

CONFIGURATION GUIDE

RADWIN 2000-PLUS FAMILY POINT TO POINT BROADBAND WIRELESS

Release 5.1.42

Doc.Rev 9

RADWIN

Table of Contents

Table of Contents.....	2
Chapter 1: Introduction.....	9
1.1. Scope of This Document.....	9
1.2. RADWIN 2000-Plus Family Overview	9
1.2.1. Radio Units	10
1.2.2. Method of Work.....	11
1.2.3. 1.2.3 Management Tools	12
1.3. Key features of the RADWIN 2000 Plus Family.....	12
1.4. What's New in Release 5.1.42.....	13
1.5. Notifications	13
Chapter 2: RADWIN Manager Overview	14
2.1. Scope of this Chapter	14
2.2. Installing the RADWIN Manager Application	14
2.2.1. Minimum System Requirements	14
2.2.2. Installing the Software	15
2.3. Initial Connection and Logon.....	15
2.3.1. Log-On with Local Connection	17
2.3.2. Log-On Changes from Previous Release	17
2.4. Other Log-on Options	18
2.5. Log-on Errors and Cautions.....	20
2.5.1. Unsupported Device	20
2.5.2. Incorrect IP Address	21
2.5.3. Incorrect Password.....	21
2.5.4. SNMP Issues.....	21
2.6. The Initial RADWIN Manager Main	22
2.7. Master ODU vs. Slave ODU	23
2.7.1. Define One Unit as an RT-A(HBS)	24
2.8. Setting RADWIN Manager Preferences.....	27
2.8.1. Preferences: Monitor	28
2.8.2. Preferences: Events.....	29
2.8.3. Preferences: Advanced.....	30
Chapter 3: Initial Link Configuration	32

3.1.	Scope of this Chapter	32
3.2.	Link Establishment.....	32
3.2.1.	Link Configuration Workflow.....	32
3.2.2.	Activating the RT-A(HBS).....	33
3.2.3.	Registering the RT-B(HSU)	43
3.2.4.	Basic Configuration for Operations.....	43
	RT-A(HBS).....	44
	RT-B(HSU).....	44
3.3.	Advanced Link Configuration	47
3.3.1.	Air Interface	47
	Throughput Mode.....	49
	Secured Sync Type.....	49
	Link ID	50
3.3.2.	Ethernet	51
	Link Configuration: MIMO Modes.....	51
	Link Configuration: Transmission Ratio.....	51
	Link Configuration: Maximum Information Rate	53
	VLAN and Quality of Service	53
3.3.3.	Changing the Link Band.....	53
3.3.4.	Configuring AES 256 Encryption Support	58
3.4.	Configuration with Telnet	60
3.4.1.	Telnet Access to Either ODU	60
Chapter 4:	Managing the Link	63
4.1.	Scope of this Chapter	63
4.2.	Link Tool Bar.....	63
4.3.	Link Configuration Window.....	64
4.3.1.	Link Configuration Tool Bar	64
	Backup and Restore.....	64
	Buzzer	64
	Refresh.....	65
4.3.2.	Link Configuration for RT-A(HBS) vs. RT- B(HSU)	65
4.4.	Configuration Tabs	66
4.4.1.	System	66
4.4.2.	Tx & Antenna.....	67
4.4.3.	Management	68
	IP Addresses.....	68
	IP Version	68
	Syslog server IP address	69

Trap Destinations	70
VLAN for Management	72
Protocols - LFF and SFF units.....	73
Protocols - RADWIN 2000 Alpha EMB / RADWIN 2000	74
Multuser Support under SNMPv3	74
Logging on as a SNMPv3 User	79
4.4.4. Hub Site Sync (RT-A(HBS) Only).....	80
4.4.5. Inventory.....	81
4.4.6. Security	82
Changing the Link Password	82
RADWIN Manager Community Strings.....	84
Editing SNMPv1 Community Strings	84
Editing SNMPv3 Passwords.....	84
Forgotten SNMPv1 Community String	85
Security Mode.....	86
4.4.7. Date & Time.....	88
4.4.8. Ethernet	90
Aging Time	90
Ethernet Ports Configuration	90
4.4.9. Operations	92
Reverting to Factory Settings	92
License Activation.....	93
Change ODU Mode	93
4.5. Deactivate RT-A(HBS).....	93
4.6. Deregister RT-B(HSU).....	93
4.7. Suspend a Deregistered RT-B(HSU).....	93
4.8. Reset the ODU	94
Chapter 5: Monitoring and	95
5.1. Retrieving Link Information (Get Diagnostics).....	95
5.2. Throughput Checking	97
5.3. Recent Events	99
5.4. Performance Monitoring	100
5.4.1. Obtaining Reports	100
5.4.2. More on the Thresholds.....	104
5.5. Manager Traps	105
5.6. Active Alarms	106
5.7. Other Diagnostic Aids.....	107
5.7.1. Link Budget Calculator	107









