	X	Restore factory default settings.
Provisioning						
Subscriber Links	Subscriber Links	✓	X	N/A	N/A	Display all Subscriber Links.
-> Link Configuration [1]	Subscriber Link Configuration	✓	X	N/A	N/A	Configure selected Link.
-> Link Status [1]	Subscriber Link Status	✓	X	N/A	N/A	Display status of selected link.
Service Groups	Service Groups	✓	X	N/A	N/A	Display all Service Groups.
-> Group Configuration [1]	Service Group Configuration	✓	X	N/A	N/A	View/edit the configuration of the selected Service Group.
-> Group Status [1]	Service Group Status	✓	X	N/A	N/A	Display the status of the selected Service Group.

Table 5: Web - Screens and User Access						
Menu Command	Screen Title	Admin		User		Description
		SC	SS	SC	SS	
-> Service Configuration [1]	Service Configuration	✓	X	N/A	N/A	View/edit the configuration of the selected Service.
-> Service Status [1]	Service Status	✓	X	N/A	N/A	Display the status of the selected Service.
New Link	Subscriber Link Configuration	✓	X	N/A	N/A	Create a new Link.
New Service Group	Service Group Configuration	✓	X	N/A	N/A	Create a new Service Group.
New Service	Service Configuration	✓	X	N/A	N/A	Create a new Service.
Clear All	N/A	✓	X	N/A	N/A	Delete all Links, Service Groups and Services.
Utilities		✓				
Reboot	N/A	✓	✓	X	X	Reboot the RDL-3000.
Spectrum Sweep	Spectrum Sweep	✓	✓	X	X	Scan for interference.
Users Management [3]	Users Management	✓	✓	✓	✓	Manage user accounts and passwords.
Firmware	Firmware Management	✓	✓	X	X	Upload new firmware.
Test	N/A	✓	✓	X	X	Test for 5 minutes, and then restore the last saved configuration (no reboot).
Antenna Alignment	Antenna Alignment	X	✓	X	X	Display RSSI readings.
Product Options	Product Options	✓	✓	X	X	View / change the product options key.
Misc.						
Save All	N/A	✓	✓	X	X	Save all configuration changes.

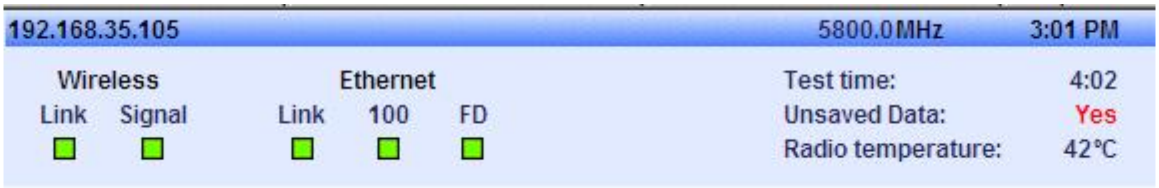
Notes:

1. Screen is displayed only after selecting the associated field item in the parent screen
2. The following settings are not affected when using the Factory Defaults function: system name, location, details and contact, frequency list, SNMP configuration, Idtable. Refer to the Diagnostics & Troubleshooting section for a comprehensive list of parameters and default settings.
3. User account can only modify the user account password.

4.3 Dashboard Display

4.3.1 General Information

The dashboard is displayed at the top of all Web screens. This feature displays a summary of important operational information.



192.168.35.105 5800.0MHz 3:01 PM

Test time: 4:02
Unsaved Data: Yes
Radio temperature: 42°C

Fig. 26: Web - Dashboard Display

IP Address: IP address of this unit.

Wireless Frequency: RF frequency in-use by this unit.

Time: Local time obtained from the Web browser.

Test time: Visible only when the Test function is active. The last saved configuration is restored when the counter reaches zero (unit is not rebooted). Click Save All in the main menu at any time to permanently save the current running configuration.

Unsaved Data: Indicates if the running configuration matches the saved configuration.

No: There are no differences between the running and saved configurations.

Yes: There are unsaved changes to the configuration. Unsaved settings are discarded when the system is rebooted. Click Save All in the main menu to permanently save the current running configuration.

Saving: The system is saving the runtime parameters to non-volatile RAM.

Radio Temperature: Internal temperature of the radio.

4.3.2 Wireless Leds

The Wireless LED indicators indicate the status of the wireless link.

Link LED

This LED is not implemented in the current software release.

Signal LED

This indication is valid only when the Link LED is on solid green. If Adaptive Modulation is enabled, the threshold refers to the 'minimum UBR' setting.

On: Wireless link is operating at or above the requested UBR.

Blink: Adaptive modulation is enabled AND the wireless link is operating below the minimum UBR.

4.3.3 Ethernet LEDs

These LED indicators provide a summary of the Ethernet port status.

Link LED

Off: Ethernet connection is not detected (e.g., Ethernet cable is disconnected).

On: Ethernet link is detected.

100 LED

Off: Ethernet port is operating at 10 Mb/s.

On: Ethernet port is operating at 100 Mb/s.

FD LED

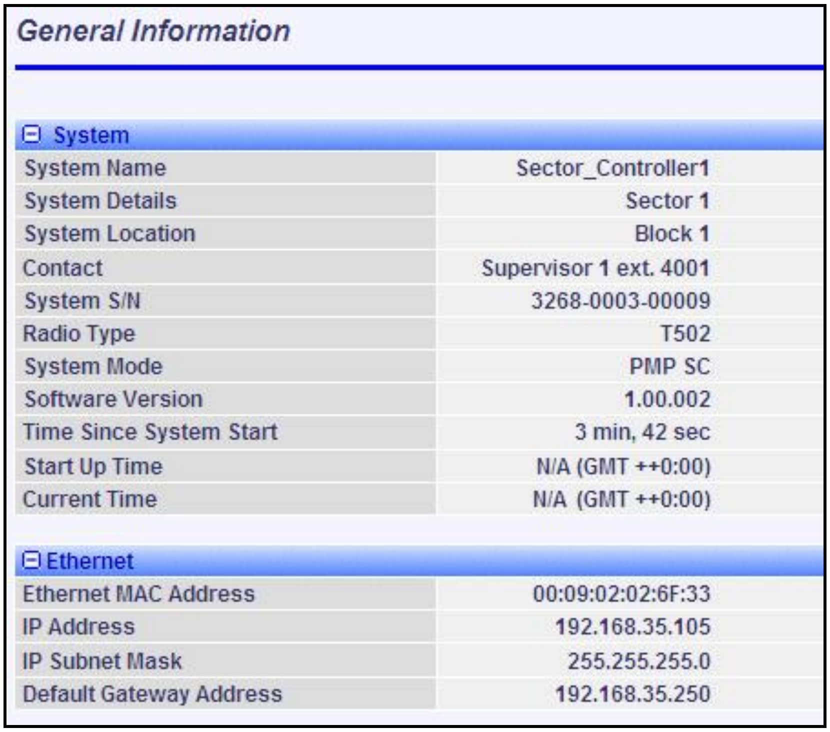
Off: Ethernet connection is operating in half-duplex mode.

On: Ethernet connection is operating in full-duplex mode.

4.4 Status Screens

4.4.1 General Information

The General Information screen displays system and the Ethernet interface details. Click ⊞ to expand fields and ⊟ to hide fields.



General Information

⊟ System

System Name	Sector_Controller1
System Details	Sector 1
System Location	Block 1
Contact	Supervisor 1 ext. 4001
System S/N	3268-0003-00009
Radio Type	T502
System Mode	PMP SC
Software Version	1.00.002
Time Since System Start	3 min, 42 sec
Start Up Time	N/A (GMT ++0:00)
Current Time	N/A (GMT ++0:00)

⊟ Ethernet

Ethernet MAC Address	00:09:02:02:6F:33
IP Address	192.168.35.105
IP Subnet Mask	255.255.255.0
Default Gateway Address	192.168.35.250

Fig. 27: **Web - General Information Screen**

System

System Name: Name assigned to this unit.

System Details: System details entered for this unit.

System Location: System location information entered for this unit.

Contact: Contact information entered for this unit.

System SN: Serial number of this unit.

Radio Type: Type of radio installed in this unit. Refer to section 8.1 System Specifications for radio specifications.

System Mode: Operating mode of this unit:

PMP SC: This unit is configured as a sector controller. The unit automatically begins transmitting poll messages to locate and register remote subscribers.

PMP SS: This unit is configured to operate as a subscriber. The unit monitors the selected RF channel(s) for poll poll messages from a sector controller.

Firmware Version: Firmware version in use on this unit.

Time Since System Start: Elapsed time since the last system reboot/power-cycle.

Start Up Time: Date and time of the last system reboot/powered-cycle. Supported only when SNTP feature is enabled.

Current Time: Current time on the RDL-3000 internal clock. Supported only when SNTP feature is enabled.

Ethernet

Ethernet MAC Address: MAC address of this unit.

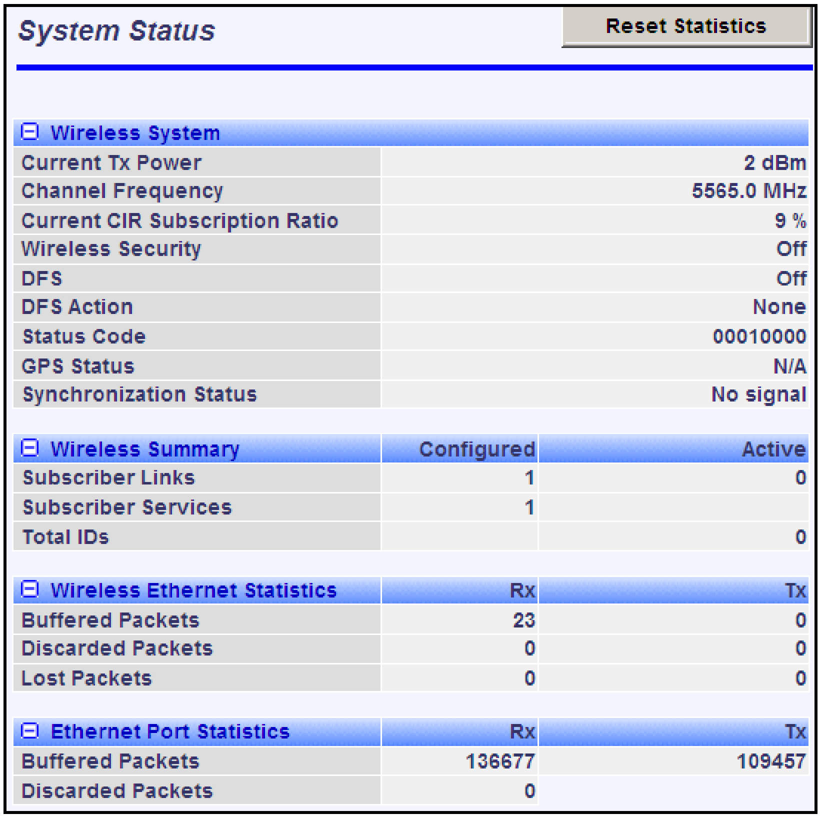
IP Address: Network IP address assigned to this unit.

IP Subnet Mask: Network IP subnet mask assigned to this unit.

Default Gateway Address: Network IP address of the default router or gateway.

4.4.2 System Status

Click **System Status** in the main menu to view information about the wireless interface and Ethernet port. Click ⊞ to expand fields and ⊟ to hide fields.



⊟ Wireless System	
Current Tx Power	2 dBm
Channel Frequency	5565.0 MHz
Current CIR Subscription Ratio	9 %
Wireless Security	Off
DFS	Off
DFS Action	None
Status Code	00010000
GPS Status	N/A
Synchronization Status	No signal

⊟ Wireless Summary	Configured	Active
Subscriber Links	1	0
Subscriber Services	1	
Total IDs		0

⊟ Wireless Ethernet Statistics	Rx	Tx
Buffered Packets	23	0
Discarded Packets	0	0
Lost Packets	0	0

⊟ Ethernet Port Statistics	Rx	Tx
Buffered Packets	136677	109457
Discarded Packets	0	

Fig. 28: **Web - SC System Status Screen**

Wireless System

Current Tx Power: Current transmit power level.

Channel Frequency: RF channel in-use.

Current CIR Subscription Ratio: (SC only) Traffic loading is determined by comparing the available bandwidth to the committed bandwidth:

<100%: Current scheduling commitments can be achieved under the present operating conditions (e.g., surplus bandwidth is available).

>100%: The unit is oversubscribed (aggregate of CIR requests exceeds available bandwidth).

Wireless Security: Status of the wireless security selection.

Off - No wireless security.

On - Data sent over the wireless interface is encrypted.

DFS: Status of the DFS function.

Off: The DFS function is disabled.

On: DFS function is activated. See DFS Action below.

DFS Action: The avoidance action to be taken when radar signals are detected. All DFS actions are recorded in the event log.

None: The DFS feature is disabled.

Tx Off: Radio transmitter is disabled for 30 minutes.

Chg Freq: Radio transmitter is changed to a different RF frequency.

Status Code: Code indicating the status of the RDL-3000 system. Code '0000 0000' indicates normal operation. Refer to the troubleshooting section of this manual.

GPS Status: Display the status of the internal GPS unit.

N/A: The GPS device is not installed (or is malfunctioning).

No Signal: There is no signal detected on the PPS port.

Locked: The RDL-3000 internal clock is synchronized to the PPS signal.

Synchronization Status: Display the synchronization status.

N/A: This message is displayed for the following conditions:

a) Synchronization mode is disabled.

b) Synchronization mode is enabled and PPS port is disabled.

No Signal: There is no signal on the PPS port.

Acquiring: A PPS signal is detected and the internal clock is being synchronized.

Locked: The internal clock is synchronized to the PPS signal.

Wireless Summary

Subscriber Links: Status of the wireless links to subscribers.

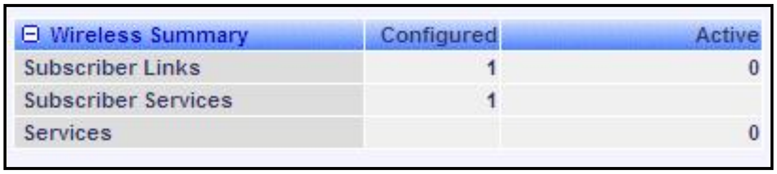
Configured: Number of provisioned Subscriber Links (subscriber will always indicate a value of 1).

Active: Number of subscribers that are online (registered with sector controller).

Subscriber Services: (Subscriber only) Status of the Services for this subscriber.

Configured: Number of provisioned Services.

Active: N/A



⊟ Wireless Summary	Configured	Active
Subscriber Links	1	0
Subscriber Services	1	
Services		0

Fig. 29: **Web - SS System Status Screen**

Services: (Subscriber only) Status of the Services on this subscriber.

Configured: N/A

Active: Number of active Services.

Wireless Ethernet Statistics

Buffered Packets: Number of packets successfully transmitted and received over the wireless interface, excluding discarded packets and packets with errors.

Rx: Wireless packets received.

Tx: Wireless packets transmitted.

Discarded Packets: Number of packets discarded by this unit.

Rx: Received wireless packets that have been discarded (e.g., Rx buffer overflow).

Tx: Transmitted wireless packets that have been discarded (e.g., Tx buffer overflow or packets not acknowledged by the remote end unit).

Lost Packets: Total number of packets containing errors.

Rx: Received wireless packets with errors (e.g., CRC).

Tx: Transmitted wireless packets with errors (reported by remote end unit).

Ethernet Port Statistics

Buffered Packets: Ingress and egress packets processed through the Ethernet port. Total does not include discarded or errored packets.

Rx: Number of packets received on the Ethernet port.

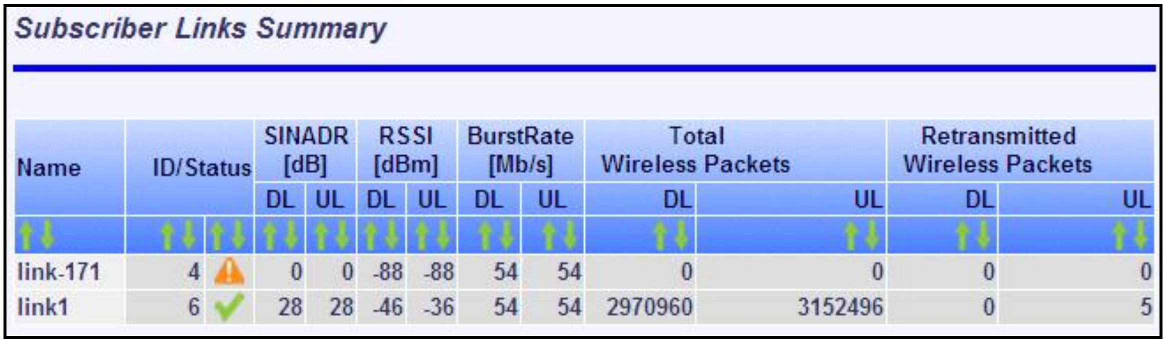
Tx: Number of packets transmitted on the Ethernet port.

Discarded Packets: Total number of discarded Ethernet packets.

Rx: Received packets discarded due to errors (e.g., CRC or buffer overflow).

4.4.3 Subscriber Links Summary (Sector Controller Only)

Click **Links Summary** in the main menu (SC) to view the status of all wireless links. This screen is available only on subscriber units.



Subscriber Links Summary

Name	ID/Status		SINADR [dB]		RSSI [dBm]		BurstRate [Mb/s]		Total Wireless Packets		Retransmitted Wireless Packets	
			DL	UL	DL	UL	DL	UL	DL	UL	DL	UL
↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓
link-171	4	⚠	0	0	-88	-88	54	54	0	0	0	0
link1	6	✓	28	28	-46	-36	54	54	2970960	3152496	0	5

Fig. 30: **Web - Subscriber Links Summary Screen**

Name: Operator-assigned name for wireless Links and related Services. Click an entry in the Name field (e.g., link-171) to display the Link Configuration screen for that item.

ID/Status: Subscriber Link identifier and status indicator.

ID: A unique identifier (4 to 127) assigned to each subscriber Link. This value is required when using the CLI interface to modify settings.

Status: Status of this link or Service.

✓ The Link/Service is available.

⚠ The Link/Service is unavailable (offline or disabled).

Click the status icon (e.g., ✓) to display the Subscriber Link Status screen.

SINADR [dB]: Ratio of the average RF signal strength to interference, noise, and distortion.

DL: SINADR reported by the remote end unit.

UL: Received signal strength to noise measured by this unit.

RSSI [dBm]: Received signal strength indicator.

DL: RSSI reported by the remote end unit.

UL: Received signal strength measured by this unit.

Burst Rate [Mb/s]: The current uplink and downlink uncoded burst rate for the link.

DL: Current downlink burst rate.

UL: Current uplink burst rate.

Total Wireless Packets: Total packets successfully processed over the wireless interface. Total does not include discarded or errored packets.

DL: Total packets transmitted over the wireless interface.

UL: Total packets received over the wireless interface.

Retransmitted Wireless Packets: Total number of wireless packets that have been retransmitted over the wireless interface.

DL: Total packets retransmitted over the wireless interface.

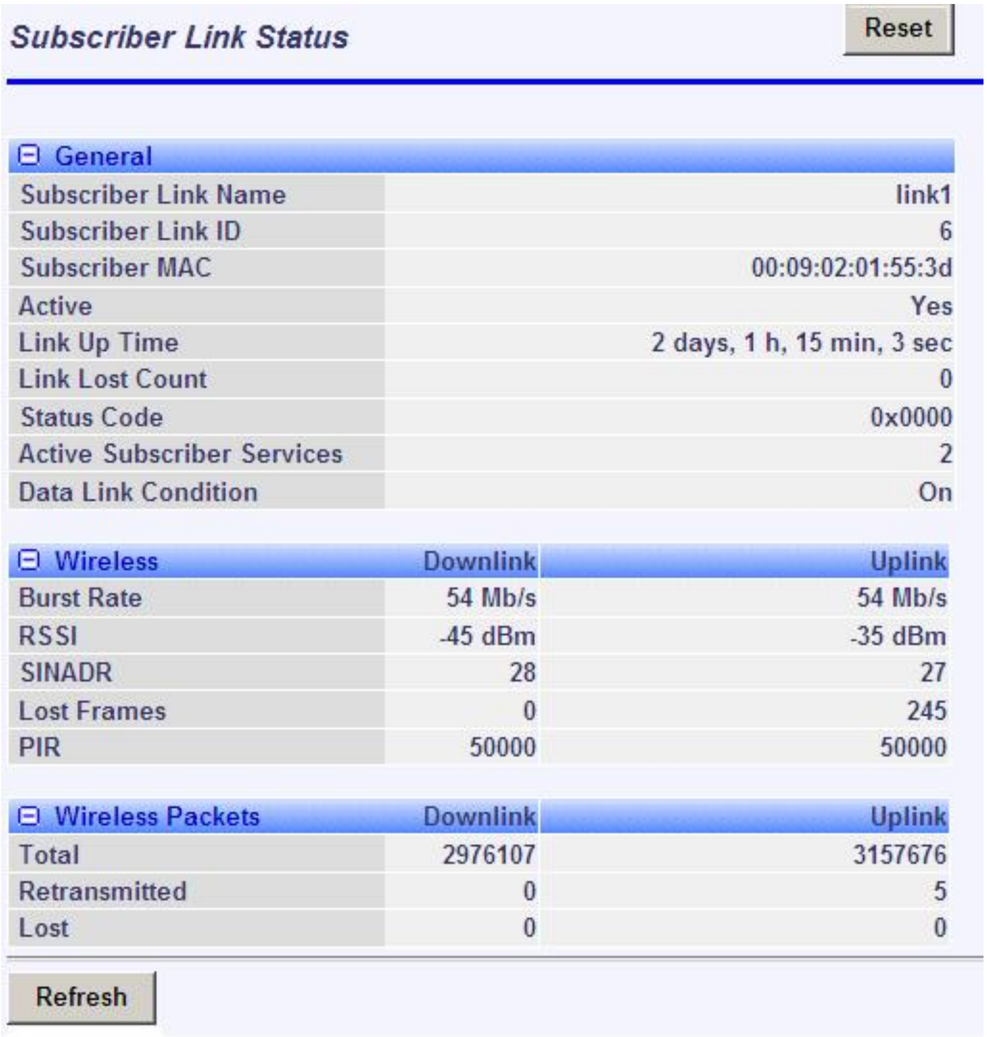
UL: Total packets retransmitted by the remote end.

4.4.4 Subscriber Link Status

Use one of the following selection methods to view the status of a wireless link:

Sector controller: Click **Links Summary** in the main menu and then click on the Link status symbol (e.g.,✓ or ⚠).

Subscriber: Click **Link Status** in the main menu.



Subscriber Link Status

⊟ General	
Subscriber Link Name	link1
Subscriber Link ID	6
Subscriber MAC	00:09:02:01:55:3d
Active	Yes
Link Up Time	2 days, 1 h, 15 min, 3 sec
Link Lost Count	0
Status Code	0x0000
Active Subscriber Services	2
Data Link Condition	On

⊟ Wireless	Downlink	Uplink
Burst Rate	54 Mb/s	54 Mb/s
RSSI	-45 dBm	-35 dBm
SINADR	28	27
Lost Frames	0	245
PIR	50000	50000

⊟ Wireless Packets	Downlink	Uplink
Total	2976107	3157676
Retransmitted	0	5
Lost	0	0

Fig. 31: **Web - Subscriber Link Status Screen**

General

Subscriber Link Name: Name assigned to this unit.

Subscriber Link ID: A unique identifier (4 to 127) assigned to each subscriber Link. This value is required when using the CLI interface to modify settings.

Subscriber MAC: MAC Address of this unit.

Active: Indicates the current status of the wireless link.

- **No**: Wireless link is not active.
- **Yes**: Wireless link is active.

Link Up Time: Total time the wireless link has been operational.

Link Lost Count: Number of times the link has been out of service.

Status Code: Coded indicator for status of this unit. Refer to section 6: Diagnostics & Troubleshooting on page 114. A code of '0x000' indicates normal operation.

Active Subscriber Services: The number of Services active on this link.

Data Link Condition: Indicate the status link:

Off: Wireless link is not active (e.g., subscriber is not registered).

On: Wireless link is active.

Wireless

The following statistics are displayed for the downlink and uplink.

Burst Rate [Mb/s]: The current uplink and downlink uncoded burst rate for the link.

Downlink: Current downlink burst rate.

Uplink: Current uplink burst rate.

RSSI [dBm]: Received signal strength indicator.

Downlink: Downlink RSSI (reported by the remote end unit).

Uplink: Uplink received signal strength (measured by this unit).

SINADR [dB]: Ratio of the average RF signal strength to interference, noise, and distortion.

Downlink: Downlink SINADR (reported by the remote end unit).

Uplink: Uplink received signal strength to noise (measured by this unit).

Lost Frames: Number of frames lost.

PIR: Operator-assigned Peak Information Rate (PIR) for this link.

Downlink: **Operator-assigned downlink Peak Information Rate (PIR) for this link.**

Uplink: **Operator-assigned uplink Peak Information Rate (PIR) for this link**.

Wireless Packets

Summary of wireless packet activity on the downlink and uplink.

Total: Total number of packets processed over the wireless interface. Total does not include discarded and errored packets.

Retransmitted: Total number of wireless packets retransmitted over the wireless interface.

Lost: Total number of wireless packets discarded by this unit due to errors.

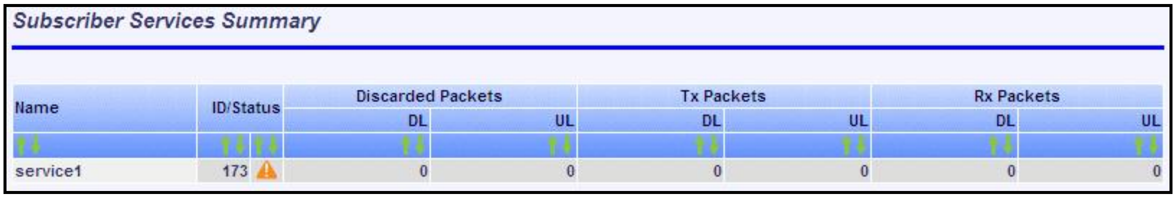
Controls

Refresh: Click to update displayed statistics counters.

Reset: Click to reset displayed statistics counters.

4.4.5 Subscriber Services Summary (Subscriber Only)

Click **Services Summary** in the main menu (SS) to view the status of all Services on this subscriber. This screen is available only on the subscriber unit.



Subscriber Services Summary

Name	ID/Status	Discarded Packets		Tx Packets		Rx Packets	
		DL	UL	DL	UL	DL	UL
service1	173 ⚠	0	0	0	0	0	0

Fig. 32: **Web - Services Summary Screen**

Name: Name assigned to this Service.

ID/Status: Service ID number and status indicator.

ID: A unique identifier (160 to 511) assigned to each Service. This value is required when using the CLI interface to modify settings.

Status: Status of this Link or Service:

✓ Link or Service is available.

⚠ Link or Service is unavailable (offline or disabled).

Click the status icon (e.g., ✓) to display the Subscriber Service Status screen.

Discarded Packets: Total number of packets discarded by this unit due to errors.

UL: Received wireless packets that have been discarded.

DL: Transmitted wireless packets discarded by the sector controller.

Tx Packets: Total number of packets successfully transmitted over the wireless interface. Total does not include discarded packets or packets with errors.

DL: Number of packets the sector controller has transmitted to this subscriber.

UL: Number of packets the subscriber has transmitted to the sector controller.

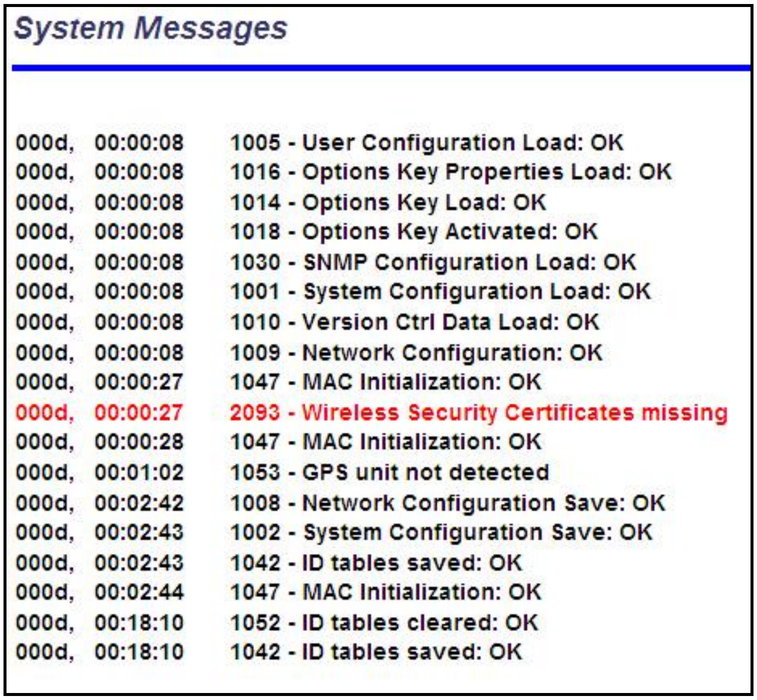
Rx Packets: Total packets successfully received over the wireless interface. Total does not include discarded or errored packets.

DL: Number of packets received from the sector controller.

UL: Number of packets the sector controller has received from this subscriber.

4.4.6 System Messages (Log)

Click **System Log** in the main menu to view the system event messages recorded by the RDL-3000.



System Messages

```
000d,  00:00:08    1005 - User Configuration Load: OK
000d,  00:00:08    1016 - Options Key Properties Load: OK
000d,  00:00:08    1014 - Options Key Load: OK
000d,  00:00:08    1018 - Options Key Activated: OK
000d,  00:00:08    1030 - SNMP Configuration Load: OK
000d,  00:00:08    1001 - System Configuration Load: OK
000d,  00:00:08    1010 - Version Ctrl Data Load: OK
000d,  00:00:08    1009 - Network Configuration: OK
000d,  00:00:27    1047 - MAC Initialization: OK
000d,  00:00:27    2093 - Wireless Security Certificates missing
000d,  00:00:28    1047 - MAC Initialization: OK
000d,  00:01:02    1053 - GPS unit not detected
000d,  00:02:42    1008 - Network Configuration Save: OK
000d,  00:02:43    1002 - System Configuration Save: OK
000d,  00:02:43    1042 - ID tables saved: OK
000d,  00:02:44    1047 - MAC Initialization: OK
000d,  00:18:10    1052 - ID tables cleared: OK
000d,  00:18:10    1042 - ID tables saved: OK
```

Fig. 33: **Web - Example of System Event Messages**

Clear Log: Click to remove all messages from the system log file.

Event Messages

The following table provides a brief description of the key system messages.

Table 6: Web - System Log Messages

Event ID	Event Description
1001	System Configuration Load: OK
1002	System Configuration Save: OK
1003	EEPROM Directory Load: OK
1004	EEPROM Directory Save: OK
1005	User Configuration Load: OK
1006	User Configuration Save: OK
1007	Network Configuration Load: OK
1008	Network Configuration Save: OK
1009	Network Configuration: OK
1010	Version Ctrl Data Load: OK
1011	Version Ctrl Data Save: OK
1012	System Description Load: OK
1013	System Description Save: OK
1014	Options Key Load: OK
1015	Options Key Save: OK
1016	Options Key Properties Load: OK
1017	Options Key Properties Save: OK
1018	Options Key Activated: OK
1019	Data server started: OK
1021	Upgrade: OK
1023	Firmware configuration: OK

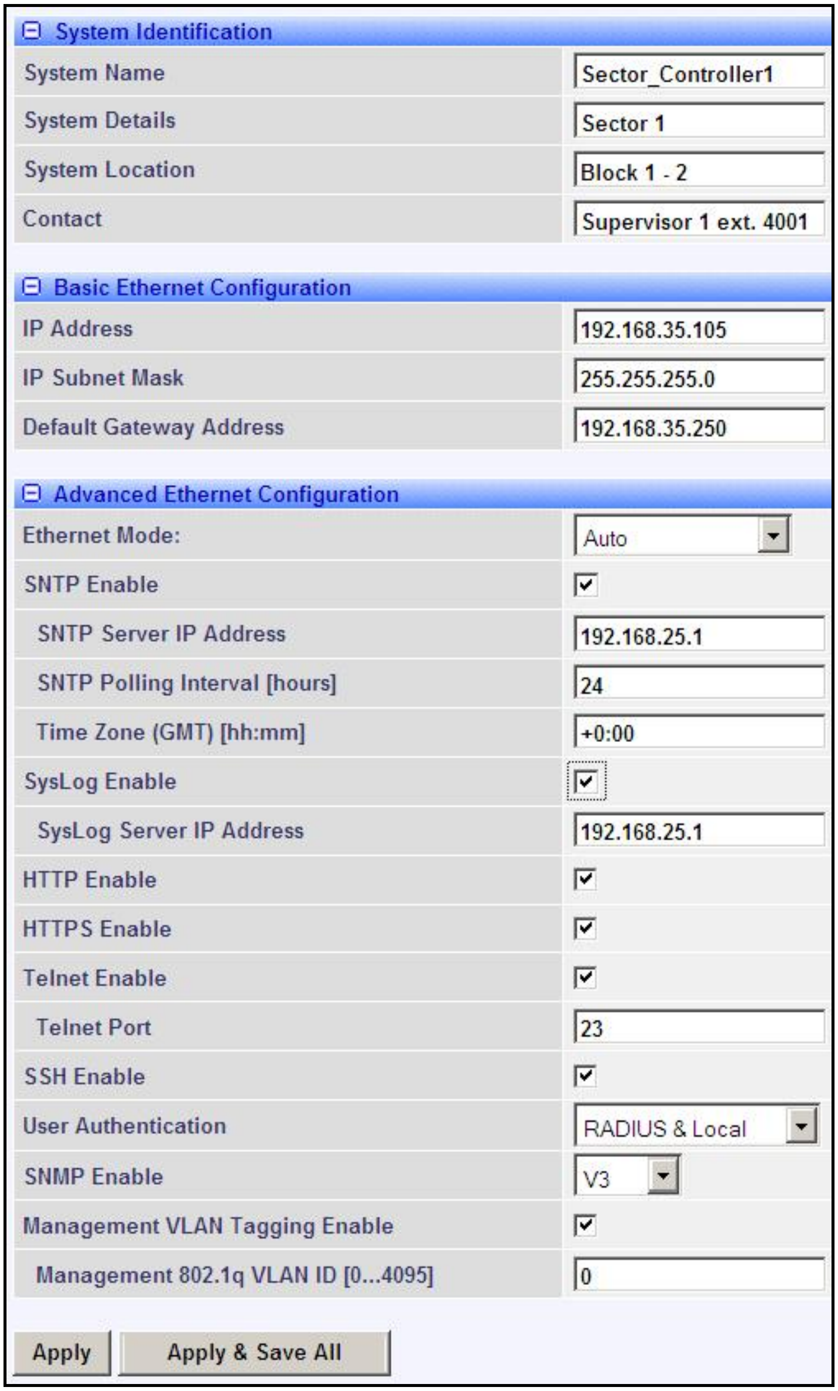
Table 6: Web - System Log Messages	
Event ID	**Event Description**
1026	Factory Data Save: OK
1029	HTTP(User Mgm): Chg User Attributes: OK
1030	SNMP Configuration Load: OK
1031	SNMP Configuration Save: OK
1032	SNTP: Time received: OK
1033	DFS: Event Detected
1033	MAC Initialization: OK
1034	DFS: Event Detected
1035	ID deleted: OK
1036	Restart freq scan (RSSI)
1037	Restart freq scan (TimeOut)
1038	Reg Req (step 1)
1039	Reg Req (step 2
1040	Reg Req (step 2)
1041	Restart freq scan (act links)
1042	ID tables saved: OK
1043	ID defined: OK
1044	ID tables not changed: OK
1045	ID modified: OK
1046	RF frequency validation: OK
2001	System Configuration Load: Error
2002	System Configuration Save: Error
2003	EEPROM Directory Load: Error
2004	EEPROM Directory Save: Error
2005	User Configuration Load: Error
2006	User Configuration Save: Error
2007	Network Configuration Load: Error
2008	Network Configuration Save: Error
2009	Network Configuration: Error
2010	Version Ctrl Data Load: Error
2011	Version Ctrl Data Save: Error
2012	System Description Load: Error
2013	System Description Save: Error
2014	Options Key Load: Error
2015	Options Key Save: Error
2016	Options Key Properties Load: Error
2017	Options Key Properties Save: Error
2018	Options Key Activated: Error
2019	No Options Key
2020	Fail to start the data server
2021	Data server
2022	Data server
2023	Upgrade client start: Error
2024	Upgrade in progress
2025	Upgrade: FAIL
2026	Upgrade: Error
2028	Factory Data Corrupted (use fallback values)
2028	TFTP: Error
2029	Firmware configuration: Error
2031	Factory Data Save: Error
2034	HTTP(User Mgm): Invalid password
2035	HTTP(User Mgm): Invalid User
2036	HTTP(User Mgm): Chg User Attributes: Error

Table 6: Web - System Log Messages	
Event ID	**Event Description**
2037	SNMP Configuration Load: Error
2038	SNMP Configuration Save: Error
2039	Invalid Options Key
2039	SNTP: Time received: Error
2040	MAC Initialization: Error
2041	MAC Busy
2042	ID database corrupted
2043	Invalid ID
2044	Max. ID number reached
2045	Int Procs programming: Error
2046	Int Procs start: Error
2047	ID action not possible
2048	ID validation: Error
2049	HW validation: Error
2050	FTP: Error
2051	WS: Timeout (WS_SEND_SESSION_REQ)
2063	SSH RSA KEY missing, using default key
2064	SSH DSA KEY missing, using default key
2065	SSL Certificate missing, using default one
2066	SSL KEY missing, using default one
2070	Pre Shared Key ERROR
2071	Authentication Packet Validation ERROR
2072	Encryption Key Validation ERROR
2073	Signature Validation ERROR
2074	Certificate Validation ERROR
2075	RNG self test ERROR
2076	DSA pair wise test failed
2077	RNG self test failed
2078	TDES self test failed
2079	AES self test failed
2080	SHA self test failed
2081	HMAC self test failed
2082	RSA self test failed
2083	DES self test failed
2084	MAC AES self test failed
2086	Upgrade image validation: ERROR
2087	Upgrade ERROR: image save
2088	SSH RSA KEY missing, using generated key
2089	SSH DSA KEY missing, using generated key
2090	Test not executed when FIPS mode changed
2091	The options key expires in less than 6 days
2092	SSL Certificate missing, HTTPS disabled
2093	Wireless Security Certificates missing
2094	Firmware validation: ERROR (%s)
2095	Image validation: ERROR
2099	Unknown Message

4.5 Configuration Screens

4.5.1 System Screen

Click **Configuration-> System** in the main menu to view and adjust the system identification and Ethernet settings. Click ⊞ to expand or ⊟ to hide fields.



⊟ System Identification

System Name	Sector_Controller1
System Details	Sector 1
System Location	Block 1 - 2
Contact	Supervisor 1 ext. 4001

⊟ Basic Ethernet Configuration

IP Address	192.168.35.105
IP Subnet Mask	255.255.255.0
Default Gateway Address	192.168.35.250

⊟ Advanced Ethernet Configuration

Ethernet Mode:	Auto
SNTP Enable	☑
SNTP Server IP Address	192.168.25.1
SNTP Polling Interval [hours]	24
Time Zone (GMT) [hh:mm]	+0:00
SysLog Enable	☑
SysLog Server IP Address	192.168.25.1
HTTP Enable	☑
HTTPS Enable	☑
Telnet Enable	☑
Telnet Port	23
SSH Enable	☑
User Authentication	RADIUS & Local
SNMP Enable	V3
Management VLAN Tagging Enable	☑
Management 802.1q VLAN ID [0...4095]	0

Fig. 34: **Web - Config - PMP SC System Configuration Screen**

System Identification

System Name: Enter the name for this unit. The system name may be up to thirty alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

System Details: Enter descriptive details about this unit. The system details may be up to thirty alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

System Location: Enter descriptive details about the location of this unit. The system location information may be up to thirty alphanumeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

Contact: Enter descriptive details about the operational/technical contact for this unit. The contact information may be up to thirty alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

Basic Ethernet Configuration

IP Address: Enter the IP address for this unit. The IP address is routable through the Ethernet port and over the wireless interface.

IP Subnet Mask: Enter the IP subnet mask.

Default Gateway Address: Enter the IP address of the default gateway or router on the Ethernet segment connected to the RDL-3000 Ethernet port.

Advanced Ethernet Configuration

Ethernet Mode: Select the operating mode of the Ethernet port.

Auto - Automatically negotiate the connection speed and duplex. This selection does <u>not</u> detect the speed and duplex of external Ethernet equipment operating at a fixed speed and duplex. The 'Auto' selection will operate successfully only when the RDL-3000 and the connected Ethernet device are <u>both</u> set to auto-negotiate.

10Mbps HD - Operate at 10Base-T half-duplex only.

10Mbps FD - Operate at 10Base-T full duplex only.

100Mbps HD -.Operate at 100Base-T half-duplex only.

100Mbps FD - Operate at 100Base-T full duplex only.

Important: Incorrect duplex settings may cause complete loss of communications on the RDL-3000 Ethernet port. It is recommended to set the Ethernet ports to operate at a fixed speed of 100Base-T/Full Duplex.

SNTP Enable: Check this box ☑ to enable the SNTP protocol support. This feature allows RDL-3000 systems to time-stamp system event messages using a network time server. When enabled, you must enter the network address of the SNTP server in the SNTP Server IP Address field.

When SNTP is enabled, the following additional configuration fields are visible:

SNTP Server IP Address: Enter the network IP address of the SNTP server.

SNTP Polling Interval [hours]: Enter the SNTP polling interval (hours).

Time Zone (GMT) [hh:mm]: Enter the offset (hours) from GMT for this time zone.

Syslog Enable: Check this box ☑ to enable saving event messages on a remote server.

When Syslog Enable is selected, the following additional configuration fields are visible:

Syslog Server IP Address: Enter the network address of the Syslog server.

HTTP Enable: Check this box ☑ to enable the HTTP (Web) interface.

HTTPS Enable: Check this box to enable HTTPS operation (secure/encrypted Web session). Refer to page 121 for a complete description of this feature.

Telnet Enable: Check this box ☑ to enable the Telnet interface (CLI).

When Telnet is enabled, the following additional configuration field is visible:

Telnet Port: Enter Telnet port address (reboot required).

SSH Enable: Check this box to enable SSH operation (secure/encrypted CLI). Refer to page 121 for a complete description of this feature.

User Authentication: The RDL-3000 supports a local authorization policy and secure centralized authentication management using a RADIUS server. At least one policy is always enabled, and both may be enabled to operate together.

The RDL-3000 can be configured for the following authentication modes:

Local Only: User name and password authentication is managed exclusively by the RDL-3000.

RADIUS Only: User name and password authentication is managed exclusively by a RADIUS server. Feature also supports a redundant RADIUS server.

Local + RADIUS: Local and RADIUS methods of user authentication are enforced.

Notes:

1. When **RADIUS Only** or **Local + RADIUS** is selected, click on the main menu item RADIUS to display the RADIUS Configuration screen.
2. *Note: Authorization data is retrieved from the RADIUS server at 10-minute intervals. For example, if a user's authorization is changed on the RADIUS server, it may require up to ten minutes before the RDL-3000 is updated with the new information.*

SNMP Enable: Select the version of Simple Network Management Protocol (SNMP). The SNMP protocol allows an application to poll a device for information and change data stored in the RDL-3000 Management Information Base (MIB).

none: SNMP is disabled.

v2: Supports SNMP v1 and v2c commands.

v3: Supports SNMP v3 exclusively. SNMP v1 and SNMP v2c commands not accepted and an authorization policy is enforced.

Click on the main menu item Configuration->System->SNMP to display the SNMP Configuration screen.

Management VLAN Tagging Enable: Control the VLAN tagged management function.

Disabled (□): There are no restrictions for management traffic.

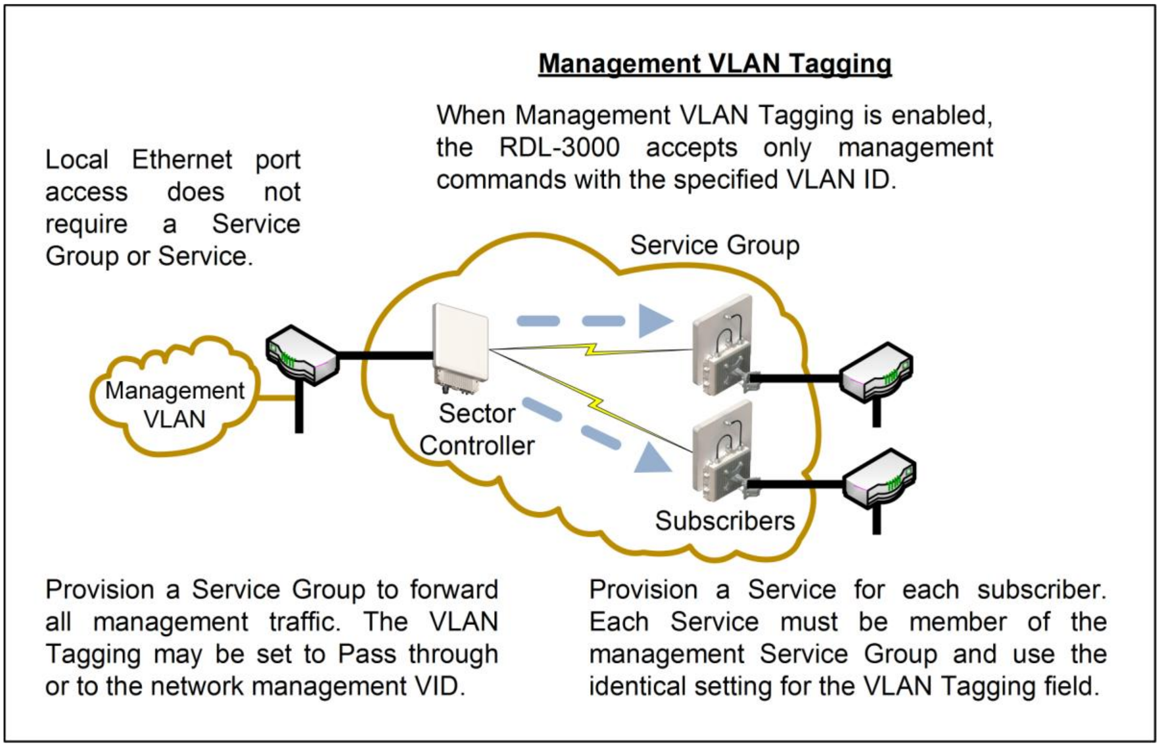
Enabled (☑): This unit can be managed only using VLAN traffic tagged with the value specified in the **Mgmt. VID** field.

On all PMP systems, over-the-air management is possible only after creating a Service Group for device management and adding a Service for each subscriber. For initial installation and setup, it is recommended to use Pass Through settings for this group and member Service for each subscriber. Set CIR and priority values to ensure management traffic has sufficient priority and bandwidth available.

When Management VLAN Tagging is enabled, the following field is visible:

Management 802.1Q VLAN ID [0...4095]: Enter the management VLAN ID. When Management VLAN Tagging Enable is selected, the system recognizes only management commands where the Ethernet packet has the matching VLAN ID.

Important*:* For initial installation and setup, it is recommended to use 'Pass through' mode for the management Service Group and member Services. Connectivity issues with VLAN services may cause the RDL-3000 management function to be unreachable and require a site visit and/or long reset operation to recover control of the unit.



Management VLAN Tagging

When Management VLAN Tagging is enabled, the RDL-3000 accepts only management commands with the specified VLAN ID.

Local Ethernet port access does not require a Service Group or Service.

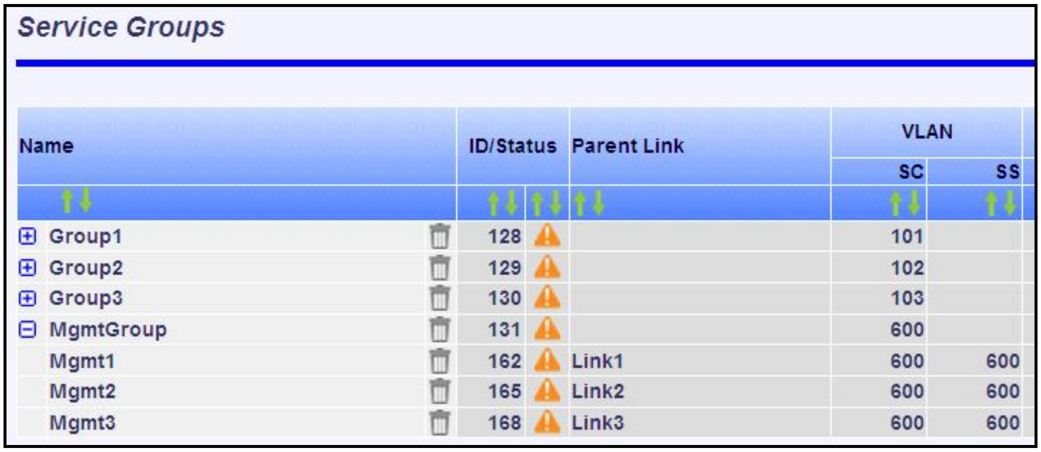
Provision a Service Group to forward all management traffic. The VLAN Tagging may be set to Pass through or to the network management VID.

Provision a Service for each subscriber. Each Service must be member of the management Service Group and use the identical setting for the VLAN Tagging field.

Fig. 35: Web - VLAN Tagged Management

Example

In the following example, the network management VLAN ID=600. Identical settings are used on the Service Group and each subscriber Service. Click ⊞ to display the Services associated with each Service Group.



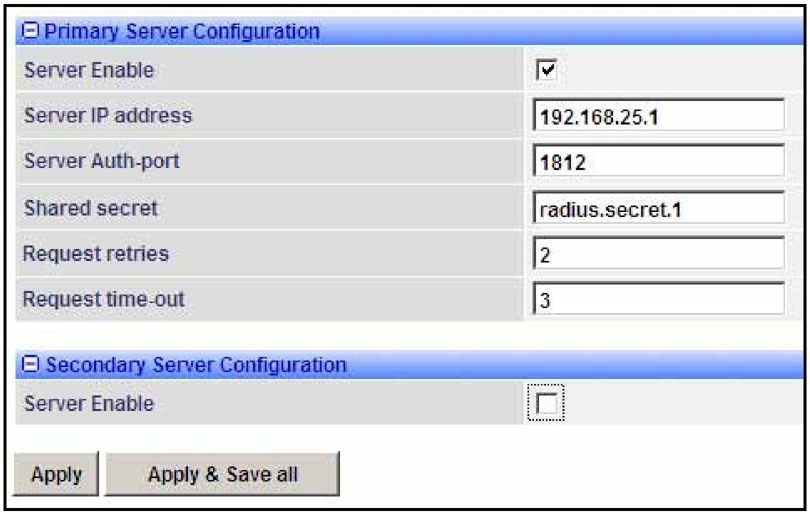
Service Groups

Name	ID/Status		Parent Link	VLAN	
				SC	SS
⊞ Group1	128	⚠		101	
⊞ Group2	129	⚠		102	
⊞ Group3	130	⚠		103	
⊟ MgmtGroup	131	⚠		600	
Mgmt1	162	⚠	Link1	600	600
Mgmt2	165	⚠	Link2	600	600
Mgmt3	168	⚠	Link3	600	600

Fig. 36: Web - VLAN Tagged Management Example

4.5.2 RADIUS Setup

When **Radius** or **Local + RADIUS** is checked ☑, click Configuration->System->RADIUS in the main menu to display the RADIUS Configuration screen. Click ⊞ to expand or ⊟ to hide fields.



⊟ Primary Server Configuration

Server Enable	☑
Server IP address	192.168.25.1
Server Auth-port	1812
Shared secret	radius.secret.1
Request retries	2
Request time-out	3

⊟ Secondary Server Configuration

Server Enable	□

Fig. 37: Web - RADIUS Configuration Screen

The following fields are provided for configuring the RADIUS server:

Server Enable: Control the RADIUS server mode.

Disabled (□):.Do not use the RADIUS server for user authentication. This unit will use only local user authentication (Utilities->User Management).

Enabled (☑): Use the RADIUS server for user authentication.

Server IP Address: RADIUS server IP address.

Server Auth-port: Listening port address on RADIUS server (default port is 1812).

Shared secret: Password for RADIUS server. The password must conform to the security policy (refer to section 4.7.2: Users Management on page 85).

Request retries: Maximum number for attempts to contact the RADIUS server.

Request time-out: Time to wait for response from the RADIUS server (seconds).

Note:

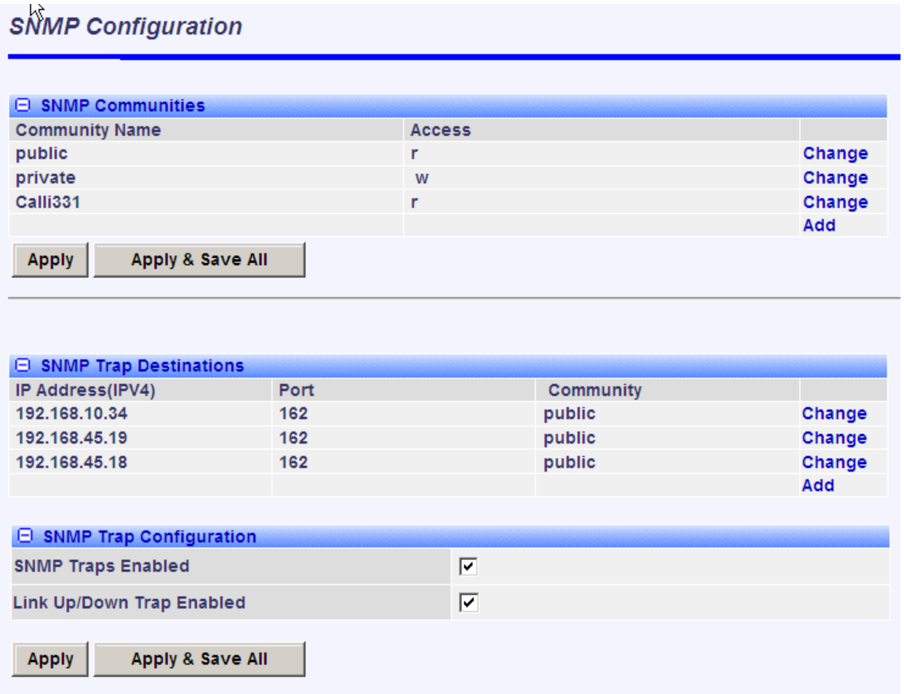
1. When using FreeRadius server, the following files on the server platform must be modified. See the RADIUS documentation for additional operating details.

Table 7: Web - Required FreeRadius Files

Define a client.	clients.conf	client 192.168.0.0/16 {secret = secret shortname = RDL3000 }
Add admin account	users.conf	admuser Auth-Type := Local, User-Password == "abc" Service-Type = Administrative-User
Add user account	users.conf	usrjoe: Auth-Type := Local, User-Password == "pass" Service-Type = NAS-Prompt-User
Reject an account.	users.conf	lameuser: Auth-Type := Reject Reply-Message = "Account has been disabled."

4.5.3 SNMP Configuration

Click Configuration->System->SNMP in the main menu to display the SNMP Configuration screen. Use this screen to view and modify all SNMP related parameters. Click ⊞ to expand or ⊟ to hide fields.



SNMP Configuration

⊟ SNMP Communities

Community Name	Access	
public	r	Change
private	w	Change
Calli331	r	Change
		Add

⊟ SNMP Trap Destinations

IP Address(IPV4)	Port	Community	
192.168.10.34	162	public	Change
192.168.45.19	162	public	Change
192.168.45.18	162	public	Change
			Add

⊟ SNMP Trap Configuration

SNMP Traps Enabled	☑
Link Up/Down Trap Enabled	☑

Fig. 38: **Web - SNMP Configuration Screen**

SNMP Community Settings

The RDL-3000 supports up to eight separate community strings. Each community string is assigned specific access rights (read/write). The 'public' and 'private' community strings are default access values and should be changed to ensure secure access.

Community Name: Name assigned to this SNMP community string.

Access: Access permissions for this entry.

> **None**: External SNMP client using this string can not read or modfy any fields. Read and write requests will be refused.
>
> **Read**: External SNMP client using this string can only read data. Write requests will be refused.
>
> **Write**: External SNMP client using this string can only write data. Read requests will be refused.
>
> **Read&Write**: External SNMP client using this string can read and write data.

Change: Click to modify this SNMP community string entry.

Add: Click to add a new SNMP community string entry (maximum eight).

Apply: Click to activate the SNMP Community settings displayed on this screen.

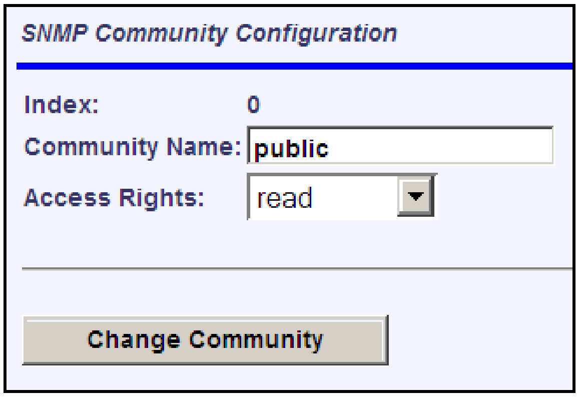
Apply & Save All: Click to activate and permanently save the SNMP Community settings on this screen. Saved settings are restored on power-up, reboot, or at the end of a test cycle.

Note: To remove a community string, click 'change' beside that entry, delete the community string (Community name' field), and click the Change Community button.

Note: Clicking on another main menu item before clicking Apply or Apply & Save All will discard any changes made to settings displayed on the current screen.

Edit SNMP Community Settings

Click Change or Add in the **SNMP Communities** section of the screen to modify existing community strings or add a new community string.



SNMP Community Configuration

Index: 0

Community Name: public

Access Rights: read

Fig. 39: **Web - SNMP Community Configuration Screen**

Index: Display the index reference number for this entry. This value is required when using the CLI interface to modify SNMP Community settings.

Community Name: Enter or modify the SNMP community name for this entry.

Access Rights: Select the access permissions for this entry.

None: Deny read and write permission for this entry.

Read: Grant read access permission only for this entry. Deny write permission.

Write: Grant write access permission only for this entry. Deny read permission.

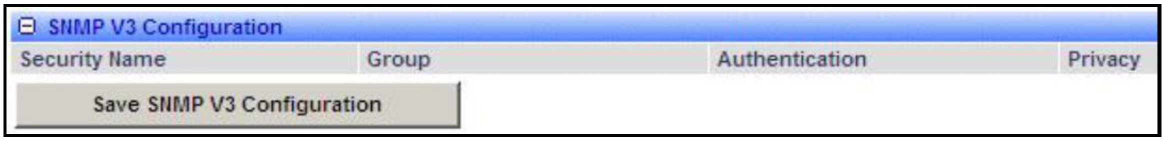
Read&Write: Grant read and write access permission for this entry.

Change Community: Click to accept changes and close this dialog.

> ***Important**: Clicking Update Configuration does <u>not</u> activate changes. In the SNMP Configuration screen, click Apply to activate changes or click Apply & Save to activate and permanently save changes.*

SNMP v3 Security Settings

SNMP v3 supports authentication and privacy settings to provide secure management access. Security methods are associated with RDL-3000 user accounts.



⊟ SNMP V3 Configuration

Security Name	Group	Authentication	Privacy

Fig. 40: **Web - SNMP V3 Configuration**

Security Name: User name of the SNMP v3 account.

Group: Group association for the SNMP v3 account.

Authentication: Authorization method for the SNMP v3 account.

MD5: MD5 (Message-Digest algorithm 5) is a cryptographic hash function with a 128-bit hash value (RFC 1321).

SHA: SHA (secure Hash Algorithm) is a set of cryptographic hash functions.

Privacy: Privacy method for this account.

None: No encryption.

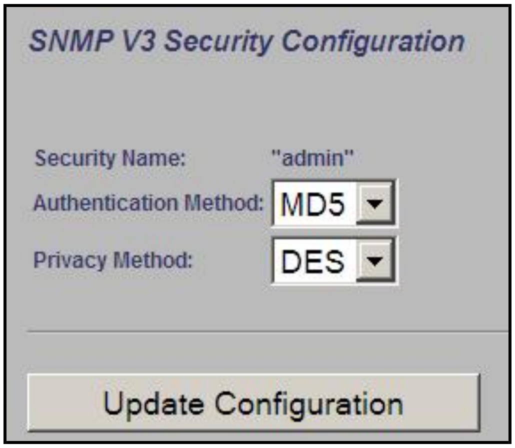
DES: DES (Data Encryption Standard) is an encryption standard.

AES: AES (Advanced Encryption Standard) is an encryption standard.

Save SNMP v3 Configuration: Click to activate the displayed settings.

Edit SNMP v3 Security

Click Change or Add in the SNMP community section of the screen to modify the associated SNMP v3 security settings. The following popup dialog is displayed:



SNMP V3 Security Configuration

Security Name: "admin"

Authentication Method: MD5

Privacy Method: DES

Fig. 41: **Web - SNMP v3 Configuration Dialog**

Security Name: name of the selected account to use for SNMP v3 requests.

Authentication Method: Select the access permissions for this entry.

MD5: MD5 (Message-Digest algorithm 5) is a cryptographic hash function with a 128-bit hash value (RFC 1321).

SHA: SHA (secure Hash Algorithm) is a set of cryptographic hash functions.

Privacy Method: Select the access permissions for this entry.

None: No encryption.

DES: DES (Data Encryption Standard) is an encryption standard.

AES: AES (Advanced Encryption Standard) is an encryption standard.

Update Configuration: Click to accept changes and close this dialog.

> ***Important***: *Clicking Update Configuration does not activate changes. In the SNMP Configuration screen click Apply to activate changes or click Apply & Save to activate and permanently save changes.*

SNMP Trap Destination Settings

This section of the SNMP Configuration screen displays the SNMP trap destination settings. The SNMP trap messages inform network management devices of changes to the RDL-3000 status.

IP Address (IPv4): IP address of this trap listener. A copy of each SNMP trap message is transmitted to this address.

Port: Destination port address of this trap listener.

Community String: (SNMP v2) Community string associated with this trap listener.

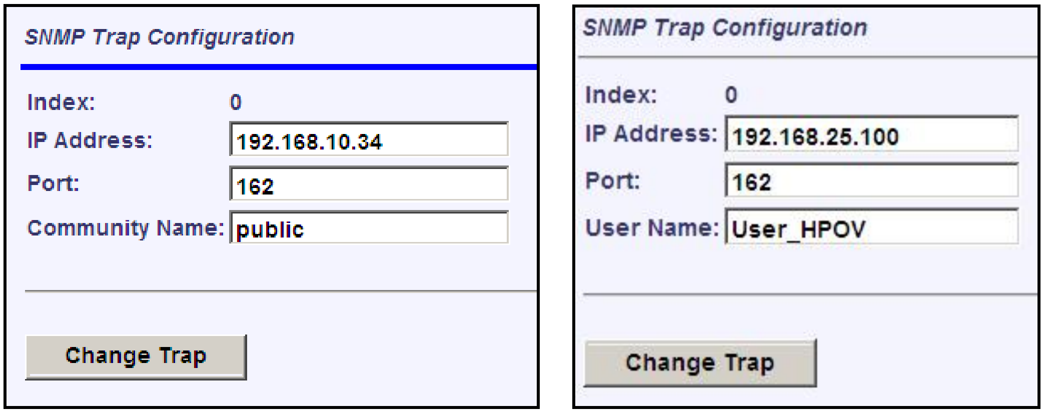
User Name: (SNMP v3) User account associated with this trap listener.

Change: Click Change to modify the existing SNMP community string.

Add: Click to create a new SNMP community string (up to eight community strings).

Edit SNMP Trap Destinations

Click Change or Add in the SNMP Trap Destinations section of the screen to modify the list of trap listeners. The following popup dialog is displayed:



SNMP Trap Configuration

Index: 0

IP Address: 192.168.10.34

Port: 162

Community Name: public

SNMP Trap Configuration

Index: 0

IP Address: 192.168.25.100

Port: 162

User Name: User_HPOV

Fig. 42: **Web - SNMP Trap Configuration Screen (V2/V3)**

Index: Display the unique reference number for this entry. This value is required when using the CLI interface to modify SNMP trap settings.

IP Address: Enter the IP address (IPv4) associated with this SNMP trap alarm.

Port: Enter the destination port address associated with this SNMP trap alarm.

Community Name: (v2) Enter the community name associated with this trap destination.

User Name: (v3) Enter the user account associated with this trap destination.

Change Trap: Click to accept changes and close this dialog.

***Important**: Clicking Change Trap does <u>not</u> activate changes. In the SNMP Configuration screen click Apply to activate changes or click Apply & Save to activate and permanently save changes.*

SNMP Trap Settings

SNMP Traps Enabled: Control the SNMP trap message function.

Disabled (□): The RDL-3000 does not send SNMP trap messages.

Enabled (☑): The RDL-3000 sends SNMP trap messages.

Link Up/Down Trap Enabled: Control SNMP trap messages for the link status.

Disabled (□): The RDL-3000 does not send SNMP trap messages based on changes to the wireless link status.

Enabled (☑): A trap message is sent for each change to the wireless link status.

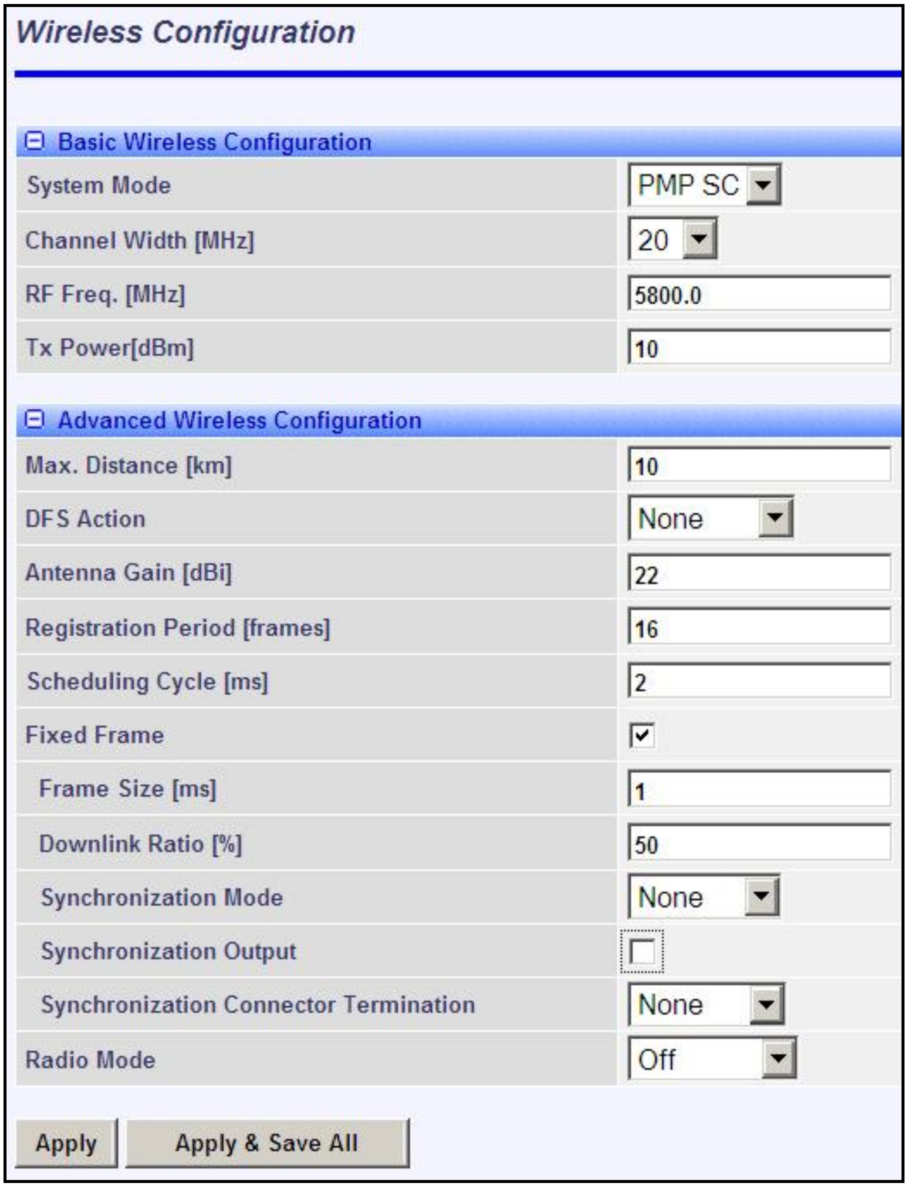
Apply: Click to activate the displayed SNMP Trap Destinations and SNMP Trap Configuration settings.

Apply & Save All: Click to activate and permanently save the SNMP Trap Destinations and SNMP Trap Configuration settings displayed on this screen. Saved settings are restored on power-up, reboot, or at the end of a test cycle.

Note: Clicking on another main menu item before clicking Apply or Apply & Save All will discard any changes made to settings displayed on the current screen.

4.5.4 Wireless Configuration

Use these settings to configure the RDL-3000 wireless interface. Some parameters are supported only by the sector controller or the subscriber. This screen is different on the sector controller and subscriber unit. Click ⊞ to expand or ⊟ to hide fields.



Wireless Configuration

⊟ Basic Wireless Configuration

System Mode	PMP SC
Channel Width [MHz]	20
RF Freq. [MHz]	5800.0
Tx Power[dBm]	10

⊟ Advanced Wireless Configuration

Max. Distance [km]	10
DFS Action	None
Antenna Gain [dBi]	22
Registration Period [frames]	16
Scheduling Cycle [ms]	2
Fixed Frame	☑
Frame Size [ms]	1
Downlink Ratio [%]	50
Synchronization Mode	None
Synchronization Output	□
Synchronization Connector Termination	None
Radio Mode	Off

Fig. 43: Web - Wireless Configuration Screen -- Sector Controller

Basic Wireless Configuration

System Mode: One unit must be configured as a sector controller to control the bi-directional data link with remote subscribers.

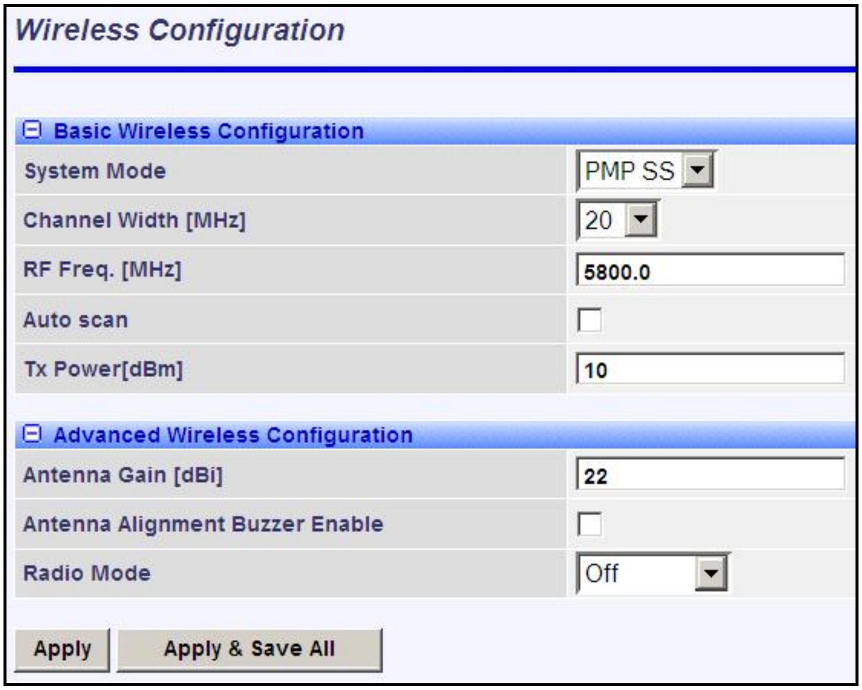
> **PMP SC**: This unit is configured as a sector controller. The unit automatically begins transmitting poll messages to locate and register remote subscribers.
>
> **PMP SS**: This unit is configured to operate as a subscriber. The unit monitors the selected RF channel(s) for poll poll messages from a sector controller.

Channel Width [MHz]: Select the channel bandwidth. The options key controls channel availability.

RF Freq. [MHz]: Enter the center frequency for the RF channel.

RF frequency range settings are restricted by the active options key.

> ***Important***: *To minimize interference between RDL-3000 links operating in close proximity, RF frequency settings should be separated by a guard interval equal or greater than the channel size. For example, when using a 20 MHz channel, the RF frequencies should be separated by >20 MHz.*



Wireless Configuration

⊟ Basic Wireless Configuration

System Mode	PMP SS
Channel Width [MHz]	20
RF Freq. [MHz]	5800.0
Auto scan	□
Tx Power[dBm]	10

⊟ Advanced Wireless Configuration

Antenna Gain [dBi]	22
Antenna Alignment Buzzer Enable	□
Radio Mode	Off

Fig. 44: Web - Wireless Configuration Screen -- Subscriber

Auto scan: (Subscriber Only) Check this box ☑ to enable the subscriber to automatically scan available RF frequency ranges to locate and register with a sector controller. When **Auto scan** is not enabled, the wireless link can be established only at the frequency specified in the RF Freq. [MHz] field.

By default, the subscriber will scan all available frequency bands enabled by the options key.

To reduce the scanning/connection time, the operator may specify a subset of frequency ranges to scan. Click on the main menu item **Configuration ->** Frequencies to display the Frequency Management screen.

Tx Power [dBm]: Enter the transmit power level (dBm) (measured at the RDL-3000 RF port). The actual system EIRP will be the power setting plus the gain of the connected antenna. See the following tables to determine the maximum transmit power setting allowed at each modulation level. When DFS is enabled, the subscriber Tx power may be adjusted automatically to avoid false triggering of the DFS feature.

> ***Important -- EIRP Levels***: *Where required by local regulations, the maximum operational power per channel for a specific antenna must not exceed the maximum allowable EIRP levels. The RF output power settings must be professionally programmed by the manufacturer or a trained professional installer. Refer to the FCC and IC notices in this manual (refer to Section 1 and Section 7).*

Table 8: Web - Maximum TX Power Settings (dBm)

Modulation	BPSK	QPSK	16 QAM		64 QAM	
Code Rate	**1/2**	**1/2**	**1/2**	**3/4**	**2/3**	**3/4**
Max. Tx Power	22	22	22	22	22	22

Advanced Wireless Configuration

Max. Distance [km]: (SC only) Enter the distance to the subscriber located farthest from the sector controller.

DFS Action: (SC only) Select the mode of operation for DFS.

The sector controller monitors for interference from radar devices and other equipment using the same channel frequency. When interference is detected, the unit will automatically take the selected action:

None: The DFS function is disabled.

Note: Where DFS is required by regional regulations, this feature is permanently enabled at the factory and can not be disabled by the installer or end-user.

Tx Off: When radar signals are detected, the transmitter is immediatelly switched off, an event message is logged, and configured SNMP trap messages are sent. After thirty minutes the unit monitors the RF channel for one minute. If radar signals are detected, the transitter remains disabled and the unit waits thirty minutes before repeating the monitoring period. Normal operation resumes only when radar signals are not detected during a one minute monitoring period.

Chg Freq: When radar signals are detected, the transmitter is immediatelly switched off, an event message is logged, and configured SNMP trap messages are sent. The unit changes frequency and monitors the new RF channel for one minute. If radar signals are detected during the monitoring period, the tramsitter remains disabled and the unit switches to the next frequency to be tested. Normal operation resumes only when radar signals are not detected during a one minute monitoring period.

Antenna Gain: Enter the antenna gain specified by the manufacturer. This field is required only when the **DFS Action** is set to **Tx Off** or **Chg Freq**.

> ***Important**: It is important to enter the gain value specified by the manufacturer. If the gain is set higher than the actual antenna gain, the sensitivity will be too low and the RDL-3000 will not be operating in compliance with the DFS standards. If the gain is set lower than the actual antenna gain, the RDL-3000 will be more sensitive to interference and this may cause false DFS triggering.*

Antenna Alignment Buzzer Enable: (SS only) Audible antenna alignment tool.

Disabled (□): The antenna alignment tool is disabled (no sound).

Enabled (☑): The antenna alignment tool is active. Faster repetition rates of the sound indicate a stronger signal is being received from the remote-end transmitter.

Registration Period [frames]: (SC only) The sector controller provides opportunities for unregistered subscribers to contact the sector controller and attempt to establish a wireless data link. The Registration Period specifies the number of wireless frames (1 to 100) to wait between transmitting these polling messages. For example, entering a value of '4' will include a registration opportunity in every 4th wireless frame.

Scheduling Cycle: Enter the period of the traffic scheduling cycle. Choosing the scheduling cycle period is generally a balance between providing lower latency (shorter cycle) and more efficient packet processing (longer cycle). The effects of changes to the scheduling cycle will vary based on the aggregate traffic composition (packet rate, packet size, etc). The scheduling cycle is restricted by the selected frame size.

The scheduling cycle can <u>not</u> be less that the frame size, or more than four times the frame size (e.g., Frame Size <= Scheduling Cycle <= frame size *4).

For example, for a 5 ms Frame Size, the Scheduling Cycle must be from 5 to 20 ms.

Fixed Frame: Select the wireless frame mode.

Disabled (□): RDL-3000 adjusts the wireless frame size automatically based on uplink and downlink traffic patterns.

Enabled (☑): Wireless frame size is fixed at the value specified in the **Frame Size** field. When fixed frame mode is enabled, the PIR is limited as follows:

Max PIR = CIR * Scheduling Cycle / Frame Size

Notes:

1. *Fixed frame mode must be used for all synchronized deployments. Refer to section 2.3:* Synchronization I/O Port (PPS) *on page 17 and the Synchronization Mode setting on this screen.*
2. *When Fixed Frame mode is enabled, the synchronization output port (PPS) mode <u>must</u> be specified.*

Frame Size [ms]: When Fixed Frame mode is enabled, the frame size must be specified. The frame size must factor equally into the 1 second synchronization interval. For example, 1000 ms / 20 ms frame = 50 fps.

Downlink Ratio [%]: (SC only) When Fixed Frame mode is selected, the proportion of each frame reserved for downlink data must be specified as a ratio between 20-80 %.

Synchronization Mode: (SC only) Select the method to synchronize the RDL-3000.

The RDL-3000 synchronization feature <u>must</u> be used at any site where two or more sector controllers are deployed (collocated), and networks of geographically collocated cells are located close enough to introduce RF interference.

None: Synchronization is disabled (RF transmitter in free-run mode).

External: The PPS port operates as an input.

The RF transmission cycle is synchronized to the signal received on the PPS port. If no signal is detected on the PPS port, the RF transmitter is synchronized to the internal clock.

Internal: The PPS port operates as an output.

The RF transmission cycle and the PPS port output are synchronized to the internal clock. When a GPS module is installed and tracking, the internal clock is synchronized to the GPS signal. Refer to the RDL-3000 installation Guidelines for additional information.

Synchronization Output: (SC only)

Disabled (□): The PPS port is disabled.

Enabled (☑): The synchronization port output is active.

Synchronization Output Termination: (SC only) Set the PPS output impedance.

When the synchronization port (PPS) output is enabled, the port termination impedance <u>must</u> be specified. When the PPS ports of collocated RDL-3000 units are cabled together, the last RDL-3000 in the daisy chain (no tee adapter) should have the termination set to 50 ohms or 75 ohms (based on cable type). All other units should be set to high impedance (None). Refer to the RDL-3000 Installation Guidelines for more information.

None: Port termination is high impedance.

50 Ohms: Port termination impedance is 50 Ohms.

75 Ohms: Port termination impedance is 75 Ohms.

Radio Enable: Select the operational mode.

Refer to the following table to determine the required RF settings.

Table 9: Web - Radio Enable - RF Port Settings

Setting	Mode	RF Port 1		RF Port 2	
		Tx	Rx	Tx	Rx
Off	RF Disabled	X	X	X	X
RF Port 1	SISO	✓	✓	X	X
RF Port 2	SISO	X	X	✓	✓

IMPORTANT*: Version 1.xx operation is limited to port RF-1. Port RF-2 must be electrically terminated (connect antenna or RF terminating device) and must be weatherproofed.*

Apply: Click to accept and activate the wireless settings displayed on this screen.

Apply & Save All: Click to permanently save the wireless settings displayed on this screen. Saved settings are restored on power-up, reboot, or at the end of a test cycle.

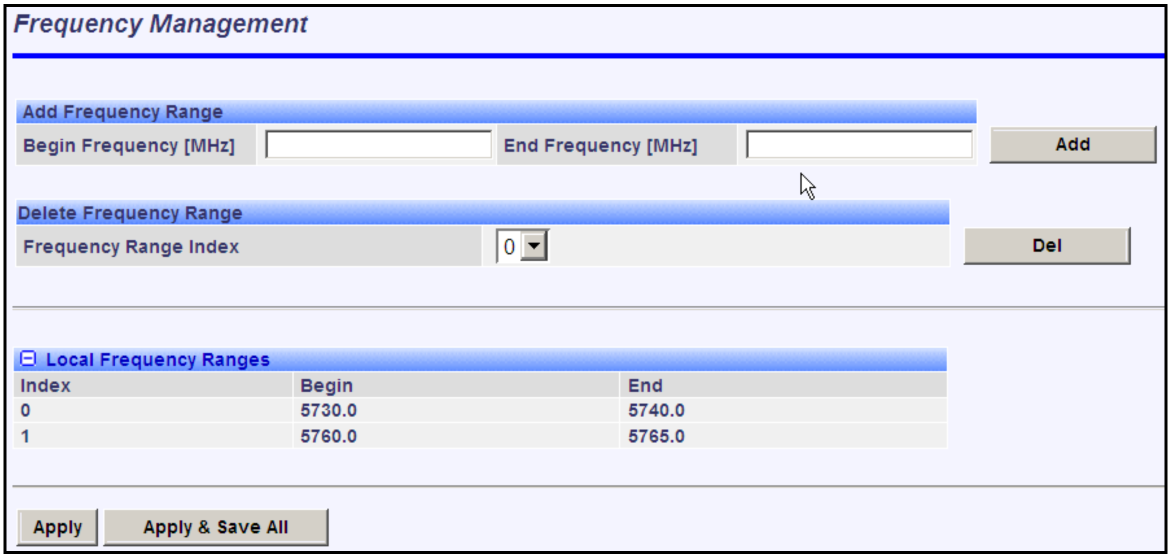
Note: Clicking on another main menu item before clicking Apply or Apply & Save All discards all changes made to settings displayed on the Wireless Configuration screen.

Frequency Management Screen

Click **Configuration**->Wireless->Frequencies to display the Frequency Management screen. Use this screen to create frequency lists for subscribers to quickly locate and re-register with the sector controller. Up to 32 frequency ranges may be entered.

Following any subscriber power-cycle, reboot, or temporary loss of the wireless link (e.g., transient interference) the subscriber first checks any frequencies in the Local Frequency Ranges table. If a sector controller is not located, then the subscriber will scan all available frequencies.

Important*: The Auto scan feature must be enabled on the subscriber to use the frequency lists. If Auto scan is disabled, the subscriber only monitors the channel selection in the RF Frequency field.*



Frequency Management

Add Frequency Range

Begin Frequency [MHz] End Frequency [MHz]

Delete Frequency Range

Frequency Range Index: 0

⊟ Local Frequency Ranges

Index	Begin	End
0	5730.0	5740.0
1	5760.0	5765.0

Fig. 45: **Web - Frequency Management Screen**

Add

Enter the start and end frequency for this range. The subscriber automatically compensates for channel size when selecting center frequencies.

Begin: Lower limit of the frequency range to scan.

End: Upper limit of the frequency range to scan.

Add: Click to save the displayed range settings (Local Frequency Range table). The range entered is not checked for validity until the Apply button is clicked.

Delete

Index: Choose the index of the frequency range to be deleted.

Delete: Click to permanently remove the selected frequency range.

Local Frequency Ranges

The entries in this table are saved in non-volatile memory and are loaded when the unit is power-cycled/rebooted.

Index: Index of this entry in the Local Frequency Range table.

Begin: Lower limit of the frequency scan interval (MHz).

End: Upper limit of the frequency scan interval (MHz).

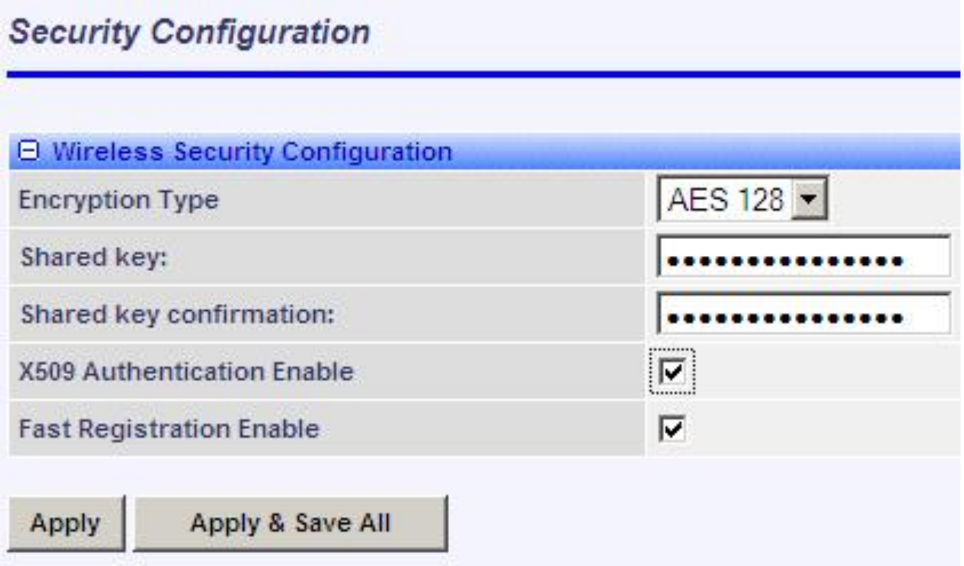
Controls

Apply: Check the current frequency range settings in the Local Frequency Range list. Invalid entries (e.g., out of range) are deleted. Valid settings are activated in the runtime configuration.

Apply and Save All: Check the current frequency range settings in the Local Frequency Range list. Invalid entries (e.g., out of range) are deleted. Valid settings are activated in the runtime configuration and saved permanently.

4.5.5 Wireless Security

Click **Configuration**->Wireless->Security to display the Security Configuration screen. Click ⊞ to expand or ⊟ to hide fields.



Security Configuration

⊟ Wireless Security Configuration

Encryption Type	AES 128
Shared key:	••••••••••••••••
Shared key confirmation:	••••••••••••••••
X509 Authentication Enable	☑
Fast Registration Enable	☑

Fig. 46: **Web - Wireless Security Screen - Sector Controller**

Encryption Type: Select the encryption type to use for data transmitted over the wireless interface. If an encryption type is selected, the identical setting must be made on both communicating units before Ethernet packets can be transferred over-the-air.

None: Encryption is disabled.*

AES 128: Advanced Encryption Standard using 128-bit encryption.

AES 192: Advanced Encryption Standard using 192-bit encryption.

AES 256: Advanced Encryption Standard using 256-bit encryption.

Shared key: Enter the encryption key to be shared between the sector controller and all subscribers in this sector. This is required only when encryption is enabled.

Shared key confirmation: Re-enter key to minimize errors. This field must be identical to the Shared Key field.

X.509 Authentication Enable: Check this box ☑ to require authentication using an installed X.509 certificate. The user-defined unit certificate, authority certificate, and RSA private key must be downloaded using the CLI 'load' command.

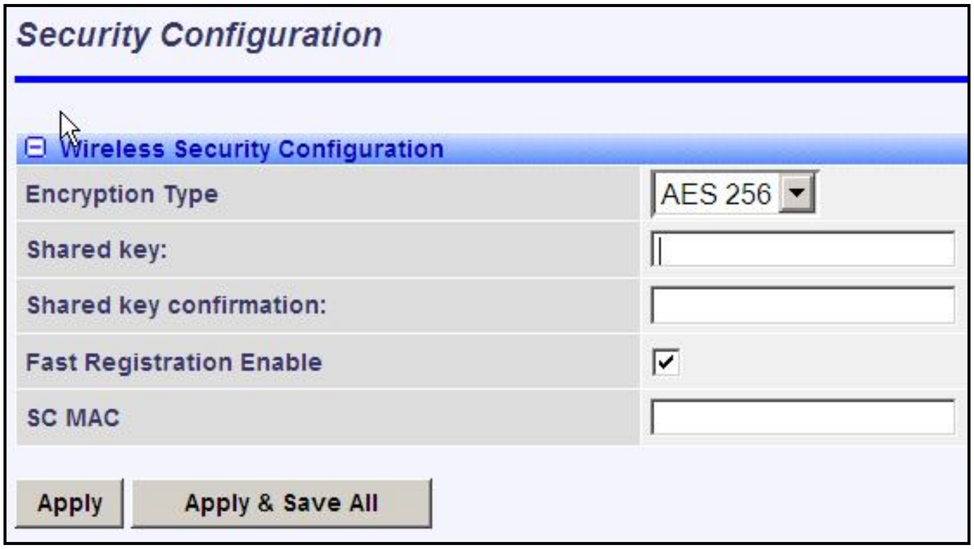
Note: This dialog item is visible only if enabled by the Options Key and X.509 certificates are loaded on the RDL-3000.

Fast Registration Enable: Check this box ☑ to enable the sector controller to use pre-shared keys for quick authentication of a subscriber (bypass Diffie-Hellman method). This feature is not available in FIPS mode.

SC MAC: (Subscriber only) MAC address of the sector controller. The subscriber will establish a wireless link only with the sector controller having the MAC address recorded in this field. If this field is blank, the subscriber will establish a wireless link with any sector controller.

Apply: Click to activate the security settings displayed on this screen.

Apply & Save All: Click to activate and permanently save the security settings on this screen. Saved settings are restored on power-up, reboot, or at the end of a test cycle.



Security Configuration

Wireless Security Configuration

Encryption Type	AES 256
Shared key:	
Shared key confirmation:	
Fast Registration Enable	☑
SC MAC	

Fig. 47: **Web - Wireless Security Screen - Subscriber**

Notes:

1. Clicking on another main menu item before clicking Apply or Apply & Save All will discard any changes made to settings displayed on the current screen.

2. HTTPS (SSL) is not available until an X.509 certificate and DSA private key have been loaded (ssl_cert_<mac>.pem and ssl_key_<mac>.pem).

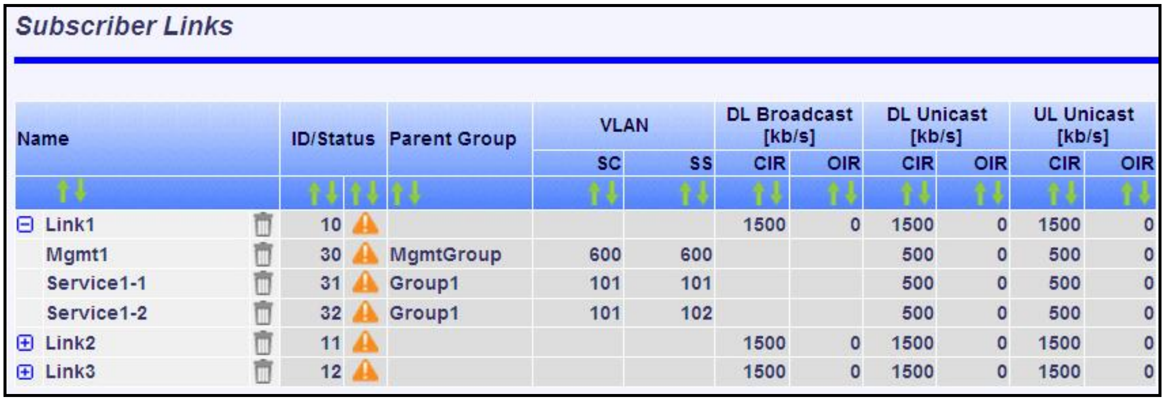
3. AES encryption is not available until the X.509 certificate and key files have been loaded (usr_wacert_<mac>.der, usr_wcert_<mac>.der, and usr_wkey_<mac>.der).

4.6 Provisioning Screens

This section describes monitoring and configuring Links, Service Groups, and Services.

4.6.1 Subscriber Links

The Subscriber Links screen provides a summary view of configuration settings for all Subscriber Links and provisioned Services. Click **Provisioning->Subscriber Links** in the main menu to display operating statistics for all subscriber wireless links. Click ⊞ to expand or ⊟ to hide Service names.



Subscriber Links

Name		ID/Status		Parent Group	VLAN		DL Broadcast [kb/s]		DL Unicast [kb/s]		UL Unicast [kb/s]	
					SC	SS	CIR	OIR	CIR	OIR	CIR	OIR
⊟ Link1	🗑	10	⚠				1500	0	1500	0	1500	0
Mgmt1	🗑	30	⚠	MgmtGroup	600	600			500	0	500	0
Service1-1	🗑	31	⚠	Group1	101	101			500	0	500	0
Service1-2	🗑	32	⚠	Group1	101	102			500	0	500	0
⊞ Link2	🗑	11	⚠				1500	0	1500	0	1500	0
⊞ Link3	🗑	12	⚠				1500	0	1500	0	1500	0

Fig. 48: Web - Subscriber Links Screen

Name: Operator-assigned name for wireless Subscriber Links and Services.

Click the Link name (e.g., Link1) to display the Subscriber Link Configuration screen.

Click the Service Name (Service1-1) to display the Subscriber Service Status screen.

Click on the trashcan symbol (🗑) to delete this Link.

ID/Status: Subscriber Link or Service identifier and status indicator.

ID: A unique identifier (4 to 127) assigned to each subscriber Link. This value is required when using the CLI interface to modify settings.

Status: Status of this Link or Service.

✓ Subscriber Link/Service is available (online).

⚠ Subscriber Link/Service is unavailable (offline or disabled).

Click the Link status icon (e.g., ✓) to display the Subscriber Link Status screen

Click the Service status icon to display the Subscriber Service Status screen.

Parent Group: The Service is a member of this Service Group.

VLAN: VLAN tagging settings.

SC: VLAN classification for this Service Group. This Service Group processes only ingress packets (sector controller Ethernet port) having this VID. This VID is removed before the packet is forwarded over the wireless interface.

Each egress packet belonging to this Service Group has this VID added (Q-in-Q) before the packet is forwarded over the sector controller Ethernet port.

SS: VLAN classification for this Service.

This Service processes only ingress packets (subscriber Ethernet port) having this VID. This VID is removed before the packet is forwarded over the wireless interface. Each egress packet belonging to this Service has this VID added (Q-in-Q) before the packet is forwarded over the subscriber Ethernet port.

DL Broadcast (Kbps): Broadcast traffic downlink rates.

CIR: Requested minimum committed downlink bandwidth.

OIR: Calculated available downlink bandwidth (based on scheduling cycle).

DL Unicast (Kbps): Unicast traffic downlink rates.

CIR: Requested minimum committed downlink bandwidth.

OIR: Available downlink bandwidth (based on scheduling cycle).

UL Unicast (Kbps): Unicast traffic uplink rates.

CIR: Requested minimum committed uplink bandwidth.

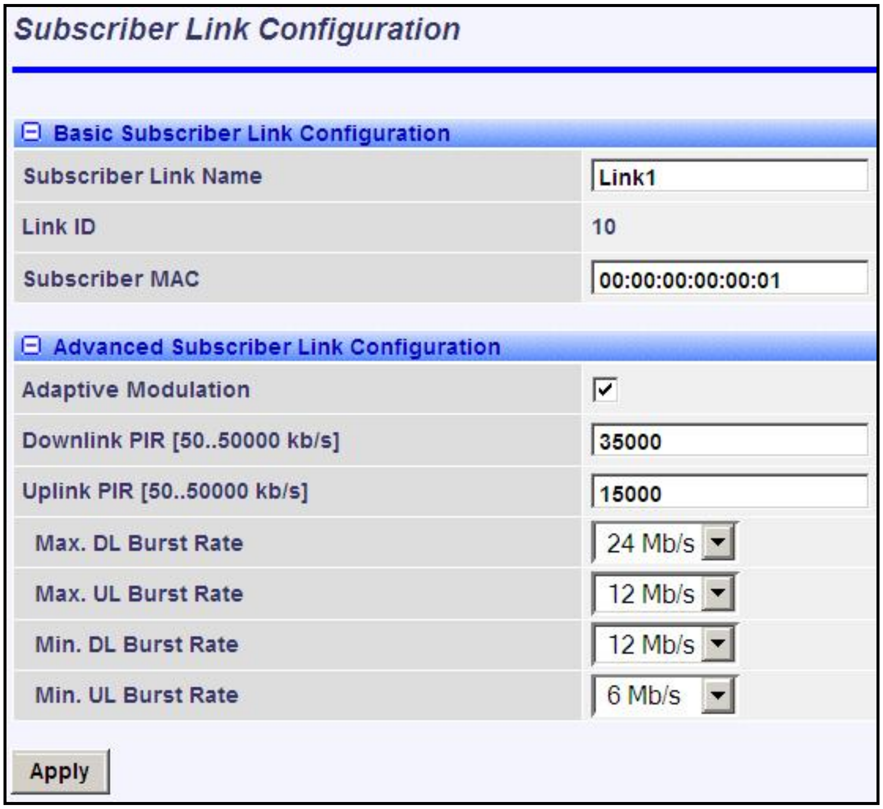
OIR: Calculated available uplink bandwidth (based on scheduling cycle).

Note: Incorrect CIR settings may result in excessive latency or dropped packets *(buffer full condition).*

4.6.2 Subscriber Link Configuration

Use this screen to display and modify settings for a Subscriber Link.

Click **Provisioning->** New Subscriber Link in the main menu to add a new Subscriber Link. To edit an existing Subscriber Link, click **Provisioning->** Subscriber Links in the main menu and click on the name of the subscriber Link (e.g., Link1). Click ⊞ to expand or ⊟ to hide fields.



Subscriber Link Configuration

⊟ Basic Subscriber Link Configuration

Subscriber Link Name	Link1
Link ID	10
Subscriber MAC	00:00:00:00:00:01

⊟ Advanced Subscriber Link Configuration

Adaptive Modulation	☑
Downlink PIR [50..50000 kb/s]	35000
Uplink PIR [50..50000 kb/s]	15000
Max. DL Burst Rate	24 Mb/s
Max. UL Burst Rate	12 Mb/s
Min. DL Burst Rate	12 Mb/s
Min. UL Burst Rate	6 Mb/s

Fig. 49: Web - Subscriber Link Configuration Screen

Basic Subscriber Link Configuration

Subscriber Link Name: Enter a name to identify this wireless link. This identifier is displayed on configuration and statistics screens. The name may contain up to fifteen alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

Link ID: (Read only) A unique identifier (4 to 127) assigned to each subscriber Link. This value is required when using the CLI interface to modify settings.

Subscriber MAC: Enter the MAC address of the subscriber for this wireless link. The sector controller will establish a wireless link only with the subscriber having this MAC address.

For example, when a subscriber unit is replaced (e.g., hardware upgrade), the sector controller will not establish a wireless link until this field is updated with the MAC address of the replacement unit.

Advanced Subscriber Link Configuration

Adaptive Modulation: The adaptive modulation feature automatically adjusts modulation and coding settings to maintain wireless link operation during periods of transient interference, power variations (fade), and reflections. Adaptive modulation can be enabled or disabled individually for each Subscriber Link.

When Adaptive modulation is enabled, the modulation and coding are adjusted automatically to achieve the highest throughput where packet error rates (PER) are lower than factory-set values. When packet error rates exceed this threshold, the modulation/code combination is adjusted to maintain the connection at a lower throughput rate. The operator must select the maximum and minimum burst rates for the uplink and downlink.

When Adaptive modulation is disabled, the operator must select only the maximum uncoded burst rate (UBR) for the uplink and downlink.

Max. DL Burst Rate: Maximum downlink UBR for unicast traffic to this subscriber.

Max. UL Burst Rate: Maximum uplink UBR for unicast traffic from this subscriber.

Min. DL Burst Rate: (Displayed only when adaptive modulation is enabled) Minimum downlink UBR for unicast traffic.

Min UL Burst Rate: (Displayed only when adaptive modulation is enabled) Minimum uplink UBR for unicast traffic.

Note: Adjustments to modulation and coding cause temporary changes to the PIR of all connections on that wireless link. This ensures interference on a wireless link does not affect the throughput of other links in that sector.

When adaptive modulation adjusts the uplink or downlink modulation/coding settings of a wireless link to below the desired minimum burst rate setting, the downlink PIR for all Services/Service Groups are reduced proportionally until the condition clears.

For example, in a link operating at 16 QAM 3/4, transient interference may result in a temporary change to 16 QAM 1/2 to maintain the required PER, and restore the higher modulation setting after the interference has cleared.

Downlink PIR: Enter the peak downlink information rate (aggregate downlink traffic for all Services and Service Groups).

Uplink PIR: Enter the peak uplink information rate (aggregate uplink traffic for all Services and Service Groups).

Note: Uplink and downlink traffic transmitted over the wireless interface is monitored to enforce PIR settings (50 - 50000 Kbps). Traffic statistics are reset at the beginning of each common one-second clock tick. If the maximum throughput is reached on any Link before the end of the current interval, that Link is excluded from sending additional traffic until after the next clock tick.

For example, if a Link transmits its full data allocation in the first 650 ms of the current metering interval, the Link will not receive any additional bandwidth allocation until the beginning of the next interval (enforced pause of 350 ms).

When adaptive modulation is enabled, automatic adjustments to the modulation/coding will result in relative changes to the PIR of that wireless link.

DL Burst Rate: Downlink burst rate for unicast traffic. The RDL-3000 will establish a wireless link only at the specified rate. The communicating wireless unit must also be operating at the same fixed rate.

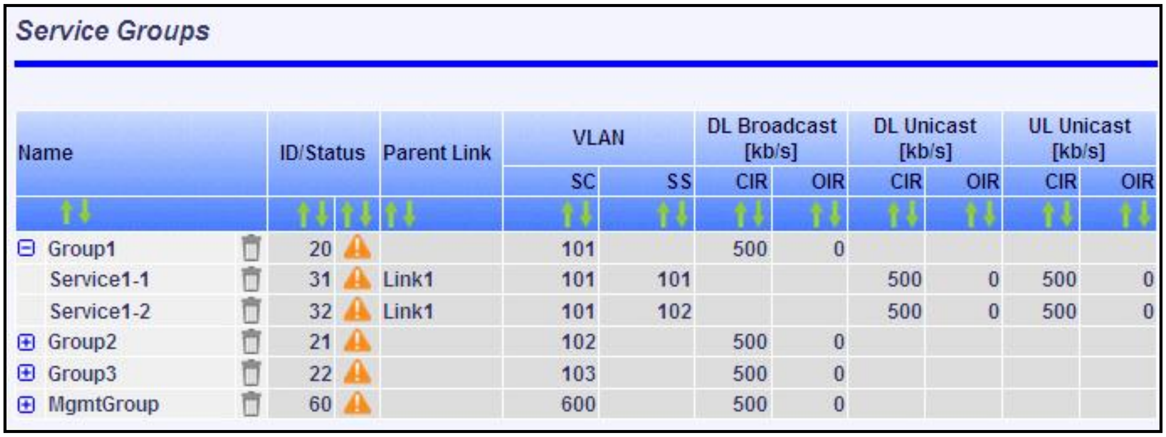
UL Burst Rate: Uplink burst rate for unicast traffic. The RDL-3000 will establish a wireless link only at the specified rate. The communicating wireless unit must also be operating at the same fixed rate.

Controls

Apply: Click to accept and activate displayed settings.

4.6.3 Service Groups

The Service Groups screen provides a summary view of configuration settings for all Service Groups and provisioned Services. Click **Provisioning->Service Groups** in the main menu to display the Service Groups screen. Click ⊞ to expand or ⊟ to hide fields.



Service Groups

Name		ID/Status	Parent Link	VLAN		DL Broadcast [kb/s]		DL Unicast [kb/s]		UL Unicast [kb/s]	
				SC	SS	CIR	OIR	CIR	OIR	CIR	OIR
↑↓		↑↓ ↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓
⊟ Group1	🗑	20 ⚠		101		500	0				
Service1-1	🗑	31 ⚠	Link1	101	101			500	0	500	0
Service1-2	🗑	32 ⚠	Link1	101	102			500	0	500	0
⊞ Group2	🗑	21 ⚠		102		500	0				
⊞ Group3	🗑	22 ⚠		103		500	0				
⊞ MgmtGroup	🗑	60 ⚠		600		500	0				

Fig. 50: **Web - Service Groups Screen**

Name: Identifies Service Groups and member Services.

Click the Service Group name to display the Service Group Configuration screen.

Click the Service name to display the Subscriber Service Configuration screen.

ID/Status: Identifier and status for the subscriber Link or Service.

ID: A unique identifier assigned to each Service Group (128 to 159) and Service (160 to 511). This value is required when using the CLI interface to modify settings.

Status: The status of this Service Group or Service.

✓ Service Group or Service is available.

⚠ Service Group or Service is unavailable (down/offline).

Click the Service Group status icon (e.g., ✓) to display the Service Group Status screen. Click the Service status icon to display the Subscriber Service Status screen.

Parent Link: The Service is assigned to this Subscriber Link.

VLAN: VLAN classification settings.

SC: VLAN classification setting at the sector controller (Service Group).

SS: VLAN classification setting at the subscriber (Service).

DL Broadcast (Kbps): Minimum rate for downlink broadcast traffic.

CIR: Operator requested bandwidth.

OIR: Assigned bandwidth.

UL Unicast (Kbps): Minimum rate for uplink unicast traffic.

CIR: Operator requested bandwidth.

OIR: Assigned bandwidth.

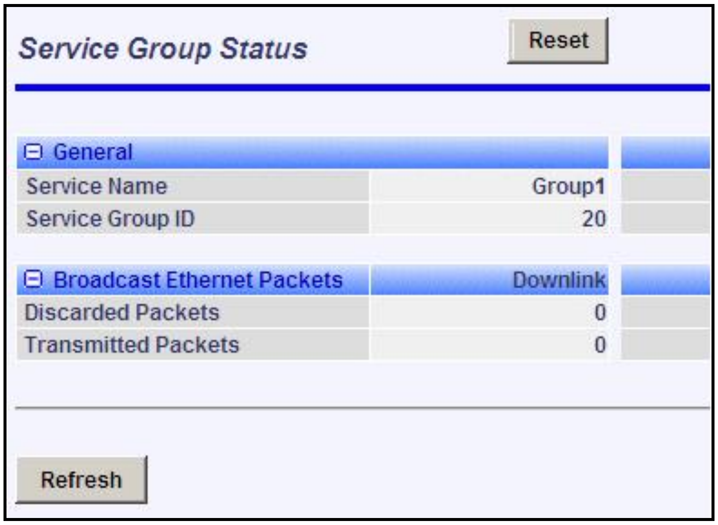
DL Unicast (Kbps): Minimum rate for downlink unicast traffic.

CIR: Operator requested bandwidth.

OIR: Assigned bandwidth.

4.6.4 Service Group Status

Use this screen to monitor the status of all Service Groups. Click **Provisioning->Service Groups** in the main menu to display the Service Groups screen. Click on the status symbol (e.g., ✓) to display the Service Group Status screen. Click ⊞ to expand or ⊟ to hide fields.



Service Group Status

⊟ General	
Service Name	Group1
Service Group ID	20

⊟ Broadcast Ethernet Packets	Downlink
Discarded Packets	0
Transmitted Packets	0

Fig. 51: **Web - Service Group Status Screen**

General

Service Group Name: Name of the Service Group.

Service Group ID: A unique identifier assigned to each Service Group (128 to 159). This value is required when using the CLI interface to modify settings.

Broadcast Ethernet packets

Discarded Packets: Total packets discarded by this unit due to errors.

Transmitted Packets: Total broadcast (or multicast) packets successfully transmitted over the wireless interface (does not include discarded or errored packets).

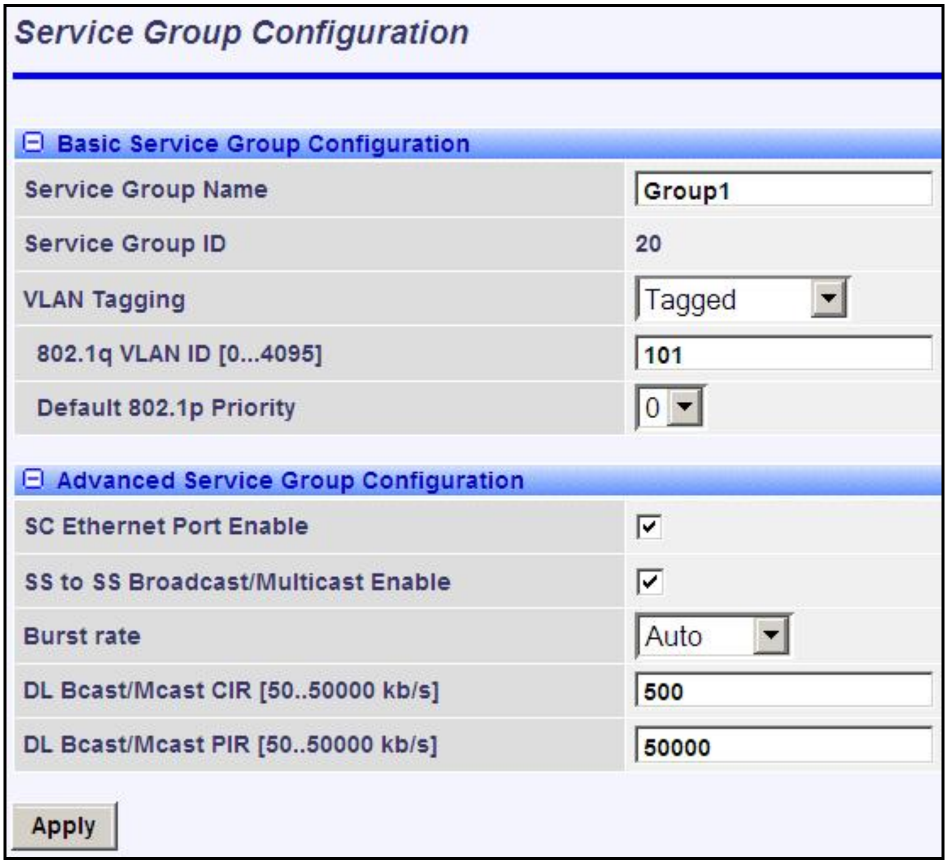
Controls

Reset: Click to reset displayed statistics counters.

Refresh: Click to update displayed statistics counters.

4.6.5 Service Group Configuration

Use this screen to create new Service Groups or view/modify existing Service Groups. Click **Service Groups** in the main menu, locate the desired Service Group in the table, and click on the Service Group name (Name column) to display this screen. Click ⊞ to expand or ⊟ to hide fields.



Service Group Configuration

⊟ Basic Service Group Configuration

Service Group Name	Group1
Service Group ID	20
VLAN Tagging	Tagged
802.1q VLAN ID [0...4095]	101
Default 802.1p Priority	0

⊟ Advanced Service Group Configuration

SC Ethernet Port Enable	☑
SS to SS Broadcast/Multicast Enable	☑
Burst rate	Auto
DL Bcast/Mcast CIR [50..50000 kb/s]	500
DL Bcast/Mcast PIR [50..50000 kb/s]	50000

Fig. 52: **Web - Service Group Configuration Screen**

Basic Service Group Configuration

Service Group Name: Enter a unique name to identify this Service group. This identifier is displayed on configuration and statistics screens. The name may contain up to fifteen (15) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

Service Group ID: (Read only) A unique identifier assigned to each Service Group (128 to 159). This value is required when using the CLI interface to modify settings.

VLAN Tagging: Select the classification mode for this Service Group.

> **Tagged**: Select tagged to associate a unique VID with this Group.
>
> **Pass-through**: Classify all packets that do not have a VLAN ID, or where the outermost VLAN ID tag does not match the VLAN ID for any tagged Group. Ethernet ingress port are discarded.

802.1Q VLAN ID [0-4095]: Enter the VID associated with this Group definition.

This field is active only when 'Tagged' is selected in the Group Tagging Mode field.

Default Priority: Enter the default 802.1p priority setting.

The default priority value is applied when a S ervice Group set to Tagged mode (add VLAN tag) receives a packet with no priority information.

Advanced Service Group Configuration

SC Ethernet Port Enable: Controls the function of the sector controller Ethernet port for group multicast traffic.

Enabled (☑): Broadcast and multicast traffic received from subscribers is forwarded over the sector controller Ethernet port.

Disabled (□): Broadcast and multicast traffic received from subscribers is not forwarded over the sector controller Ethernet port.

SS To SS Broadcast and multicast Enable:

Enabled (☑): Broadcast and multicast traffic received from subscribers is forwarded over the wireless interface to all subscribers associated with the group.

Disabled (□): Broadcast and multicast traffic received from subscribers is not forward over the wireless interface.

Burst Rate: Enter the uncoded burst rate for downlink broadcast and multicast traffic belonging to this Group. Use the 'Auto' setting (recommended) to have the rate selected automatically based on the current operating conditions. To set this to a fixed value, first identify the group member having the lowest Max DL Burst Rate setting, and then calculate the rate using the formula:

Burst_Rate = Max DL Burst Rate - 1

Note: Applications requiring a higher broadcast or multicast rate (e.g., video) may use a higher setting at the risk of less reliable retransmissions.

DL Bcast/Mcast CIR [50..50000 Kbps]: Set the CIR for downlink broadcast and multicast traffic belonging to this group.

DL Bcast/Mcast PIR [50..50000 Kbps]: Set the PIR for downlink broadcast and multicast traffic belonging to this group.

Note: Traffic transmitted over the wireless interface is monitored to enforce CIR/PIR settings. Traffic statistics are reset at the beginning of each common one-second clock tick. When adaptive modulation is enabled, automatic adjustments to the modulation/coding will result in relative changes to the CIR/PIR of that wireless link.

Controls

Apply: Click to accept and activate displayed settings.

4.6.6 Subscriber Service Status

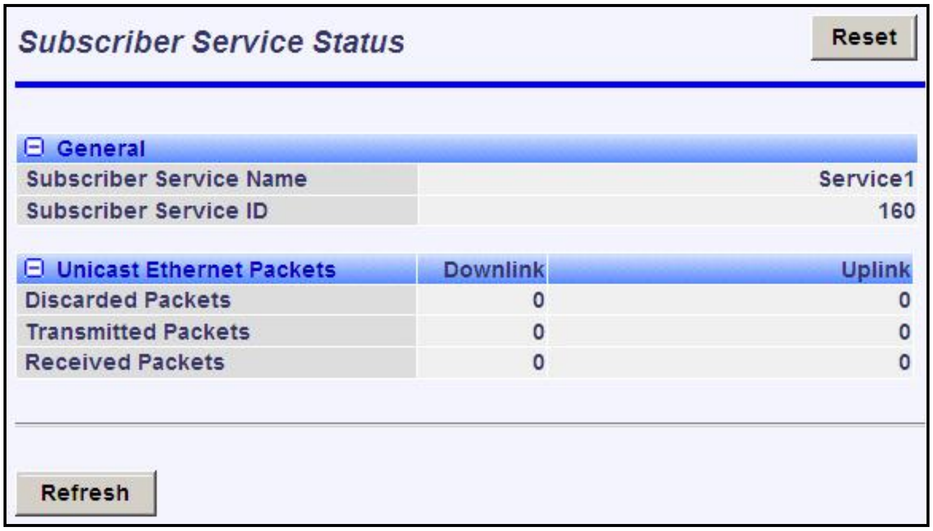
Services status and configuration screens can not be displayed directly; the operator must first select a Subscriber Link or Service Group, and then choose the Service from the list. Refer to the following screens:

4.4.5: Subscriber Services Summary (Subscriber Only) on page 51

4.6.1: Subscriber Links on page 72

4.6.3: Service Groups on page 76

This screen displays status and statistics information for a Service. Click ⊞ to expand or ⊟ to hide fields.



Subscriber Service Status

⊟ General	
Subscriber Service Name	Service1
Subscriber Service ID	160

⊟ Unicast Ethernet Packets	Downlink	Uplink
Discarded Packets	0	0
Transmitted Packets	0	0
Received Packets	0	0

Fig. 53: **Web - Subscriber Service Status Screen**

General

Service Name: Operator-assigned name for this Service.

Service ID: A unique identifier assigned to each Service (160 to 511). This value is required when using the CLI interface to modify settings.

Ethernet Packets

Packets: **Discarded**: Total number of packets discarded by this unit due to errors.

Rx: Received wireless packets discarded.

Tx: Transmitted wireless packets discarded by remote end unit.

Packets Transmitted: Total packets successfully processed over the wireless interface. Total does not include discarded or errored packets.

Rx: Total received wireless packets.

Tx: Total transmitted wireless packets.

Packets Received: Total packets successfully processed over the wireless interface. Total does not include discarded or errored packets.

Rx: Total received wireless packets.

Tx: Total transmitted wireless packets.

Controls

Reset: Click to zero all displayed statistics counters.

Refresh: Click to update displayed statistics counters.

4.6.7 Subscriber Service Configuration

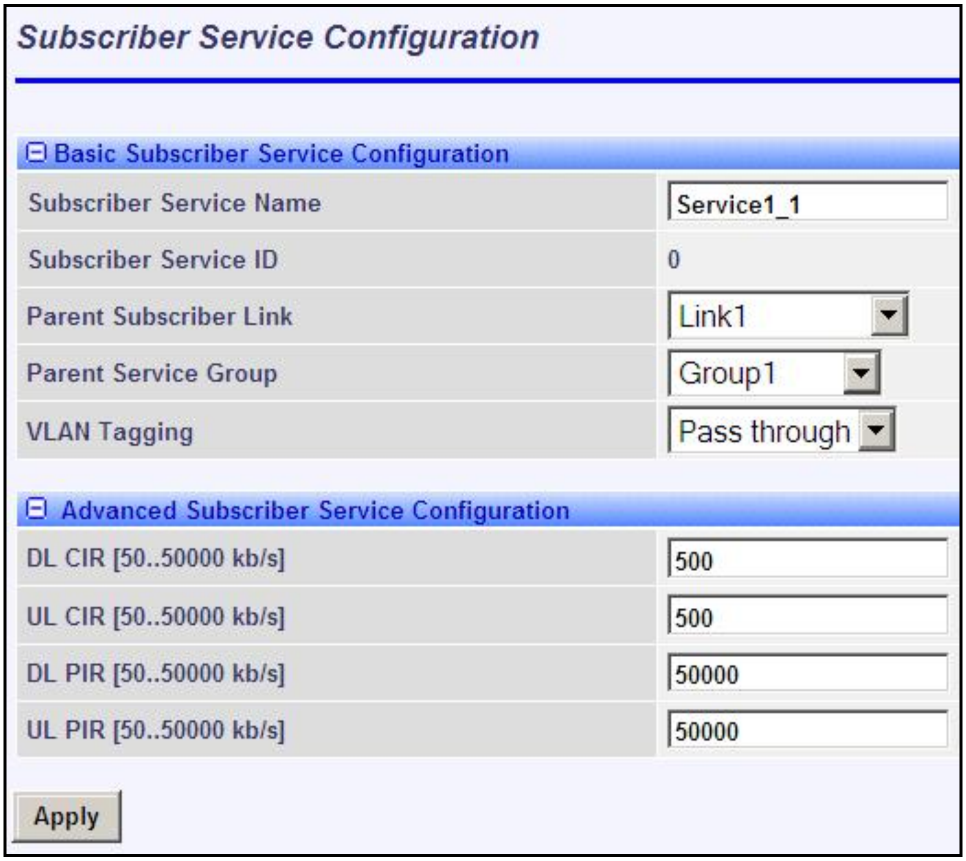
Services status and configuration screens can not be displayed directly; the operator must first select a Subscriber Link or Service Group, and then choose the Service from the list. Refer to the following screens:

4.4.5: Subscriber Services Summary (Subscriber Only) on page 51

4.6.1: Subscriber Links on page 72

4.6.3: Service Groups on page 76

To add a new Service, click **New Service** in the main menu. To edit existing Services, click **Subscriber Links** in the main menu, click ⊞ to expand the Link hosting this Service, and then click the Service name (Name field). The Service Configuration screen is displayed and the fields can be updated. Click ⊞ to expand or ⊟ to hide fields.



Subscriber Service Configuration

⊟ Basic Subscriber Service Configuration

Subscriber Service Name	Service1_1
Subscriber Service ID	0
Parent Subscriber Link	Link1
Parent Service Group	Group1
VLAN Tagging	Pass through

⊟ Advanced Subscriber Service Configuration

DL CIR [50..50000 kb/s]	500
UL CIR [50..50000 kb/s]	500
DL PIR [50..50000 kb/s]	50000
UL PIR [50..50000 kb/s]	50000

Fig. 54: **Web - Subscriber Service Configuration Screen**

Basic Service Configuration

Service Name: Enter a name for this Service (15 characters maximum). The Service name is displayed on configuration and statistics screens.

Parent Subscriber Link: Each Service must be associated with a Link (subscriber). Use the drop-down menu to choose the subscriber Link for this service.

Parent Service Group: Each Service must be associated with a S ervice Group to manage broadcast and multicast traffic. Use the drop-down menu to choose the Service Group for this service.

VLAN Tagging: Select the classification mode for this Service.

Tagged: Select tagged to associate a unique VID with this Group.

Pass-through: Classify all packets that do not have a VLAN tag, or where the outermost VLAN ID tag does not match the VLAN ID for any tagged Group.

802.1Q VLAN ID [0-4095]: Enter the VID associated with this Group definition.

This field is applied only when 'Tagged' is selected in the Group Tagging Mode field.

Default Priority: Enter the default 802.1p priority setting.

The default priority value is applied when a Service Group set to Tagged mode (add VLAN tag) receives a packet with no priority information.

Advanced Service Configuration

DL CIR: Enter the committed information rate for downlink unicast traffic.

UL CIR: Enter the committed information rate for uplink unicast traffic.

DL PIR: Enter the peak information rate for downlink unicast traffic.

UL PIR: Enter the peak information rate for uplink unicast traffic

The traffic each Service transmits over the wireless interface is monitored to enforce PIR settings (50 - 50000 Kbps). Traffic statistics are reset at the beginning of each common one-second clock tick. If the maximum throughput is reached on any Service before the end of the current interval, that Service is excluded from sending additional traffic until after the next clock tick.

For example, if a Service transmits its full data allocation in the first 650 ms of the current metering interval, that Service will not receive any additional bandwidth allocation until the beginning of the next interval (enforced pause of 350 ms).

When adaptive modulation is enabled, automatic adjustments to the modulation/coding will result in relative changes to the PIR of all Services and Service Groups using that wireless link. Incorrect PIR settings may result in excessive latency or dropped packets *(buffer full condition).*

Controls

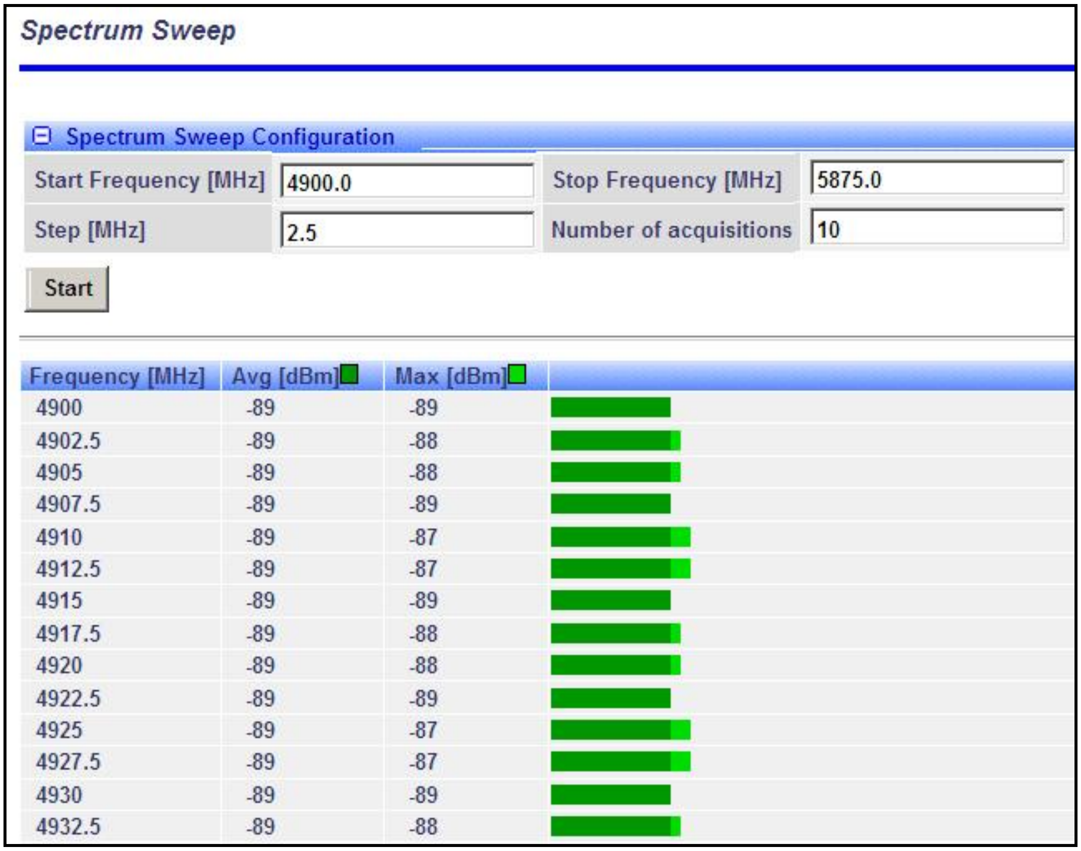
Apply: Click to accept and activate displayed settings.

4.7 Utilities Screens

4.7.1 Spectrum Sweep

Use the RDL-3000 **Spectrum Sweep** feature to determine if RF spectrum is clear of interference. Click **Utilities ->** **Spectrum Sweep** in the left hand menu to display the Spectrum Sweep configuration screen. Click ⊞ to expand or ⊟ to hide fields.

Configurable survey settings allow you to scan a specific frequency range. Configurable survey parameters include the high and low frequency limits, the step size, and the number of samples at each step. The output graph displays the average (dark green) and maximum (light green) RSSI measured at each step.



Spectrum Sweep

⊟ Spectrum Sweep Configuration

Start Frequency [MHz]	4900.0	Stop Frequency [MHz]	5875.0
Step [MHz]	2.5	Number of acquisitions	10

Start

Frequency [MHz]	Avg [dBm]🟩	Max [dBm]🟩
4900	-89	-89
4902.5	-89	-88
4905	-89	-88
4907.5	-89	-89
4910	-89	-87
4912.5	-89	-87
4915	-89	-89
4917.5	-89	-88
4920	-89	-88
4922.5	-89	-89
4925	-89	-87
4927.5	-89	-87
4930	-89	-89
4932.5	-89	-88

Fig. 55: **Web - Spectrum Sweep Screen**

Spectrum Sweep Configuration

Start Frequency (MHz): Enter center frequency of the lowest channel to be scanned.

End Frequency (MHz): Enter center frequency of the highest channel to be scanned.

Step (MHz): Enter the frequency step (MHz) to use when scanning from the lowest to the highest frequency. The step selection must be a multiple of 2.5 MHz (e.g., 2.5, 5, etc).

No. of acquisitions: Enter the number of times the frequency is sampled at each step. The recommended range is 10 to 100 samples.

Controls

Start: Click to begin the scan.

Spectrum Sweep Chart

Frequency (MHz): Center frequency of the scanned channel.

Ave (dBm): Average measured signal for all samples.

Max (dBm): Maximum measured signal for all samples.

Bar Graph: Graph of average (dark green) and peak (light green) results.

Performing a Sweep

1. Prepare the RDL-3000:

   For PMP sector controllers, the transmitter is disabled automatically during a sweep.

   Note: To run a sweep from a PMP Subscriber location, the sector controller transmitter must be disabled for the duration of the test.

2. Click Wireless **Spectrum Sweep** in the main menu. It is recommended to scan using the smallest available channel with a step size of 1/2 the planned channel size (e.g., use a 5 MHz step size when scanning for a free 10 MHz channel). For example:

   Start/Stop = 5735 / 5830

   Step [MHz] = 5

   No. of Acquisitions = 10

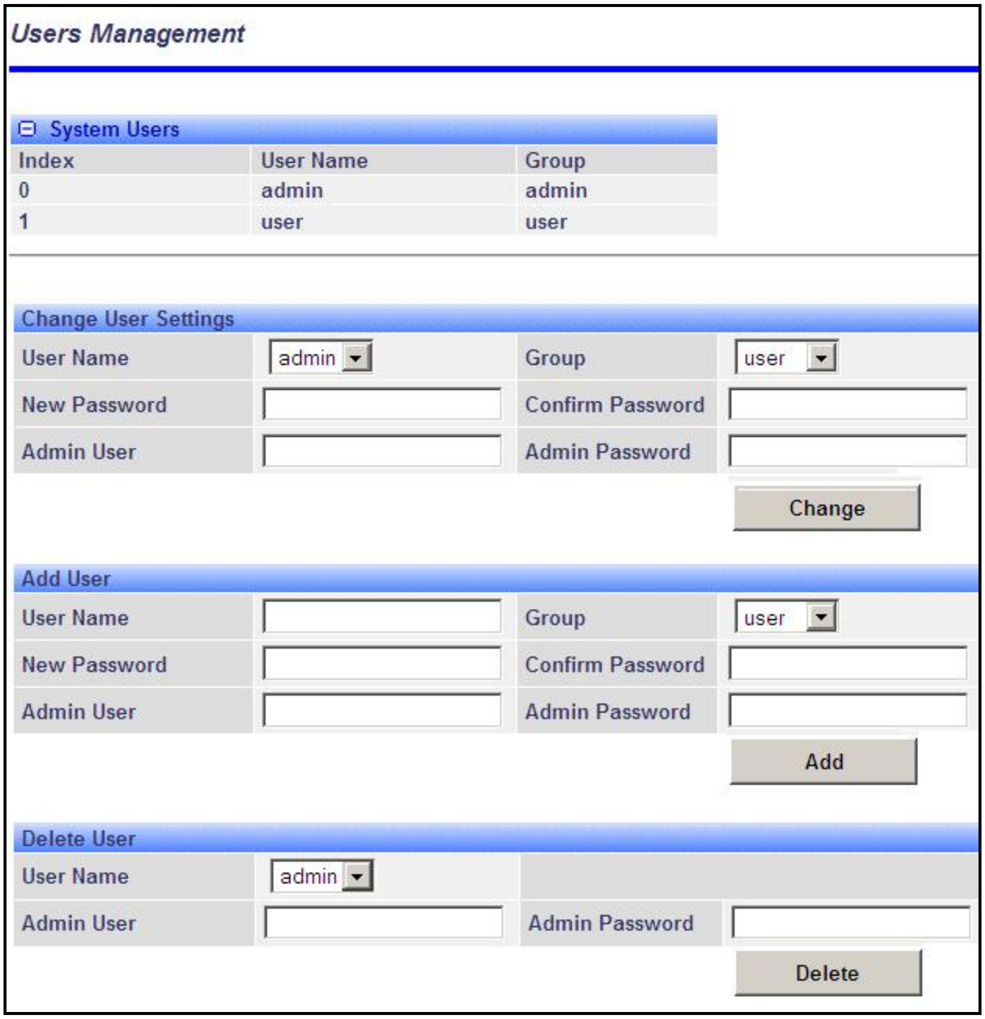
3. Click Start button to begin the sweep.

4. Review the results. A channel is 'clear' when free of interference for at least +/- one-half the channel bandwidth from the desired center frequency. For example, a 20 MHz channel should have no interference detected for at least +/- 10 MHz from the candidate channel.

   When a clear channel is identified, reduce the frequency range and step size while increasing the sample size to monitor the channel over a longer period.

4.7.2 Users Management

Use the Users Management screen to manage user account and passwords on the RDL-3000. Click **Utilities -> Users Management** in the left hand menu to display the System Password screen. Click ⊞ to expand or ⊟ to hide fields.



Users Management

⊟ System Users

Index	User Name	Group
0	admin	admin
1	user	user

Change User Settings

User Name	admin ▾	Group	user ▾
New Password		Confirm Password	
Admin User		Admin Password	

Change

Add User

User Name		Group	user ▾
New Password		Confirm Password	
Admin User		Admin Password	

Add

Delete User

User Name	admin ▾		
Admin User		Admin Password	

Delete

Fig. 56: Web - Users Management Screen

The RDL-3000 supports administrator and user accounts. See Table 5: Web - Screens and User Access on page 39 for permissions associated with each group.

Administrators can add new user accounts and modify passwords. Usernames may be 1 to 19 alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_), Passwords may be 8 to 15 alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

***Important**: There must always be at least one 'administrator' account active on the RDL-3000. You can <u>not</u> manage the RDL-3000 if all accounts are 'user'.*

Note: When user authentication is set to RADIUS Only or Local + RADIUS, the authorization data is retrieved from the RADIUS server at ten minute intervals. For example, if a user's authorization is changed on the RADIUS server, it may be up to ten minutes (max.) before the RDL-3000 is updated.

System Users

User Name: Operator-assigned login name for this user.

Group: Select a group for the new user account. See Table 5: Web - Screens and User Access table.

Change User Settings

Use these controls to change the settings for an existing account.

User name: Select the existing user account to be modified.

Group: Select the group to be associated with this username (optional).

New Password: Enter the new user password for this account (optional).

Confirm Password: Re-enter new user password (if changing user password).

Admin User: Enter the name of the administrator authorizing this change.

Admin Password: Enter the administrator password.

Change: Click to activate and permanently save changes.

Add User

Use these controls to create a new account.

Name: Enter a name for the new user account.

New Password: Enter a password for the new account.

Confirm Password: Re-enter the password for the new account.

Admin User: Enter the name of the administrator authorizing this change.

Admin Password: Enter the administrator password.

Add: Click to activate the new account and permanently save changes.

Delete User

Use these controls to delete an existing user.

User name: Select an existing user account.

Admin User: Enter the name of the administrator authorizing this change.

Admin Password: Enter the administrator password.

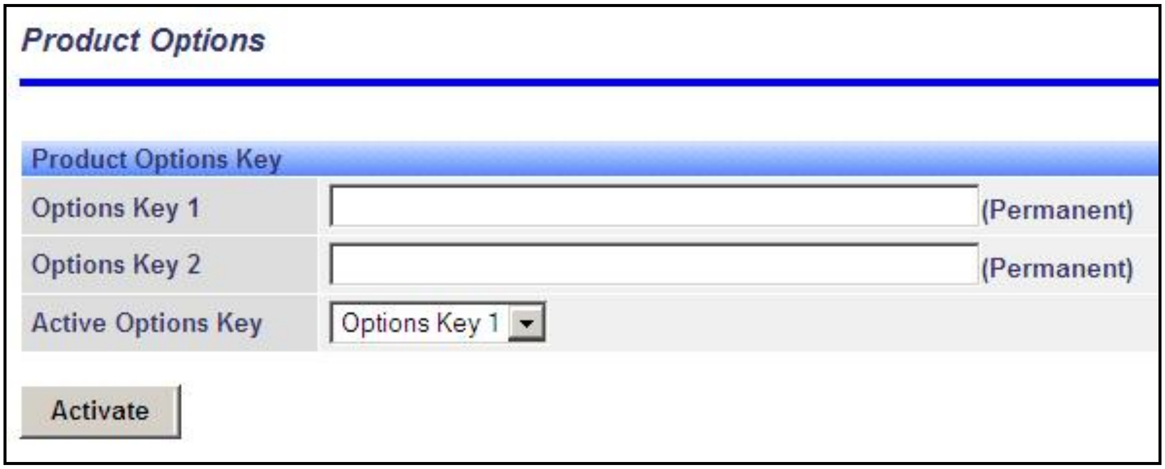
Del: Click to delete user and permanently save changes.

4.7.3 Product Options

Click **Utilities -> Product Options** in the left hand menu to display the Product Options screen. The options keys (a string of numbers, letters, and dashes) enable RDL-3000 features including the maximum uncoded burst rate (UBR) and frequency ranges. Options keys are based MAC address, making each key unique to a specific RDL-3000.

***Important**: If the RDL-3000 is placed in-Service without entering a purchased permanent Options Key, the wireless link will experience Service outages.*

At least one valid permanent options key must be purchased and installed before the RDL-3000 is placed in-Service. A second options key (permanent or temporary key) may be added to trial new options. When a temporary options key is active, a message is logged and an SNMP trap is generated every six hours during the last five days of operation.



Product Options

Product Options Key

Options Key 1		(Permanent)
Options Key 2		(Permanent)
Active Options Key	Options Key 1	

Fig. 57: **Web - Product Options Screen**

Options Key 1: Enter a valid permanent key. A permanent Options Key must be entered for in-Service operation. The temporary options key shipped with the RDL-3000 will expire and Service is interrupted.

Options Key 2: Enter a second valid permanent or temporary options key (optional).

Active Options Key: The Active Options Key field selects the preferred key. If valid, the selected key is activated immediately when the Activate button is clicked. This selection is not affected by switching firmware versions. If the (temporary) active key expires, the RDL-3000 will attempt to remain operational by automatically switching to the other key (e.g., permanent key).

***Important**: Always enter and activate a purchased permanent options key before testing temporary keys -- otherwise you will experience a Service outage on the wireless link when the temporary key expires.*

Controls

Activate: Click to validate and activate options key(s). Invalid keys are discarded and an error message is recorded in the event log. If two keys are entered in the same session (before clicking Activate), keys are saved only if both keys are valid. When each key is validated, the key 'type' is displayed adjacent to the key indicating either 'Permanent' or 'Temporary'.

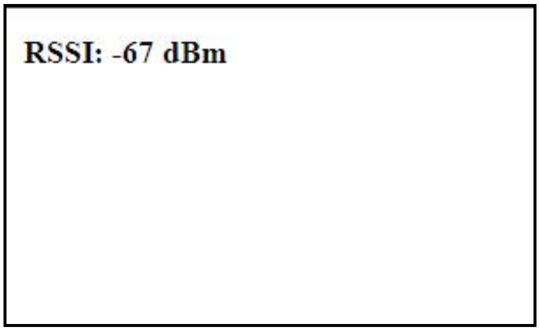
The RDL-3000 has the following default settings when operating with no option key:

Table 10: Web - Defaults with No Options Key	
System	
SNMP	V2
VLAN for Data (Classification)	Disabled
VLAN for Management	Disabled
Wireless	
System Mode	PMP SS Only
Channel Width	10 MHz
RF Freq.	T502 radio (MHz): 4940-4990, 5150-5250, 5495-5600, 5650-5725, 5725-5795, 5815-5875
Auto Scan	Disabled
Tx Power	10 dBm max.
DFS	Disabled
Security	
AES	Disabled
Secure Management: HTTPS, SSH, SNMPv3	Disabled
X.509 Authentication	Disabled
Provisioning.	
No of Subscribers	0
Max UL/DL UBR	3 Mbps

4.7.4 Antenna Alignment Screen

Click **Utilities -> Antenna Alignment** in the main menu to display the Antenna Alignment Tool screen. This screen is provided to assist aligning the subscriber antenna.

The most reliable method for obtaining optimum performance from a wireless link is by fine alignment of the antenna to the position providing the highest RSSI (Received Signal Strength Indication). This web page assists alignment by providing continuous updates of the current measured RSSI value.



RSSI: -67 dBm

Fig. 58: **Web - Antenna Alignment Tool Screen**

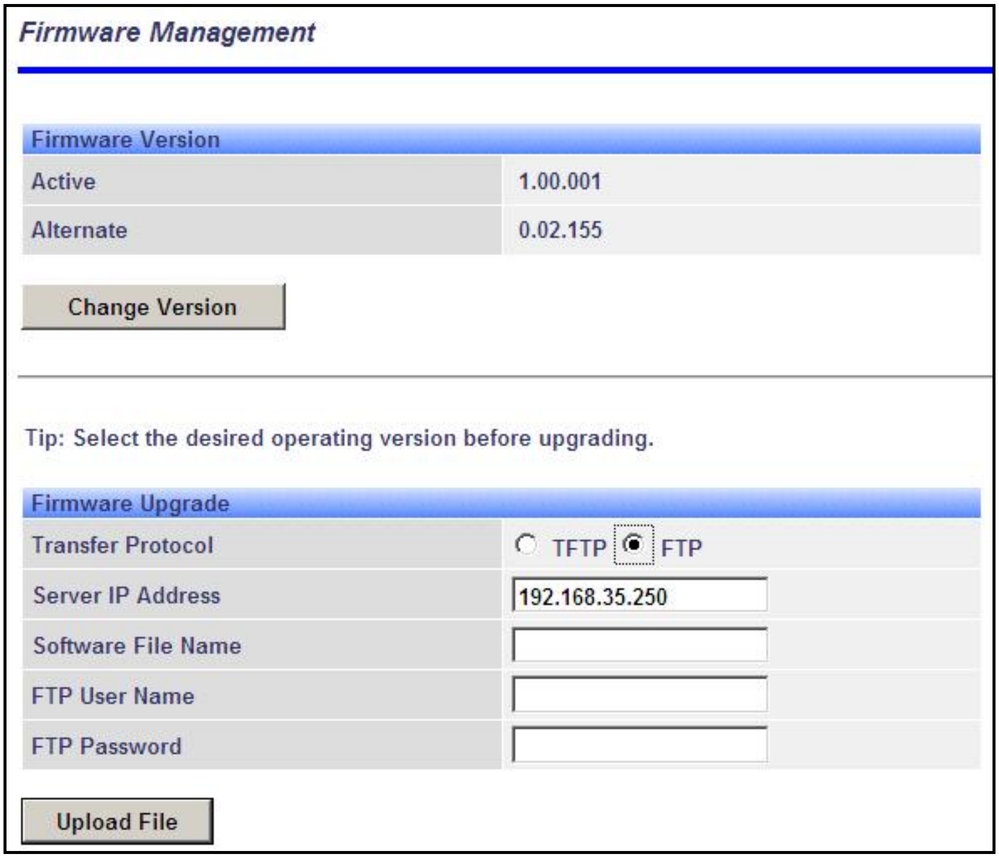
If Wi-Fi service is available, you may also be able to access the web alignment page directly from a laptop computer and most web-enabled handheld devices using the following URL:

http:// [RDL-3000 IP Address] / usr / aa.html

For example: http:// 192.168.20.25 / usr / aa.html

4.7.5 Firmware Management Screen

Click **Utilities -> Firmware** in the main menu to display the Firmware Management screen. Use this screen to upgrade the RDL-3000 with new firmware. The RDL-3000 contains non-volatile storage for two versions of the firmware. The upload overwrites the Alternative (inactive) version.



Firmware Management

Firmware Version	
Active	1.00.001
Alternate	0.02.155

Tip: Select the desired operating version before upgrading.

Firmware Upgrade	
Transfer Protocol	○ TFTP ● FTP
Server IP Address	192.168.35.250
Software File Name	
FTP User Name	
FTP Password	

Fig. 59: **Web - Firmware Management Screen**

Firmware Version

Active: This is the firmware currently in use by the RDL-3000.

Alternative: This is the inactive firmware. Firmware downloaded to the RDL-3000 will overwrite this version.

Change Version: Click to switch the Active and Alternative firmware versions and reboot the RDL-3000.

Firmware Upgrade

Transfer Protocol: Select the type of file server:

TFTP: Use Trivial File Transfer Protocol for file upload.

FTP: Use File Transfer Protocol for file upload.

Server IP Address: Enter the IP address of the computer with the firmware upgrade file. The designated computer must be running a TFTP/FTP server.

Firmware File Name: Name of the firmware binary file (including file extension).

FTP User Name: Enter the user account name on the FTP server (FTP only).

FTP Password: Enter the password for the user account name on the FTP server (FTP only).

Upgrade Steps

Important; The RDL-3000 firmware binary file must be located in the default upload directory of the TFTP/FTP server.

1. Login to the RDL-3000 Web interface and click **Utilities -> Firmware** in the main menu.
2. Select TFTP or FTP, enter the IP Address of the server, and enter the full name of the binary file (including the .bin extension). If FTP is selected, enter account name and password.
3. Click Upload File to begin the file transfer. The transfer may require up to eight minutes based on the data transfer rate. Do not interrupt the transfer process.

   When the transfer is complete, the RDL-3000 checks the integrity of the uploaded file and registers a status message in the event log. If errors were introduced during the transfer process, the firmware file is discarded and the upload must be repeated.
4. When the transfer has completed successfully, click the Change Version button to select the firmware version to load on the next system reboot.

Chapter 5

5 CLI Interface

This section describes the procedures for configuring and operating the RDL-3000 using CLI over a Telnet connection. The following procedures require a PC equipped with a Web browser, Ethernet port, and an Ethernet Cat-5e crossover cable for connection to the PoE power adapter. The IP address and subnet mask of the PC must be on the same subnet as the RDL-3000.

For example: IP address = 192.168.25.11, Net Mask = 255.255.255.0

5.1 Telnet Access

Use the following steps to establish a Telnet session with the RDL-3000. Refer to the *RDL-3000 User* Manual section *5: CLI Interface* for a complete description of the available commands.

1. On the PC, open a Telnet client and enter the unit IP address. The factory default IP is '192.168.25.2'.
2. Login to the RDL-3000 using the assigned username and password. The default username is 'admin', and the default password is 'admin'.

For example,

```
telnet 192.168.25.2
username: admin
password: admin
```

5.2 Command Summary

Online help is available for all commands, and the Tab key can be used for auto-complete functions. The following table lists all RDL-3000 commands available from root mode (default mode when you login).

Table 11: CLI - Command Summary

Command	Description
apply	Activate changes without overwriting saved configuration.
arp	Add a static ARP definition to the RDL-3000 ARP table.
chgver	Change default version of firmware and reboot.
clear	Clear commands.
del	Delete an ID.
enable	Enable an ID.
freq	Enter frequency ranges for autoscan and DFS.
generate	Create DSA key for SSH locally on RDL-3000.
get	Display the value of a statistic or parameter.
load	Load commands.
logout	End the current Telnet session.
new	Create a new ID.
ping	Send a ping message from the RDL-3000 system.
reboot	Reboot the RDL-3000.
reset	Reset the RDL-3000 statistics values.
save	Save the selected configuration settings.

Table 11: CLI - Command Summary

script	Generate a configuration script.
set	View/modify a system parameter value.
show	View system compound objects (e.g., configuration).
snmpcommunity	View/modify the SNMP community settings.
snmptrap	View/modify the SNMP trap settings.
upgrade	Upload a firmware binary image to the RDL-3000.
user	View/modify the user/password configuration.
whoami	Display login name for this Telnet session.

Table 12: CLI - Root Mode Commands

Command	Description
Tab	When entering a command, hit the Tab key at any time to perform auto-complete or view available options.
?	Use the '?' character to display help for any command or mode. Example: From the root directory, enter the following command to list all parameters that can be changed using the 'set' command: set ?
CTRL-Z	Return to root mode. Cancel command entry (alternative to backspace delete).
exit	Return to parent node / mode. all (exit all) Return to root mode.
logout	Terminate this telnet session. May be entered from any mode.

5.3 Command Set

5.3.1 apply

Use the ***apply*** command to activate changes to the configuration without overwriting the last saved configuration. This is equivalent to clicking the Apply button in the configuration screens.

apply <config>

config

Activate all changes to the configuration, but do not save changes permanently in the non volatile RAM.

Note: Use this command in combination with reboot to temporarily test changes to the configuration. For example:

5.3.2 arp

Use the ***arp*** command to manually (e.g., for wireless link aggregation). A maximum of two static (persistent) entries can be added to the table. Use the 'save config' command to permanently save changes to the static entries in the ARP table. Static entries loaded at boot time are recorded in the RDL-3000 system log.

arp <add> <del> <print>

add <**Host**> <**MAC**>

Add a new static entry in the RDL-3000 ARP table. Use 'save config' to save these entries permanently. A maximum of two static entries can be added to the table.

Host Host IP address. Must be same subnet as RDL-3000 unit.

MAC Host MAC address (e.g., 01-02-03-04-05-06)

del **<Host>**

Delete a static or dynamic entry from the ARP table. Also see command 'clear arptable'.

Host: Host IP address of ARP entry to be deleted

print

Print the ARP table. The * indicates manually entered values.

For example:

```
192.168.25.12# arp print
     192.168.25.1   at 00:05:5d:e0:5b:10
     192.168.25.22  at 11:22:33:44:55:66 *
Persistent MACs:
     192.168.25.22  at 11:22:33:44:55:66
     192.168.25.33  at 01:02:03:04:05:06
```

5.3.3 chgver

Use the ***chgver*** command to change the firmware version loaded when the RDL-3000 is rebooted.

chgver (no options)

Switch to the binary saved in the alternate version of firmware. This command works silently (no operator confirmation) and the RDL-3000 reboots immediately.

Note: Use 'get swver' to list the active and alternate versions of firmware.

5.3.4 clear

Use the ***clear*** command to delete all entries in a table.

clear <arptable> <freqlist> <idtable> <log>

arptable

Delete all static entries in the ARP table (refer to arp).

freqlist

Delete all frequency ranges from list (refer to 'freq' command).

idtable

Delete all IDs from the idtable.

log

Delete all messages from the log.

5.3.5 del

Use the ***del*** command to delete a specific ID or security key/certificate.

del <file> <folder> <id>

file <name> <mode>

Remove a file from runtime memory and non volatile RAM.

name <filename>

File name must be of the following format:

dsa_key_<mac>.pem	DSA key used for SSH.
rsa_key_<mac>.pem	RSA Key used for SSH.
ssl_cert_<mac>.pem	SSL Certificate.
ssl_key_<mac>.pem	SSL Key.
usr_wcert_<mac>.der*	User wireless certificate.
usr_wkey_<mac>.der*	User wireless key.
usr_wacert_<mac>.der*	User wireless authority certificate.

The <mac> portion is the MAC address of the board. For example: dsa_key_00-09-02-00-01-02.pem

mode <usr | factory | fips>

Specify the type of information to display.

usr	User entered files (default if type is not specified).
factory	Factory default files (requires hardware jumper selection).
fips	FIPS mode files.

id <id>

Remove a Service Group, Service, or Link table entry.

id Unique number for Service Group, Service, or Link.

folder <usr | factory | fips>

Remove all files from the specified table.

usr - User entered files (default).

factory - Factory use only.

fip - FIPS mode files.

5.3.6 enable

Use the ***enable*** command to enable a specific ID (Service Group, Service, or Link).

enable <id>

Enable a specific ID.

id Unique number for Service Group, Service, or Link.

5.3.7 freq

Use the ***freq*** command to configure frequency ranges when using autoscan or DFS.

freq <add> <clearall> <del> <print> <reload>

add <begin> <end>

Add a frequency range (up to 32 ranges).

begin - start frequency (MHz)

end - end frequency (MHz)

clearall

Delete all entries from the frequency list.

del <idx>

Delete a frequency validation range

idx - Frequency validation range index. Use 'print' to display IDs.

print

Print the list of frequency ranges.

```
Local frequency ranges:
index     begin     end
-------------------------------
0         5810.0    5820.0
1         5830.0    5835.0
```

reload

Reload the active list of frequency validation ranges.

5.3.8 generate

Use the **generate** command to generate a DSA key for use with SSH. The generated key is saved in runtime memory and non volatile RAM. *A system reboot is required to activate the new key.*

generate <sshkey>

The RDL-3000 generates a key using its internal encryption module.

sshkey <dsa | rsa>

dsa	Generate DSA key for SSH.
rsa	Generate RSA key for SSH.

5.3.9 get

Use the ***get*** command to view system parameters. Use the following general format to view a parameter.

get <*parameter*>

activeids

Number of active IDs (Services, Service Groups, and Links).

activelinks

Number of active Links.

dldpkt

Number of downlink discarded packets.

dloir <id>

Get the downlink offered information rate for the service.

dlrpkt

Number of downlink Rx packets.

dltpkt

Downlink Tx packets.

erxpkt

Number of Ethernet packets received.

erxpktd

Number of Ethernet packets received that were discarded.

ethsts

Speed and duplex settings for the Ethernet port.

etxpkt

Number of Ethernet packets transmitted.

gpssts

Status of the GPS device.

grpoir <id>

Get the Offered Information Rate (OIR) for the specified service Group.

id Index value of the Service Group

idenable <id>

Check the status of a Link, Service Group, or Service.

off = Link, Service Group, or Service is disabled (use enable to activate).

on = Link, Service Group, or Service is active (enabled).

lactive <id>

Link active status.

ldlblk

Downlink total blocks.

ldlbr

Downlink burst rate.

ldldblk

Downlink discarded blocks.

ldllfr

Downlink lost frames.

ldlrblk

Downlink retransmitted blocks.

ldlrssi

Downlink RSSI.

ldlsnr

Downlink SINADR.

llostc

Wireless link lost.

lrcon

Number of Services provisioned on this Link.

lrsrv

Number of links with registered service connections.

lscode

Link status code.

lulblk

Uplink total blocks.

lulbr

Uplink burst rate.

luldblk

Uplink discarded blocks.

lullfr

Uplink lost frames.

lulrblk

Uplink retransmitted blocks.

lulrssi

Uplink RSSI.

lulsnr

Uplink SINADR.

luptime

Link up-time.

mac

RDL-3000 MAC address.

radiotype

Radio type:

T502: 4.940 - 5.850 GHz (TDD)

regconn

Number of configured connections. (?)

regsrv

Number of configured Services.

regstations

Number of configured stations.

rffreq

RF frequency setting.

rfstatus

Status RF transmitter.

swver

List the downloaded firmware versions.

syncsts

Synchronization status.

sysstarttime

Time when the system started.

sysuptime

Time elapsed from reboot.

temperature

Internal temperature of the radio.

txpower

Current Tx power setting.

uldpkt

Uplink discarded packets.

uloir <id>

Get the uplink offered information rate (OIR) for the service.

ulrpkt

Uplink Rx packets.

ultpkt

Uplink Tx packets.

werxpkt

Wireless Eth Rx packets.

werxpktdis

Wireless Eth Rx discarded packets.

werxpkterr

Wireless Eth Rx packets with errors.

wetxpkt

Wireless Eth Tx packets.

wetxpktdis

Wireless Eth Tx discarded packets.

wetxpkterr

Wireless Eth Tx packets with errors.

5.3.10 load

Use the ***load*** command to install encryption keys into the RDL-3000.

load <file> <idtable> <script>

file <server IP> <filename> <usr | factory | fips> <tftp | sftp> <user> <password>

Load a key or certificate file from FTP server. The file is saved in non volatile RAM area. A reboot is required to activate changes to security data. The filename must be one of the following:

dsa_key_<mac>.pem	DSA key used for SSH.
rsa_key_<mac>.pem*	RSA Key used for SSH.
ssl_cert_<mac>.pem	SSL Certificate.
ssl_key_<mac>.pem	SSL Key.
usr_wcert_<mac>.der**	User wireless certificate.
usr_wkey_<mac>.der	User wireless key.
usr_wacert_<mac>.der	User wireless authority certificate.

The <mac> portion is the MAC address of the board.

For example: dsa_key_00-09-02-00-01-02.pem

Specify where to store the security information.

usr	User entered files (default if type is not specified).
factory	Default files.
fips	FIPS mode files (FIPS mode must be active).

For example:

load file 192.168.25.10 ssl_key_00-09-02-00-b2-73.pem usr tftp

idtable (no parameters)

Load all IDs from flash memory. This can be used to restore all IDs from the last saved configuration.

script <server IP> <filename>

Use this command to load the RDL-3000 configuration information from a file (created using script command) located on a remote TFTP server. The file must be located in the TFTP default directory. The 'save config' command must be used to save the loaded configuration in non volatile memory. A reboot may be required to activate the loaded configuration settings.

For example:

load script 192.168.25.10 RDL3000-Unit035-091121.cfg

5.3.11 logout

Use the ***logout*** command to terminate the current Telnet session.

logout

Terminate the current Telnet session (no parameters).

5.3.12 new

Use the ***new*** command to create a new Service Group, Service, or Link.

new <conn> <group> <link>

conn <id>

Create a new Service.

id - Specify a unique ID for this Service.

group <id>

Create a new Service Group.

id - Specify a unique ID for this Service Group.

link <id>

Create a new Link.

id - Specify a unique ID for this Link.

service <id>

Create a new Service.

id - Specify a unique ID for this Service.

5.3.13 ping

Use the ***ping*** command to initiate an ICMP ping command from the RDL-3000. This can be used to confirm network access to FTP/TFTP servers, syslog servers, etc.

ping <IP address> <Number of Packets>

IP address	IP address of target.
Number of Packets	Number of ICMP packets to send (1 to 16).

5.3.14 reboot

Use the ***reboot*** command to reboot the RDL-3000 firmware. Command the RDL-3000 to reboot. Entering 0 (zero) cancels reboot in-progress.

reboot <seconds>

seconds	Number of seconds to wait before rebooting.

Note: Use this command in combination with Apply to temporarily test changes to the configuration. For example:

set radio rf1	*Modify desired parameter*
reboot 600	*Schedule reboot in 5 minutes*
apply	*Activate configuration changes (without saving)*
(5 min later)	*RDL-3000 reboots and loads saved configuration*

5.3.15 reset

Use the ***reset*** command to zero the RDL-3000 statistics or ID table.

reset <stats>

Enter ID of specific Service, Service Group, or Link to be reset.

stats <id>

Reset statistics for a Service Group, Service, or Link.

id - Specify an ID to reset statistics only for that Service Group, Service, or L ink. Default is to reset all statistics.

5.3.16 save

Use the ***save*** command to copy edited parameter settings into non-volatile memory.

save [option] <Enter>

save <config> <defaultconfig> <idtable> <snmp>

config

Save Ethernet, wireless, and user configuration settings.

defaultconfig

Overwrite parameters with the factory default settings. The following settings are not affected: system name, location, details and contact, frequency list, SNMP configuration, Idtable.

idtable

Save current idtable settings.

snmp

Save current SNMP settings.

5.3.17 script

Use the ***script*** command to save a file containing a string of Commands that can be used to restore the current (active) configuration of the RDL-3000.

The file is saved in the TFTP default directory. The filename may be any name and extension valid for the TFTP server platform. It is recommended use a filename that uniquely identifies the RDL-3000 unit and the current date (e.g., Red-AD0023-080723.cfg). See 'load' command.

script <server> <name>

server - TFTP server IP address
name - Script file name

Note: User account groups, usernames and passwords are not saved by t he script command. Accounts must be created manually by a user using Telnet or a Web browser. The 'user' commands are interactive and can not be automated.

5.3.18 set

Use the ***set*** command to view and/or change a parameter. Use the apply command to activate changes made using the set command. Use the save command to permanently save changes (to non volatile RAM).

set <parameter>

activekey <1 | 2> <key>

Select the active options key (position 1 or 2). Advance notice is provided when a temporary options key is about to expire. If the temporary options key is selected as the active key, a message is logged and an SNMP trap is generated every 6 hours during the last five days of operation.

key - Optionally enter a new key value.

adaptmod <off | on>

Enable or disable the adaptive modulation function.

off - Disable

on - Enable

antgain <gain>

Set the antenna gain (used for DFS).

<gain> Enter gain in dBm.

autoscan <off | on>

Enable or disable the Autoscan function.

off - Disable

on - Enable

When enabled, the Subscriber automatically scans available channels to locate the current operating frequency.

bsmac <00:00:00:00:00:00 | mac_address>

If set to a no n-zero value, the subscriber is allowed to c onnect only to this sector controller with this MAC address (may use '-' or ':' for separators).

bsporten <id> <off | on>

Enable and disable sector controller Ethernet port.

id - ID of port

off - Disabled

on - Enabled

buzzer <off | on>

Enable or disable the audible alignment buzzer.

off - Disable

on - Enable

When enabled, the rate of the tone is proportional to the receive signal strength (faster rate = stronger signal).

chsize <bandwidth>

Enter the channel bandwidth (enabled by options key).

bandwidth Enter bandwidth in MHz (e.g., 20).

congid <id> <gid>

Assign a Service Group to this Service.

id - Service ID number.

gid - Service Group ID number.

conlid <id> <lid>

Assign a Link to this Service.

id - Service ID number.

lid - Link ID number.

conpri <id> <0 - 7>

Service default priority.

convid <id> <1 - 4095>

Set or show Service VLAN ID

id - Service reference ID number.

conviden <id> <off | on>

Enable or disable VLAN connections.

id - Service ID number.

on - VLAN is enabled.

off - VLAN is disabled.

dfsaction <none | txoff | chgfreq>

Select the mode of operation for DFS.

None (0): The DFS function is disabled.

Tx Off (1): Transmission is immediately disabled when radar signals are detected. This action is recorded in the message log and an SNMP trap message is sent (if SNMP enabled).

Chg Freq (2): Relocate transmission to an alternative frequency immediately when radar signals are detected. This action is recorded in the message log and a trap message is sent (if SNMP enabled).

dlcir <id> <50 - 50000>

Service downlink committed information rate (CIR) (Kbps).

id - Service ID number.

dlminrate <id> <1 - 54>

Link minimum downlink uncoded burst rate (Mbps). Entry values are dependent on the channel bandwidth (chsize).

id = Link ID number.

dlpir <id> <50 - 50000>

Service downlink peak information rate (PIR) (Kbps).

id - Service ID number.

dlrate <id> <6 - 54>

Link maximum downlink uncoded burst rate.

id = Link ID number.

dlratio <20-80>

Set the downlink ratio.

encmode <0 - 4>

Set the encryption mode. The same encryption level must be selected on communicating systems.

0 - Disable

1 - Not used

2 - AES 128

3 - AES 192

4 - AES 256

ethmode <auto | 10hd | 10fd | 100 fd | 100hd>

Enter a value for the combined Ethernet speed and duplex.

auto - Auto-negotiate

10hd - 10Base-T Half Duplex

10fd - 10Base-T Full Duplex

100hd - 100Base-T Half Duplex

100fd - 100Base-T Full Duplex

fastreg <off | on>

Fast registration mode.

id - Service reference ID number.

fixframe <off|on>

Configure the fixed frame mode.

off - Use dynamic frames based on traffic patterns.

on - Wireless frames are fixed at the size specified in the **framesize** field.

framesize <size>

When Fixed Frame is enabled, enter the frame size (1 - 20 ms).

size - Enter the fixed frame size (ms).

gateway <ip>

Enter the IP address of the default gateway on this segment.

gmt <value>

Enter the time offset from GMT (e.g., -5 for EST).

grpcir <id> <50 - 50000>

Service Group Committed Information Rate (CIR) for downlink broadcast and multicast traffic.

id - Group ID number.

grppir <id> <50 - 50000>

Service Group peak information rate (PIR) (Kbps). Applies to uplink and downlink traffic.

id - Group ID number.

grppri <id> <pri>

Service Group default priority.

id - Group reference ID number.

pri - Group 802.1p priority setting (0-7).

grprate <id> <6 - 54>

Service Group maximum rate (Mbps). Applies to uplink and downlink.

id - Group reference ID number.

grpvid <id> <vid>

Display/set the value of the VLAN ID for this Service Group.

id - [id number]

vid - VLAN ID

grpviden <id> <off | on>

Display the status or enable/disable this Service Group.

id - [id number]

off - Disabled

on -Enabled

http <off | on>

Enable or disable the HTTP function. When disabled, the Web interface will not be available.

off - Disable

on - Enable

https <off | on>

Enable or disable the HTTPS function.

off - Disable

on - Enable

idname <id> <name>

View or modify the name associated with an ID.

id - ID for Link, Service, or Service Group.

name - Name (maximum 15 text characters).

ipaddr <ip> <mask>

Enter the IP address and subnet mask of the RDL-3000. Confirmation is required.

Example:

set ipaddr ip 192.168.100.10 mask 255.255.255.0

ldlpir <id> <50-50000>

Link downlink PIR.

id = Link ID number.

lulpir <id> <50-50000>

Link uplink PIR.

id = Link ID number.

maxdst <distance>

Maximum distance to a subscriber.

value - Distance (Km) to farthest subscriber.

maxtxpower <-10 - 25>

Enter the Tx power level (dBm). This setting is for the transceiver output only. The actual EIRP depends on the gain of the connected antenna. The maximum value is determined by the options key.

mgmtag <off | on>

Enable or disable the HTTPS function. See also **mgmvid**.

off - Do not use VLAN to identify management traffic.

on - Enable VLAN tagged management traffic. See **mgmvid**.

mgmvid <1 - 4095>

Specify Management VLAN ID. See also **mgmtag**.

vlan_id - Management VLAN ID.

netmask <mask>

RDL-3000 IP netmask in standard format.

For example: set netmask 255.255.255.0

optionskey <key> <1 | 2>

Enter the options key string followed by the key position (0 or 1). This command works silently to validate, save, and activate the key. Event messages are logged for each of these operations. Enter the 'show log' command to view event messages.

peermac <MAC>

MAC address of the communicating RDL-3000. Required for wireless encryption (e.g., *00:05:5d:e0:5b:10*

pskey <key>

Enter the encryption key to be shared between the sector controller and all subscribers in this sector. This is required only when encryption is enabled.

radio <off | rf1 | rf2 >

Enable or disable the radio transmitter.

off - Disable both radios

rf1: Use only radio 1 (SISO).

rf2: Use only radio 2 (SISO).

***IMPORTANT**: Version 1.xx operation is limited to port RF-1. Port RF-2 must be electrically terminated (connect antenna or RF terminating device) and must be weatherproofed.*

radius <ip | mode | port | retries | secret | timeout>

Configure the RADIUS server (allowed in FIPS mode).

The first parameter for all commands must be the radius server identifier (1 or 2):

ip <1 | 2> <IP address>

IP address of RADIUS server.

1 - Primary RADIUS server.

2 - Secondary RADIUS server.

For example: Set the primary RADIUS server IP address and then set the secondary RADIUS server IP address:

set radius ip 1 192.168.100.50

set radius ip 2 192.168.100.51

mode <1 | 2> <off | on>

Mode of RADIUS server.

off - Disable RADIUS server.

on - Enable RADIUS server.

port <1 | 2> < 1-9999 >

Listening port address on RADIUS server (default port is 1812).

retries <1 | 2> < 1-999 >

Maximum number for attempts to contact target RADIUS server.

secret <1 | 2> < text >

Password for RADIUS server. Must conform to security policy.

timeout<1 | 2> < 1- 90 >

Time to wait for response from RADIUS server (seconds).

regper <4 - 100>

The number of frames between registrations.

rffreq < 4.940.0 - 5875.0>

Center frequency (MHz) for the RF channel. Sites operating in close proximity should minimize interference by using a factor of the channel size for separation. For example, 20 MHz channels should have >20 MHz separation.

schcycle <1-20>

The period determines the amount of data to be sent on a Service group or Service during each scheduling cycle. Enter scheduling cycle (ms).

snmp < none | v2 | v3 >

Select the mode of the snmp agent and the version. This selection is exclusive (e.g., selecting v3 excludes support of v2c).

none - Disable the SNMP agent.

v2 - Enable SNMP v2c support.

v3 - Enable SNMP v3 support.

snmptraplink < off | on>

SNMP trap message for each Link-up and Link-down event.

off - Disable the SNMP trap message.

on - Enable the SNMP trap message.

snmptraps < off | on>

Enable or disable sending all SNMP traps.

off - Disable all SNMP trap messages.

on - Enable all SNMP trap messages.

sntp < off | on>

SNTP enable setting.

off - Disable SNTP protocol support.

on - Enable SNTP protocol support.

sntpip <ip>

Enter the SNTP server IP address. Valid only if sntp is enabled.

sntppoll <1 - 24>

Enter the SNTP polling interval in hours. Enter period in hours.

srvgid <id> <gid>

Assign a Service Group to this Service.

id - Service ID number.

gid - Service Group ID number.

srvlid <id> <lid>

Assign a Link to this Service.

id - Service ID number.

lid - Link ID number.

srvpri <id> <0 - 7>

Service default priority.

srvvid <id> <1 - 4095>

Set or show Service VLAN ID

id - Service reference ID number.

srvviden <id> <off | on>

Enable or disable VLAN connections.

id - Service ID number.

on - VLAN is enabled.

off - VLAN is disabled.

ssh <off | on>

Enable or disable the SSH function.

off - Disable

on - Enable

sstoss <id> <off | on>

Status of packet routing between SSs.

id - Link ID number.

off - Disable forwarding broadcast packets from SS to SS.

on - Enable forwarding broadcast packets from SS to SS.

srvgid <id> <gid>

Assign a Service Group ID to this Service.

id - Service ID number.

gid - Service Group ID number.

srvgid <id> <lid>

Assign a Link ID to this Service.

id - Service ID number.

lid - Link ID number.

srvpri <id> <pri>

Assign a priority to this Service.

id - Service ID number.

pri - Assign a priority (0-7).

srvvid <id> <vlan_id>

Assign a VLAN ID to this Service.

id - Service ID number.

vlan_id - Service VLAN ID.

srvviden <id> <mode>

Enable/disable VLAN for this Service.

id - Service ID number.

mode - off = Pass Through, on = VLAN tagged.

syncmode < none | int : internal | ext : external >

Enable/disable VLAN for this Service.

none - Synchronization is disabled.

int - Synchronization using internal clock (or GPS if available).

ext - Synchronize to PPS port input.

syncout < off | on >

Enable/disable synchronization port (PPS).

off - Synchronization port is disabled.

on - Synchronization port is enabled.

syncterm < none | 50 | 75 >

Enable/disable VLAN for this Service.

none - High impedance.

50 - Port termination impedance is 50 Ohms.

75 - Port termination impedance is 75 Ohms.

syscontact <text>

Enter contact descriptive for this unit. Enter up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

sysdescr <text>

Enter system description for this unit. Enter up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

sysloc <location>

Enter location description for this RDL-3000 location**.** Enter up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

syslog <off | on>

Syslog enable setting.

off - Disable syslog server protocol support.

on - Enable syslog server protocol support.

syslogip <ip>

Enter the syslog server IP address. Valid only if syslog is enabled.

sysmode <pmpsc | pmpss>

pmpsc - The sector controller (sector controller) begins transmitting automatically; sending poll messages to locate the remote subscribers (pmpss).

pmpss - Subscribers monitor the selected channel(s) until polled by the pmpsc (sector controller).

sysname <text>

Enter the name for this unit. Use any combination of up to 20 letters and numbers.

telnet <off | on>

Enable or disable the Telnet port. If the Telnet port is disabled, it will not be possible to use the CLI interface.

off - Disable

on - Enable

Changes to this field are effective only following reboot.

telnetport <1 - 65535>

Telnet port address

port - Limits for the telnet port are 22..79 and 81..65534 (default is 23).

Changes to this field are effective only following reboot.

ulcir <id> <50-50000>

Enter the uplink committed information rate for the service (Kbps).

id - [id number]

ulminrate <id> <6 - 54>

Link minimum downlink uncoded burst rate.

id - Link ID number.

ulpir <id> <50 - 50000>

Service uplink peak information rate (PIR) (Kbps).

id - Service ID number.

ulrate <id> <1-54>

Link maximum uplink uncoded burst rate.

id - Link ID number.

usrauthmode <local> <radius>

Set the user authentication mode. Specify local services, the RADIUS server, or both in combination.

local - use local authentication.

radius - Use the RADIUS server.

x509auth <off | on>

Enable or disable authentication.

off - Allow network registrations without authentication.

on - Require authentication using X.509 certificates.

5.3.19 show

Use the ***show*** command to display system statistics.

show <config> <conns> <groups> <files> <idtable> <links> <log> <snmp> <service> <stats>

config

Display system configuration information.

conns <id>

Display information for a Service. Default is to display all Services.

id ID of Service.

```
192.168.25.2(show)# conns 4
     196           Data A      Conn
     197          Voice A      Conn
```

files <run | usr>

Display the key and certificate files.

run - Display keys currently in use.

usr - Display the user keys and certificates (default).

groups

Display information for all Service Groups.

```
192.168.25.2(show)# groups
     128            Voice     Group
     129            Data     Group
```

idtable

Display information for all system IDs.

```
192.168.25.2(show)# idtable
      ID             Name     Type        Status
------------------------------------------------------
       4            Sub A      Link        Enabled
       5          Sub B     Link        Enabled
      10          Sub C     Link        Enabled
      15          Sub D     Link        Enabled
      128         Voice     Group       Enabled
      129         Data      Group       Enabled
      160         Data A    Conn        Enabled
      161         Voice A   Conn        Enabled
      162         Data B    Conn        Enabled
      163         Voice B   Conn        Enabled
      164         Data C    Conn        Enabled
      165         Voice C   Conn        Enabled
```

links

Display information for all Links.

```
192.168.25.2(show)# links
       4            Sub A     Link      Down
       5            Sub B     Link      Down
      10            Sub C     Link      Down
      15            Sub D     Link      Down
```

log

Display the system events log.

service

Show the list of enabled service connections.

```
192.168.25.2(show)# service 17
     174         service1     Conn
```

snmp

Display the SNMP configuration.

stats

Display available statistics.

5.3.20 snmpcommunity

Use the ***snmpcommunity*** command to configure SNMP community permissions.

snmpcommunity <add> <clearall> <default> <del> <print>

add <name> <rights>

Add a new SNMP community to the SNMP community table. The index value is assigned automatically. Up to eight community entries can be entered.

name

Enter the SNMP community name.

rights

Specify the rights for this community string. Where.

0: Deny read and write permission (enter zero).
r: Grant read access permission only.
w: Grant write access permission only.
rw: Grant read and write access permission.

clearall (no parameters)

Delete all SNMP parameters.

default <idx>

Set all SNMP parameters to factory default settings.

idx Specify single entry to be set to default (use 'print' command to display ids).

del <idx>

Delete the specified community entry.

idx	Specify single entry to be deleted (use 'print' command to display ids).

print

List all SNMP communities and associated permissions.

5.3.21 snmptrap

Use the ***snmptrap*** command to configure the SNMP trap message reporting.

snmptrap <off | on> <add> <change> <clearall> <del> <print>

add <ipaddr> <port> <identity>

Create a new SNMP trap. The index value is assigned automatically. Up to eight settings may be entered.

ipaddr	Enter destination IP address
port	Enter destination port address.
identity	v2: Enter associated SNMP community string. v3: Enter account username for authorization.

change <idx> [-p <port>] [-i <ip_add>] [-c <community>] [-u username]

Modify the specified SNMP setting.

idx	Index of the SNMP trap (use 'print' command to display ids).
-i <ip_add>]	Enter destination IP address.
-p <port>]	Enter destination port address.
-c <community>	Enter associated SNMP community string (SNMP V1 or V2).
-u <username>	Enter account username for authorization (SNMP V3 only).

clearall

Delete all SNMP parameters.

del <idx>

Delete the specified SNMP trap.

idx	Index of the SNMP trap to be deleted (use 'print' command to display ids).

linkupdown

Trap indicates when the wireless Link is lost and recovered.

Off - Enable link up/down trap.

On - Disable link up/down trap.

off

Disable all SNMP traps.

on

Enable all SNMP traps.

print

List all SNMP trap settings.

5.3.22 upgrade

Use the ***upgrade*** command to upload a new firmware binary file to the RDL-3000.

upgrade <ip addr> <file name> <user name> <password>

ip addr

IP address of the FTP/TFTP server.

file name

Name of the binary file to be uploaded.

user name

FTP account name (FTP server only).

password

FTP account password (FTP server only).

Notes:

1. TFTP: You must specify the TFTP server address and the full name of the binary file (including .bin extension). The firmware binary file must be located in the default directory of the TFTP server.

2. FTP: You must specify the FTP server address, account user name, account password, and the full name of the binary file (including .bin extension). The firmware binary file must be located in the default directory for the specified user account.

5.3.23 user

Use the ***user*** command to manage user accounts, passwords, and user Groups. When in user mode, only the <chgpasswd> field is available, since the user can change only their own password. The other commands are available only for members of the administrator Group.

The RDL-3000 supports administrator and user accounts. See Table 5: Web - Screens and User Access on page 39 for permissions associated with each group.

user <add> <attr> <chgpasswd> <del> <print>

add <username> <usertype>

Administrators can use this command to add new user accounts. Usernames may be 1 to 19 alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_), Passwords may be 8 to 15 alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_). The operator must confirm their own password and a password for the new account.

username	Enter name of new administrator or user account.
usertype	Specify the type of account being created.
user	User account.
admin	Administrator account.

attr <username> < none | MD5 | SHA > < none | DES | AES >

Choose the authentication method and privacy method to be used for SNMP v3 requests. An authentication method must be selected to enable usage of the privacy method. Only combination SHA authentication + AES privacy is valid in FIPS mode.

username - Account to setup for SNMP v3 authorization.

chgpasswd <user name>

Administrators can change the password of any account. Users can change only their own password. Users are prompted to enter new password information.

username	Account to be modified.

del <username>

Delete a user account.

username	Account to be deleted.

print

Display a list of user accounts.

5.3.24 whoami

Use the ***whoami*** command to display the username of the current Telnet session. This command is not available when logged in as administrator.

whoami

Display username for this Telnet session.

6 Diagnostics & Troubleshooting

This section provides basic diagnostic and troubleshooting procedures. If the system can not be restored to normal operation using the procedures in this section, contact your local Redline representative for assistance. Include the model name and serial number of the system in your communications.

6.1 Interface Connection Issues

Attempt to login to the RDL-3000 using a Web browser. The following table lists common troubleshooting tips for the web interface.

Table 13: Diag. - Web Interface Diagnostics

Symptom	Possible Problem	Solution
General Information screen is not displayed	Incorrect IP address and/or subnet mask.	Perform a ping test from the host computer command line. If the ping test is unsuccessful (timeout), then the problem may be the IP address is not correct. Perform a long reset to apply the default IP address (192.168.25.2) and subnet mask (255.255.255.0). Refer to section 0: Long Reset (Lost Password or IP) on page 118.
	Problems with host computer, or RDL-3000.	If the ping is successful, reset the RDL-3000 and/or reset the host computer.
	Host PC ARP table is not correctly configured	Run 'arp -d' whenever the RDL-3000 is replaced. Check that the subnet mask for the host PC matches the subnet mask of the RDL-3000. Verify that the host and the RDL-3000 are set for the same subnet and are not using a duplicate or reserved IP address.

6.2 Testing Configuration Changes

The operator can use the reboot and apply functions to test changes to the configuration that may result in loss of the wireless link. Use the following steps to test new setup values for a five minute period and then restore the last saved configuration.

1. Make all necessary editing changes to the configuration.
2. Issue the command 'reboot 300'. This will set a timer to reboot the RDL-3000 in five minutes (5 x 60 seconds). A longer or shorter time can also be specified.
3. Issue the 'apply' command to activate all edited changes.
4. If connectivity to the RDL-3000 is lost, wait 5 minutes for the unit to reboot automatically and restore the previous settings.
5. Use 'save config' to save these settings and 'reboot 0' to cancel the timed reboot operation.

6.3 Status Code Definitions

The PMP status code displays the current alarm conditions as a series of hexadecimal characters. The value '1' indicates the associated condition is active. All unused bits are set to zero. To determine the status, the hexadecimal number must be converted to binary notation. For example, if 'Radio Over Temperature' bit 1 and 'PLL Error' bit 4 were active, the status code value would be Hex '12' (binary 0001 0010).

Table 14: Diag. - PMP Status Code Bits

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	9	8	7	6	5	4	3	2	1	0

Table 15: Diag. - PMP Status Codes

Bit	Description
1	Radio temperature too high
4, 5, 6	PLL Errors
8	Firmware Error
16	No Ethernet packets received by the wireless MAC
17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28	MAC Internal Errors

6.4 Working with System Parameters

The RDL-3000 is a highly configurable communications device. This section describes how to view, modify, test, and save parameter settings.

6.4.1 Parameters Overview

The RDL-3000 maintains the following sets of parameters:

Runtime Parameters	Currently active system settings. These values are loaded from 'Saved Parameters' at system reboot.
Editing Copy of Parameters	These values are loaded from 'Saved Parameters' at system reboot. The operator can use the Web or CLI interface to modify these values. Activate changes by using the 'apply' function. Save changes permanently by using the 'save' functions.
Saved Parameters	These values are saved in non volatile RAM and are loaded at reboot. Use the 'save' function to overwrite the last saved settings with the current contents of the 'Editing Copy of Parameters'. A separate copy of Saved Parameters is maintained for each firmware version (Active and Alternative).
Factory Default Parameters	Load these settings to restore the RDL-3000 to a known state.
TFTP Server	The 'Runtime Parameters' can be saved to a file on a TFTP server. Settings are saved as CLI commands in a text file. Saved configurations can be loaded directly from a file.
Factory Default Parameters	Use this function to restore the RDL-3000 to a known state.

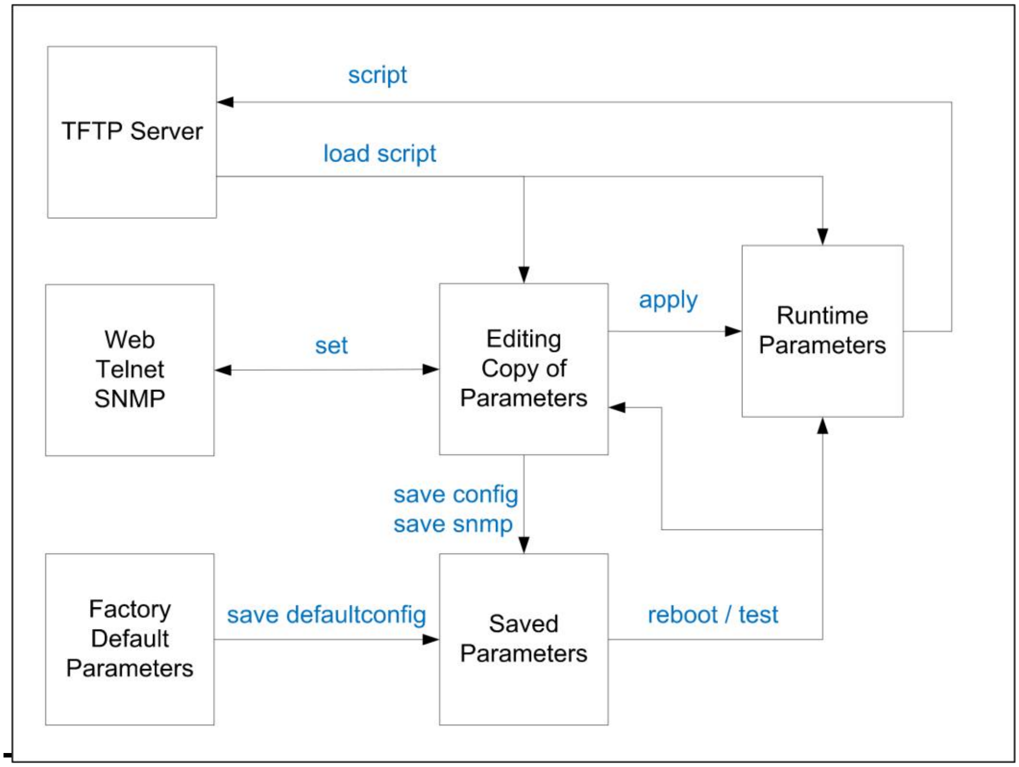


Fig. 60: **Diag**: **- Saving Parameters in Non Volatile RAM**

6.4.2 Factory Default Settings

Use the Web interface (click Factory Defaults in main menu) or the CLI interface (save defaultconfig) to restore the RDL-3000 to a known state.

Table 16: **Diag. - Factory Default Settings**

CLI Parameter	**Web Field**	**Option Key**	**Def Cfg Button Setting**
System			
syscontact	System Contact		Blank
sysdescr	System Details		Blank
sysloc	System Location		Blank
sysname	System Name		RDL-3000
Ethernet			
ethmode	Ethernet Mode		Auto
gateway	Default Gateway Address		192.168.25.1
gmt	Time Offset		+0.00
http	HTTP Enable		On
https	HTTPS Enable		N/C
ipaddr	IP Address		192.168.25.2
mgmtag	Mgmt Tag Enable		Off
mgmvid	Mgmt VID		0
netmask	IP Subnet Mask		255.255.255.0

Table 16: Diag. - Factory Default Settings			
CLI Parameter	**Web Field**	**Option Key**	**Def Cfg Button Setting**
snmp	SNMP		V2
snmpcommunity	SNMP Community Strings		'public', read 'private', read/write
snmptraplink	SNMP Traps		Off
snmptraplist	SNMP Trap List		Cleared
snmptraps	SNMP Trap Links		Off
sntp	SNTP Enable		N/C
sntpip	SNTP IP Address		192.168.25.1
sntppoll	Polling Interval		24
ssh	SSH		N/C
syslog	Sys Log Enable		Off
syslogip	Sys Log IP		192.168.25.1
telnet	Telnet Enable		On
telnetport	Telnet Port		23
userauthmode	User Authentication		Local
Wireless			
antgain	Antenna Gain		30
autoscan	Autoscan		Off
chsize	Channel Size		Key = No change No Key = 10 MHz
dfsaction	DFS Action	Y	Based on Key: No Key = chgfreq Required = chgfreq Not Req = none
dlratio	Downlink Ratio		No change.
pskey	Pre-shared key		No change.
fixframe	Fixed Frame Mode		Off
framesize	Framing Cycle		1
maxdst	Max. Distance		0
radio	Radio Enable		rf1
regper	Registration Period		16
rffreq	RF Freq. (MHz)		Based on key T502 = 5800
schcycle	Scheduling Cycle		2
syncmode	Synchronization mode		None
syncout	Sync port mode		None (port disabled)
syncterm	Sync port impedance		None (high)
sysmode	System Mode		Key = unchanged No Key = PMP SS
txpower	Tx Power		14
Misc.			
activekey	Active Key		No change
adaptmod	Adaptive		Off

Table 16: Diag. - Factory Default Settings			
CLI Parameter	**Web Field**	**Option Key**	**Def Cfg Button Setting**
buzzer	Buzzer		Off
dlcir	Service DL CIR		500
encmode	Encryption Type	Y	None
freq	Frequency List		No change.
grpcir	Service UL CIR		500
maxtxpower	Maximum Tx Power		14 dBm
optionskey	Options Key		No change
radius	RADIUS		Disabled
ulcir	Service UL CIR		500
ulpir	Service UL PIR		50 000
user	Users Management screen		admin / admin [2] user/user:
x509auth	X.509 Authentication		Off

1. SNMP v2 only in PMP mode; 2. All user-created accounts are deleted.

6.5 Long Reset (Lost Password or IP)

If the operator can not access the RDL-3000 management interface (unknown IP, username, and/or password), a long reset operation must be performed to provide access the unit. The long reset provides an opportunity to login to the RDL-3000 using the default IP, usernames and passwords. The long reset procedure requires local access to the RDL-3000 PoE adapter to power-cycle the RDL-3000, and a PC with an Ethernet cable and a Telnet client or Web browser.

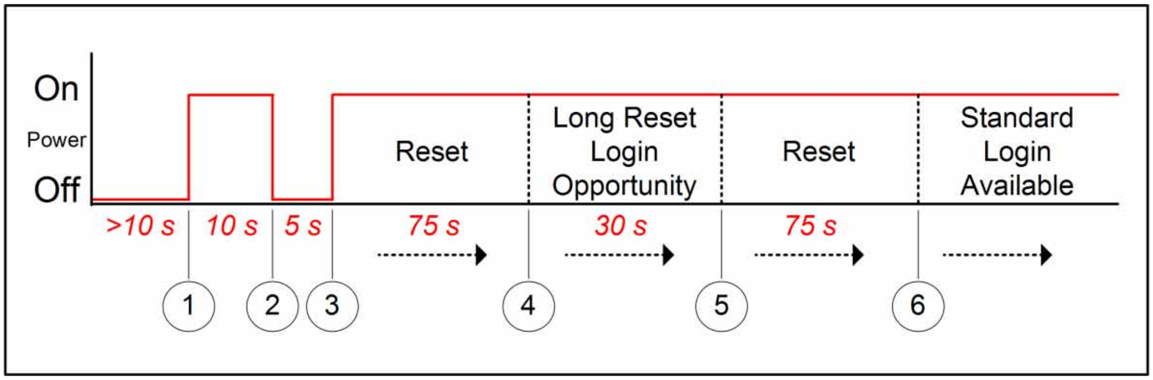


Fig. 61: Diag. - Recovering Lost IP Address

6.5.1 Long Reset Using Telnet

Use the following steps to gain access to the RDL-3000 management interface. It is recommended to use a clock display on the PC to ensure accurate timing.

Telnet

1. Power-off the RDL-3000 PoE adapter and remove the local network Ethernet cable. Use an Ethernet jumper cable to connect the PC directly to the PoE adapter DATA (INPUT) Ethernet port. Prepare the PC for Telnet access by opening a command prompt window on the PC and typing the following command (do not press the Enter key until step 6):

```
telnet 192.168.25.2
```

2. Restore power to the RDL-3000 PoE adapter and wait 10 seconds.

3. Power-off the RDL-3000 PoE adapter for 5 seconds.
4. Restore power to the RDL-3000 PoE adapter.
5. Wait 75 seconds, then press the ENTER key on the PC to start the Telnet session. When the login prompt appears, you have a window of 30 seconds to login using the default username (admin) and password (admin).

   If a login prompt does not appear, re-enter the Telnet command during the 30 second interval. If this is not successful, repeat steps 1 to 4 using an initial wait time of 70 to 90 seconds).

   Note: If the operator does not login during this step, the RDL-3000 reboots automatically after 30 seconds and is operational after an additional 75 seconds.
6. When login is successful, the admin and user accounts are reset to the factory default usernames and login values and all other user accounts are deleted. No other parameters are changed. All standard configuration commands are now available to the operator. If the IP was unknown, this can be now displayed and/or changed. Modify settings as required and reboot the RDL-3000 to exit from long reset mode.

Web

If using a web browser to access the RDL-3000, prepare the PC for by opening a Web browser on the PC and typing the following URL into the address bar:

http://192.168.25.2

Follow the steps for 'Long Reset Using Telnet', substituting the Web browser for Telnet.

6.5.2 Restore Default Passwords Only

Use this procedure if the unit IP address is known and it is desired only to restore the default usernames and passwords. All other configuration settings are preserved.

Telnet

1. Perform a long reset and use Telnet to login to the RDL-3000 using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).
2. Enter the command **reboot** to restart the unit. Do not enter any other commands.
3. Login to the RDL-3000 using the user-configured IP address and the default administrator username (admin) and password (admin).

Web

1. Perform a long reset and use a Web browser to login to the RDL-3000 using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).
2. Click **Configuration->System** to display the **System Configuration** screen.
3. Click on the **Reboot** buttons at the bottom of the screen to reboot the RDL-3000.
4. Login to the RDL-3000 using the user-configured IP address and the default administrator username and password (admin/admin).

6.5.3 Restore Factory Configuration

Use the following steps to restore the RDL-3000 to the factory configuration

Telnet

1. Perform a long reset and use Telnet to login to the RDL-3000 using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).

2. Enter the command **save defaultconfig**. The RDL-3000 will automatically reboot.
3. Wait for the reboot to complete (10 seconds) and login to the RDL-3000 using the default IP address (192.168.25.2) and the default administrator username (admin) and password (admin).

Web

1. Perform a long reset and use a Web browser to login to the RDL-3000 using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).
2. Click **Configuration->System** to display the **System Configuration** screen.
3. Click on the **Def Cfg** button at the bottom of the screen to reload the factory settings and automatically reboot the RDL-3000.
4. Wait for the reboot to complete (10 seconds) and login to the RDL-3000 using the default IP address (192.168.25.2) and the default administrator username (admin) and password (admin).

Chapter 7

7 Security

7.1 Overview

The Redline RDL-3000 provides a high level of security and reliability. Security features include wireless authentication using X.509 certificates, and wireless encryption using AES encryption. AES encryption is optional and may be purchased separately and enabled by loading an AES-enabled options key.

7.1.1 Authentication

The RDL-3000 supports the following authentication features:

- X.509 certificates for authentication
- Challenge-response mechanism during the link setup

7.1.2 Management Security

The RDL-3000 includes security mechanisms for device management.

- TLS 1.0 for HTTPS for secure Web access
- SSH v2 for secure command line operation
- SNMP v3 with AES support

7.1.3 Data Security

The RDL-3000 includes security mechanisms that provide sender authentication and security and integrity for data sent over the wireless interface. These features include:

- Wireless speed encryption for data traffic
- Messages encrypted and validated using AES in CCM (Counter with Cipher Block Chaining-Message Authentication Code)
- Separate keys for data traffic and key transport:
  - Diffie-Hellman for key setup
  - AES Wrap algorithm for key transport
  - Keys are changed at random intervals

AES (Advanced Encryption Standard) option is an encryption standard used worldwide to protect sensitive information. The AES cryptographic cipher uses a block length of 128 bits and key lengths of 128, 192 or 256 bits. As used in the United States, AES is a Federal Information Processing Standard (FIPS) -- FIPS Publication 197 describing cryptographic algorithms for use by U.S. Government organizations to protect sensitive, information. The AES block cipher has been ratified as a standard by National Institute of Standards and Technology of the United States (NIST).

7.1.4 Physical Security

The Redline RDL-3000 is enclosed in a weatherproof aluminum alloy case. The module's enclosure is sealed using tamper-proof labels. The security of the RDL-3000 system is further increased by the following factors:

- Stream cipher cannot be reverse-engineered -- even by destroying the equipment

- Key generation algorithm cannot be reverse-engineered -- even by destroying the equipment
- MAC address of a system cannot be changed without damaging the equipment
- Two communicating RDL-3000 systems detecting they have the same MAC address will immediately shut down

Important Security Guidelines:

1. Store encryption keys and certificate information in a secure location.
2. Always use secure transfer (e.g., SSH or SSL) when working with encryption keys and certificates.
3. It is recommended to use the RDL-3000 local Ethernet port to transfer encryption keys and certificates, or sftp if loading certificates or keys across an open network.

7.2 Wireless Authentication

Wireless authentication is a standard feature on all RDL-3000 systems.

7.2.1 Out-of-Box Operation

Wireless authentication is not supported out of box. Each RDL-3000 system to use wireless authentication must meet the following requirements:

1. The operator must generate and load X.509 certificate and key files
2. The wireless certificate and key files must be loaded into the user (usr) table. The files can only be loaded using the CLI interface (Telnet or SSH). Reboot the RDL-3000 to activate the certificate and key.
3. Configure and activate authentication services.

7.2.2 Generate X.509 Certificate and Key Files

Use a commercially available tool to create the required X.509 certificates and keys. The filenames used must comply with the following requirements:

usr_wacert_<mac>.der	X.509 authority certificate
usr_wcert_<mac>.der	X.509 certificate
usr_wkey_<mac>.der	Private key

7.2.3 Load Wireless X.509 Certificates and Keys

Use the following steps to setup wireless authentication:

1. Copy the certificate and key files to the default directory of a TFTP server.
2. Use the Command 'load' to copy the certificate and key files from the TFTP server to the RDL-3000.
3. Use the command 'show files usr' to verify the files have been successfully loaded.
4. Reboot the RDL-3000 to activate changes.

7.2.4 Enabling Authentication

The wireless X.509 certificate and key files must be loaded into the usr table and the RDL-3000 rebooted to activate the new keys before wireless authentication can be enabled. Use one of the following methods to enable authentication:

CLI: set x509auth on

Web: Configuration screen -> Wireless Security Configuration:

X.509 Authentication Enable ☑

Note: Save the configuration to activate changes.

Example

Load certificate files and key from the TFTP server at 192.168.25.10 to the RDL-3000 having MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.10 usr_wacert_00-09-02-01-C1-9A.der usr tftp
192.168.25.2# load file 192.168.25.10 usr_wcert_00-09-02-01-C1-9A.der usr tftp
192.168.25.2# load file 192.168.25.10 usr_wkey_00-09-02-01-C1-9A.der usr tftp
192.168.25.2# show files usr
    dsa_key.pem     size=672     md5=fa9bd7a1f465fd7e9fed30150b0608c4
    usr_wkey.der    size=1194    md5=1c5c5ddd0f08604a3b48cf41a8570557
    usr_wacert.der  size=1144    md5=ff0ce6923fc67a02d1e7bc6fa4856f94
    usr_wcert.der   size=999    md5=82b115af9dba510e5af8ce558e964265
192.168.25.2# reboot
    ...
192.168.25.2# set x509auth on
192.168.25.2# save config
```

7.3 AES Encryption

AES 128 bit wireless encryption is a standard feature on all RDL-3000 systems. AES 246-bit wireless encryption is an optional feature that may be purchased separately. AES encryption is not supported on RDL-3000 systems.

7.3.1 Out of Box Operation

AES encryption is not supported out of box. Each RDL-3000 system to be use AES encryption must meet the following requirements:

1. AES 128-bit:
   An options key enabled for AES 128-bit operation must be obtained (no charge), loaded on the RDL-3000, and be the currently active options key. AES 128-bit operation is a standard feature for RDL-3000 systems.
2. AES 256-bit:
   An options key enabled for AES 256-bit operation must be purchased, loaded on the RDL-3000, and be the currently active options key. AES 256-bit operation is a chargeable upgrade for RDL-3000 systems.

7.3.2 Enabling AES

Use the following steps to setup and enable AES encryption:

1. Obtain an AES-enabled upgrade options key for all communicating RDL-3000 systems.
2. Copy the new options key to each RDL-3000 and set this to be the active key.

   Refer to section 4.7.3: Product Options on page 87.
3. Choose the same AES encryption setting on all communicating RDL-3000 systems. A data link can be established only between systems with identical security settings.

   Web: Configuration screen -> Wireless Security Configuration: Encryption Type (None, AES 128, AES 192, AES 256)
4. Enter the shared key to be used for all communicating RDL-3000 units.
5. Save the configuration to active changes.

7.4 SSH for Secure CLI

SSH is a standard feature on all RDL-3000 systems. SSH provides secure access when using the command line interface (CLI) to manage RDL-3000 equipment. When SSH is required, TELNET (unsecured access) should be disabled. Use an SSH client (e.g., OpenSSH, Putty, etc) to access an RDL-3000 using SSH.

It is recommended that system operators generate a unique certificate and private-public keys, and load these on the RDL-3000 before using the HTTPS feature in a production environment.

7.4.1 Out-of-Box Operation

The RDL-3000 provides out-of-box use of the SSH interface. If no user-generated DSA key has been loaded on the RDL-3000, a temporary key is generated automatically.

> Each reboot, a new self-generated key (ssh_key<mac>.pem) is loaded into the user table. The self-generating key feature is disabled when the user loads a key in the user (usr) table or generate a key using the CLI 'generate' command.

Note: When using the self-generated key, a warning message may be displayed, based on the SSH client security settings (e.g., 'Warning: Potential Security Breach. The servers host key does not match ...'). The operator has full access to the secure CLI interface.

7.4.2 Enabling SSH

SSH is disabled by (factory) default. Use the CLI or Web interface to enable SSH:

Web interface:	*Configuration screen -> Ethernet: SSH Enable* ☑
CLI Command:	*set ssh on*

7.4.3 Loading an SSH Key File

Use the following steps to load user-generated X.509 certificate and key files:

1. Use a commercially available tool to create the required key file. The DSA key file must conform to the following:
   - Maximum key size is 2048 bits
   - Key filename must be in the following format:

     dsa_key_<mac>.pem
2. Copy the key file to the default directory on a TFTP server.
3. Use the CLI 'load' command to load the SSH DSA key into the user (usr) table. It is recommended to use the local Ethernet port when transferring encryption keys and certificates to the RDL-3000.
4. Reboot the RDL-3000 to activate changes.
5. Login to the RDL-3000 and verify the files have been successfully loaded.

Example

Use TFTP server at IP address 192.168.25.10 to load an SSH key file for the RDL-3000 with MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.10 dsa_key_00-09-02-01-C1-9A.pem usr tftp
192.168.25.2# show files usr
    dsa_key.pem    size=672     md5=fa9bd7a1f465fd7e9fed30150b0608c4
192.168.25.2#
192.168.25.2# reboot
```

7.4.4 SSH Key Generate Utility

Use the Command 'generate sshkey dsa' to create a DSA key and save this file in the user (usr) table. This key file is persistent through reboots. After executing the generate command, the RDL-3000 must be rebooted to activate the new key.

Example: Generate a new DSA key file.

```
192.168.25.2# generate sshkey dsa
```

```
192.168.25.2# reboot
```

7.5 HTTPS/SSL for Secure Web

HTTPS (SSL) is a standard feature on all RDL-3000 systems. HTTPS uses authentication and encryption to provide secure access over an unsecured network. When HTTPS is required, HTTP (unsecured access) should be disabled.

7.5.1 Out-of-Box Operation

The RDL-3000 provides out-of-box HTTPS (SSL) using an embedded X.509 certificate. The embedded certificate is identical for all shipped RDL-3000 equipment and is intended only to for initial system configuration. Use of the embedded certificate does not provide a secure solution.

When using the embedded certificate, warning messages may be displayed based on browser security settings (e.g., '*The security certificate presented was not issued by a trusted certificate authority. The security certificate presented was issued for a different website address.*) The operator has full access to the secure Web interface.

It is recommended that system operators generate a unique certificate and private-public keys, and load these on the RDL-3000 before using the HTTPS feature in a production environment.

7.5.2 Enabling HTTPS/SSL

HTTPS is disabled by (factory) default. Use the Web interface or CLI to enable HTTPS:

Web interface: Configuration screen -> Ethernet: HTTPS Enable ☑

Command: set https on

Save the configuration to active changes.

To access the RDL-3000 using HTTPS, the URL entered in the Web browser must specify 'https' or directly reference port 443.

Example: To access the RDL-3000 when HTTPS is enabled (default IP shown):

https://192.168.25.2/	*(Web browser defaults to port 443)*
http://192.168.25.2:443/	*(Operator specifies port 443)*

7.5.3 Loading HTTPS/SSL Certificates and Keys

Use the following steps to load user-generated X.509 certificate and key files:

1. Use a commercially available tool to create the required certificate and key files.

   The X.509 certificate file must conform to the following:

   - Maximum file size is 1400 bytes
   - Subject must match the access method (e.g., IP or name)
   - Filename must be formatted as follows:

     ssl_cert_<mac>.pem

   The SSL (RSA) key file must conform to the following:

   - Maximum 2048 bits.
   - Filename must be formatted as follows:

     ssl_key_<mac>.pem

2. Copy the key files to the default directory on a TFTP server.
3. Use the CLI 'load' command to load the RSA key and certificate. It is recommended to use the local Ethernet port when transferring encryption keys and certificates to the RDL-3000.

4. Use the command 'show files usr' to verify the files have been successfully loaded.
5. Reboot the RDL-3000 to activate changes to the key files. HTTPS is available when the system reboot is completed.

Example

Load HTTPS (SSL) key and certificate files from the TFTP server at 192.168.25.1 to the RDL-3000 having MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.1 ssl_cert_00-09-02-01-C1-9A.pem usr tftp
192.168.25.2# load file 192.168.25.1 ssl_key_00-09-02-01-C1-9A.pem usr tftp
192.168.25.2# show files usr
    dsa_key.pem      size=672       md5=fa9bd7a1f465fd7e9fed30150b0608c4
    usr_ssl_key.der   size=1194      md5=1c5c5ddd0f08604a3b48cf41a8570557
    usr_ssl_cert.der   size=1144      md5=ff0ce6923fc67a02d1e7bc6fa4856f94
192.168.25.2# reboot
```

Chapter 8

8 Appendices

8.1 Technical Specifications

Table 17: Spec. - RDL-3000 Technical Specifications

RF:	
T502 Radio:	
RF Band:	4.940 - 5.875 GHz (TDD) [1]
Rx Sensitivity:	-89 dBm @ 3 Mbps max.
Tx Power:	+25 dBm max. [1]
Center Steps:	2.5 MHz [2]
Channel Size:	5, 10, 20 MHz (firmware selectable) [1]
Rx Sensitivity:	-98 dBm @ 3 Mbps max., 5 MHz channel, BPSK
System Capability:	LOS, Optical-LOS, and Non-LOS > 50 dB Rx Dynamic Range Maximum Tx Power: 25 dBm (Ave. Max.) [1,3] Minimum Tx Power: -10 dBm Dynamic Frequency Selection (DFS) Automatic link distance ranging
Ethernet Data Rate:	Up to 100 Mbps average rate (20 MHz chan.)[4]
PoE Cable:	Up to 91.5 m (300 ft) [5]
Over The Air Encryption:	AES-128, AES 192, and AES-256
Node Authentication:	X.509 certificates
Network Attributes:	802.3x Ethernet flow control Automatic link ranging DHCP pass-through, Transparent bridge 802.1Q VLAN classification CIR/PIR Support
Modulation/Coding:	BPSK 1/2, QPSK 1/2, 16 QAM 1/2, 16 QAM 3/4, 64 QAM 2/3 and 64 QAM 3/4
MAC:	Time Division Multiple Access (TDMA) Automatic Repeat Request (ARQ) error correction (per link) Dynamic adaptive modulation (per link) Packet fragmentation, Concatenation
Network Services:	Transparent to 802.3 Services and applications
Duplex Technique:	Dynamic TDD (time division duplex) (per link)
Wireless Transmission:	OFDM (orthogonal frequency division multiplexing)
Network Service:	10/100 Ethernet (RJ-45)
System Configuration:	HTTP/HTTPS (Web) interface, SNMP, SSH, Telnet (CLI), TFTP
Network Management:	SNMP v2c or v3: standard and proprietary MIBs
Power Requirements:	Standard IEEE 802.3at PoE (25 W max.)
Operating Temperature:	-40 C to 60 C (-40° F to 140° F)
Dimensions/Weight:	290.7 mm x 268.4 mm x 63.5 mm (11.45 in x 10.57 in x 2.50 in)
Ingress Protection:	IP67
Weight:	2.7 Kg (6 lb) without bracket or antenna

Table 17: Spec. - RDL-3000 Technical Specifications

Storage Temperature:	-50 C to 70 C	
Compliance:		
	IEC, EN, and UL/CSA 60950	
	EN 301 489-1, EN 301 489-17	
	4.9 GHz:	Industry Canada RSS 111[6], FCC Part 90[6]
	5.4 GHz:	ETSI EN 301 893 Industry Canada RSS 210[6], FCC part 15[6]
	5.8 GHz:	ETSI EN 302 502, Industry Canada RSS 210[6], FCC part 15[6]
	OMAN-TRA	
		4.9-5.8 GHz R/0062/11 D080214

[1] Limited by regional regulations.

[2] Center frequency is dependent on region.

[3] Maximum power based on radio type, modulation, and coding.

[4] Actual Ethernet data throughput is dependent on: protocols, packet size, burst rate, transmission latency, link distance, and license key options.

[5] With surge arrestor installed.

[6] Pending.

Specifications are subject to change without notice.

Note: Refer to the *RDL-3000 antenna Guide* for a list of supported antennas and mounting brackets.

8.2 Classification: Services and Service Groups

8.2.1 Packet Classification at the Sector Controller

The RDL-3000 PMP deployment can be configured for use with VLAN tagged traffic, untagged traffic, or a combination these two types. Ingress packets received on the sector controller Ethernet port are classified according to the criteria in the following table. These descriptions do not include management traffic for the RDL-3000 sector controller or subscriber.

Table 18: **Spec. - Classification: Packet Received on SC Ethernet Port**

VLAN tag matches a Service Group VID	
Known unicast address	Priority: Preserve original 802.1p priority bits. Tag: Remove outermost matching VLAN tag. Forward: To destination only. Rate: Downlink rate of member Service for this subscriber.
Unknown unicast address:	Priority: Preserve original 802.1p priority bits. Tag: Remove outermost matching VLAN tag. Forward: All Service Group members. Rate: Two modulation steps below the lowest rate currently in-use across all active Services
Multicast or broadcast address:	Priority: Preserve original 802.1p priority bits. Tag: Remove outermost matching VLAN tag. Forward: All Service Group members. Rate: Downlink rate of this Service Group.
VLAN tag *does not match any Service* Group VID -- OR -- untagged packet	
Pass through service group not defined:	Discard packet.
Pass through service group defined --- AND --- known unicast destination	Priority: Service Group default priority. Tag: Unchanged Forward: Destination only. Rate: Downlink rate of member Service for this subscriber.
Pass through service group defined --- AND --- unknown address (all types)	Priority: Service Group default priority. Tag: Unchanged Forward: All Service Group members. Rate: Two modulation steps below the lowest rate currently in-use across all active Services.
Pass through service group defined --- AND --- multicast or broadcast address	Priority: Service Group default priority. Tag: Unchanged Forward: All Service Group members. Rate: Downlink rate of this Service Group.

Table 19: Spec. - Classification: Packet Received on SC Wireless Interface

Service Group type: Tagged	
Known unicast address --- AND --- destination is Ethernet port	Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To sector controller Ethernet port [1].
Known unicast address --- AND --- destination is subscriber	Forward: Retransmit packet unmodified over the wireless interface to the destination subscriber. Rate: Downlink rate for member Service on this subscriber.
Multicast or broadcast	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group [2]. Rate: Downlink rate for Service Group. --- AND --- Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To sector controller Ethernet port [1].
Service Group type: Pass through	
Known unicast address --- AND --- destination is Ethernet port	Forward: Packet unmodified to the sector controller Ethernet port [1].
Known unicast address --- AND --- destination is a subscriber	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group [2]. Rate: Downlink rate for member Service on this subscriber.
Unknown unicast	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group [2]. Rate: Downlink rate is two modulation steps below the lowest rate currently in-use across all active Services. --- AND --- Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To sector controller Ethernet port [1].
Multicast or broadcast	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group [2]. Rate: Downlink rate for Service Group. --- AND --- Forward: Packet unmodified to the sector controller Ethernet port [1].

Notes: 1 If sector controller Ethernet port is enabled, 2. If SS to SS Multicast enabled.

8.2.2 Packet Classification at the Subscriber

The RDL-3000 PMP deployment can be configured for use with VLAN tagged traffic, untagged traffic, or a combination these two types. Ingress packets received on the subscriber Ethernet port are classified according to the criteria in the following table.

Table 20: Spec. - Classification: Packet Received on SS Ethernet Port

VLAN tag matches a Service VID	
Known unicast	Priority: Preserve original 802.1p priority bits. Tag: Remove outermost matching VLAN tag. Forward: To sector controller. Rate: Uplink rate of Service matching this tag.
Unknown unicast:	Priority: Preserve original 802.1p priority bits. Tag: Remove outermost matching VLAN tag. Forward: To sector controller. Rate: Uplink rate of Service matching this tag.
Known multicast or broadcast:	Priority: Preserve original 802.1p priority bits. Tag: Remove outermost matching VLAN tag. Forward: To sector controller. Rate: Uplink rate of Service matching this tag.
VLAN tag *does not match any Service* VID -- OR -- untagged packet	
Pass through service group not defined:	Discard packet.
Pass through service group defined --- AND --- known unicast	Priority: Service Group default priority. Tag: Unchanged Forward: To sector controller. Rate: Uplink rate of (Pass through) member Service.
Pass through service group defined --- AND --- unknown unicast	Priority: Service Group default priority. Tag: Unchanged Forward: To sector controller. Rate: Uplink rate of (Pass through) member Service.
Pass through service group defined --- AND --- multicast or broadcast	Priority: Service Group default priority. Tag: Unchanged Forward: To sector controller. Rate: Uplink rate of (Pass through) member Service.

Notes: 1 If SS to SS Multicast enabled.

Table 21: Spec. - Classification: Packet Received on SS Wireless Interface

Member of Service Group type: Tagged	
Any type	Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To subscriber Ethernet port.
Member of Service Group type: Pass through	
Any type	Forward packet unmodified to the subscriber Ethernet port

8.2.3 VLAN (802.1Q) Field Definitions

The tag is located at the position used for the EtherType/Size field in untagged frames.

Table 22: Spec. - 802.1Q Tag Field

16 bits	3 bits	1 bit	12 bits
TPID	PCP	CFI	VID

Tag Protocol Identifier (TPID): 16-bit field set to 0x8100 identifies the IEEE 802.1Q-tagged frame. Located at the EtherType/Size field position (untagged frame).

Priority Code Point (PCP): 3-bit field IEEE 802.1p priority bits from 0 (lowest) to 7 (highest).

Canonical Format Indicator (CFI): 1-bit field. Value 0 indicates MAC address is in the standard format for Ethernet switches.

VLAN Identifier (VID): 12-bit field specifying the VLAN. The VLAN value may be 1 to 4094. Value 0 indicates the 802.1Q tag is specifying only a priority**.**

8.3 ID Mapping

The following table lists the ID ranges assigned for each provisioning type.

Table 23: RDL-3000 ID Ranges

Description	ID Range	Total
Links	4-127	123
Service Groups	128-159	31
Services	160-511	351

8.4 Regional Codes

A regional code is integrated into each options key. This feature restricts system operation to the frequencies allowed by regional regulatory statutes.

Options keys are unique to a specific RDL-3000 (keyed to MAC address). Available frequencies are limited to the radio type (e.g., 5.4 GHz).

Table 24: Spec. - Regional Identification Codes

Regions	Band	Radio	DFS/CBP Required [1]	Channel Size (MHz)	Channel Step (MHz)	Start - End [2] (MHz)
Region 00						
Lab Use Only	5.400-5.875	T502	User selectable	3.5	2.5	5470-5875
				5	2.5	5470-5875
				7	2.5	5470-5875
				10	2.5	5470-5875
				14	2.5	5470-5875
				20	2.5	5470-5875
Region 01						
ME CALA 5.8G	5725-5850	T502	Not required [3]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5730-5845
				14	2.5	
				20	2.5	5735-5840
Region 04						
CE 5.8G	5725-5875	T502	Not required [4]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5730-5870
				14	2.5	
				20	2.5	5735-5865
Region 05						
US 5.8G	5725-5850	T502	Not required [3]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5730-5845
				14	2.5	
				20	2.5	5735-5840
US 5.3G	5250-5350	T502	Required [3]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5260-5340
				14	2.5	
				20	2.5	5265-5335
Region 06						
IC 5.8G	5725-5850	T502	Not required [3]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5730-5845
				14	2.5	
				20	2.5	5735-5840
IC 4.9G	5250-5350	T502	Not required [5]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5260-5340
				14	2.5	
				20	2.5	5265-5335

Table 24: Spec. - Regional Identification Codes

Regions	Band	Radio	DFS/CBP Required [1]	Channel Size (MHz)	Channel Step (MHz)	Start - End [2] (MHz)
IC 5.3G	5250-5350	T502	Not required [5]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5260-5340
				14	2.5	
				20	2.5	5265-5335
Region 07						
AUS 5.8G	5725-5850	T502	Not required [3]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5730-5845
				14	2.5	
				20	2.5	5735-5840
Region 08						
GER 5.8G		T502	Required [6]	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5750-5870
				14	2.5	
				20	2.5	5765-5865
Region 09						
IN 5.8G		T502	Not required	3.5	2.5	
				5	2.5	
				7	2.5	
				10	2.5	5830-5870
				14	2.5	
				20	2.5	5835-5865

Notes:

1. Where DFS is required by regional regulations, this function is permanently enabled at the factory and can not be disabled by the installer or end-user.
2. Center frequencies.
3. FCC Part 15
4. ETSI EN302 502 v1.2.1
5. IC RSS-210
6. TKG § 55/EN302 502

8.5 FCC & IC Certified Antennas

8.5.1 4.94 - 4.99 GHz Radio: FCC & IC Antennas

This device has been designed to operate with the antennas listed in the following table, operating with the maximum specified gain settings.

Table 25: Spec. - FCC & IC Antennas: 4.94 - 4.99 GHz PTP Operation

Redline Order #	Application	Gain	Type	Max. Tx Power Setting (dBm)		
		(dBi)		5 MHz	10 MHz	20 MHz
A9014MTD	PTP	14	90°, 4.9-5.9 GHz, Panel, Dual Pol.	22	22	22
A6015MTD	PTP	15	60°, 4.9-5.9 GHz, Panel, Dual Pol.	22	22	22
A2308MFD	PTP	23	8°, 4.9-5.9 GHz, Panel, Dual Pol.	22	22	22
A2FT2906LTPD	PTP	29	6°, 4.9-5.9 GHz, Parabolic, Dual Pol.	18	22	22
A3FT3204LTPD	PTP	32	4°, 4.9-5.9 GHz, Parabolic, Dual Pol.	15	18	22

8.5.2 5.8 GHz Radio: FCC & IC Antennas

This device has been designed to operate with the antennas listed in the following table, operating with the maximum specified gain settings.

Table 26: Spec. - FCC & IC Certified Antennas: 5.8 GHz PTP Operation

Redline Order #	Application	Gain	Type	Max. Tx Power Setting (dBm)		
		(dBi)		5 MHz	10 MHz	20 MHz
A9014MTD	PTP	14	90°, 4.9-5.9 GHz, Panel, Dual Pol.	22	22	22
A6015MTD	PTP	15	60°, 4.9-5.9 GHz, Panel, Dual Pol.	22	22	22
A2308MFD	PTP	23	8°, 4.9-5.9 GHz, Panel, Dual Pol.	22 *	22	22
A2FT2906LTPD	PTP	29	6°, 4.9-5.9 GHz, Parabolic, Dual Pol.	19 *	19	19
A3FT3204LTPD	PTP	32	4°, 4.9-5.9 GHz, Parabolic, Dual Pol.	16 *	16	16

* 5 MHz channel set to the lowest/highest channel setting is allowed only at reduced power. See Table 27: Spec. - FCC & IC Certified Antennas: 5.8 GHz PTP Band Edge Operation.

Table 27: Spec. - FCC & IC Certified Antennas: 5.8 GHz PTP Band Edge Operation					
Redline Order #	Application	Gain (dBi)	Type	Max. Tx Power Setting (dBm)	
				5 MHz Channel Setting	
				5.730 GHz	5.845 GHz
A9014MTD	PTP	14	90°, 4.9-5.9 GHz, Panel, Dual Pol.	18	18
A6015MTD	PTP	15	60°, 4.9-5.9 GHz, Panel, Dual Pol.	18	18
A2308MFD	PTP	23	8°, 4.9-5.9 GHz, Panel, Dual Pol.	18	18
A2FT2906LTPD	PTP	29	6°, 4.9-5.9 GHz, Parabolic, Dual Pol.	18	18
A3FT3204LTPD	PTP	32	4°, 4.9-5.9 GHz, Parabolic, Dual Pol.	16	16

Table 28: Spec. - FCC & IC Certified Antennas: 5.8 GHz PMP Operation						
Redline Order #	Application	Gain (dBi)	Type	Max. Tx Power Setting (dBm)		
				5 MHz	10 MHz	20 MHz
A9014MTD	PMP	14	90°, 4.9-5.9 GHz, Panel, Dual Pol.	18	18	18
A6015MTD	PMP	15.5	60°, 4.9-5.9 GHz, Panel, Dual Pol.	17	17	17
A2308MFD	PMP	23	8°, 4.9-5.9 GHz, Panel, Dual Pol.	9	9	9

9 AN-80i Replacement with RDL-3000

This section describes issues related to replacing an in-service AN-80i sector controller with an RDL-3000.

9.1.1 Link IDs

The ID assignments for Links, Service Groups, and Services are restricted to specific ranges. The values are assigned automatically by the RDL-3000 when using the Web interface or CLI to create new entries.

If replacing an in-service AN-80i sector controller with an RDL-3000, it is recommended to save the current AN-80i configuration using the CLI 'script' command, and then load this configuration into the RDL-3000 replacement unit. The RDL-3000 will automatically map the Group and Connection ID numbers to valid Service Group and Service numbers. The AN-80i sector controller must have a maximum of 351 connections.

Table 29: **AN-80i Replacement - RDL-3000 ID Ranges**

Description	ID Range	Total
Links	4-127	123
Service Groups	128-159	31
Services	160-511	351

Table 30: **AN-80i Replacement - AN-80i ID Ranges**

Description	ID Range	Total
Links	4-63	59
Groups	64-95	31
Connections	95-511	416