5.7.2.	Online Help	107
5.7.3.	Customer Service	107
Chapter 6:	Backup, Restore, and Upgrade	108
6.1.	Scope of this Chapter	108
6.2.	System & Site Backup.....	109
6.3.	Bulk Software Backup	109
6.4.	System & Site Restore.....	112
6.5.	Upgrading an Installed Link	113
Chapter 7:	VLAN Functionality.....	117
7.1.	Scope of this Chapter	117
7.2.	VLAN Tagging - Overview	117
7.2.1.	VLAN and Related Terminology	117
7.2.2.	VLAN Background Information on the.....	117
7.3.	Requirements	117
7.4.	VLAN Tagging	118
7.4.1.	QinQ (Double Tagging) for Service Providers	118
7.4.2.	VLAN Untagging	118
7.4.3.	Port Functionality	118
Ingress Direction	119	
Egress Direction	119	
7.5.	VLAN Configuration Using the	120
7.5.1.	Management Traffic and Ethernet Service Separation	120
7.5.2.	Configuration of VLAN Tagging for.....	121
Chapter 8:	Quality of Service.....	124
8.1.	Scope of this Chapter	124
8.2.	Prerequisites.....	124
8.3.	QoS - Overview	124
8.4.	Setting up the Link for QoS.....	125
8.4.1.	Preparing for QoS.....	125
8.4.2.	Assigning Queue Priorities	127
Chapter 9:	FCC/ISED DFS Considerations.....	128
9.1.	Scope of this Chapter	128
9.2.	FCC 5.4GHz Device Registration	128
9.3.	Registering the Device	128
9.4.	TDWR Table	132
Chapter 10:	Spectrum View	136
10.1.	Scope of this Chapter	136



10.2.	What is Spectrum View	136
10.3.	Who needs it	136
10.4.	Two Ways to Run Spectrum View	137
10.5.	Where is the Spectrum View Data stored	137
10.6.	Spectrum View Main Window.....	137
10.7.	Spectrum View Display Function.....	139
10.8.	Running Spectrum View	140
10.9.	Zooming in and out	142
Chapter 11:	Web Interface for Alpha EMB/Int units.....	144
11.1.	Scope of this Chapter	144
11.2.	Login	144
11.3.	Web UI Overview	145
11.3.1.	History.....	146
11.3.2.	Main icons.....	146
	Configure	148
11.3.3.	System.....	148
	General	148
	Coordinates.....	148
11.3.4.	Service (Client site only).....	149
	MIR (Maximum Information Rate)	149
	MIMO Modes.....	150
	QoS Configuration (Client site).....	150
	VLAN	151
	Quality Detection.....	157
11.3.5.	Tx & Antenna	159
	Air Interface	160
11.3.6.	Management	160
	Network.....	160
	Trap Destinations.....	162
	Protocol	164
	Syslog Server (Hub site only).....	164
	Users	166
	RADIUS User Authentication.....	168
	Advanced	173
11.3.7.	Hub Site Sync (Hub site only)	174
11.3.8.	Inventory.....	175
	Dying Gasp.....	175
11.3.9.	Security.....	177



SNMP Communities	178
Link Password	179
11.3.10. Date & Time	180
11.3.11. Ethernet	181
LAN Ports	181
Tx Ratio (Hub site only)	182
QoS Configuration (Hub site)	183
11.3.12. General (Hub site only)	185
11.3.13. WiFi	185
11.4. Events 	186
11.5. Spectrum 	188
11.6. Maintenance 	190
11.6.1. Upgrade	190
11.6.2. Backup	190
11.6.3. Restore	190
11.7. Diagnostics 	191
11.7.1. RSS Monitor	191
11.7.2. Ping	192
11.7.3. Trace	192
11.7.4. Diagnostics File	192
11.7.5. Sniffing	192
11.8. Operations 	193
11.8.1. Reset	193
11.8.2. Factory Default	193
11.8.3. Licenses	193
11.8.4. Change Mode	194
11.9. User Profile Icon 	194
11.10. Radio List	194
11.11. Right Pane	195
11.12. First-Time Use	196
11.12.1. Update Connection Parameters	197

11.12.2. Define one unit as the Master ODU	198
11.12.3. Activate the Alpha EMB/Int.....	199
11.12.4. Register the Client site Unit.....	199
Appendix A: Terminology	201
Appendix B: SSH CLI.....	210
Appendix C: Revision History	212
User Handbook Notice	213



Chapter 1: Introduction

1.1. Scope of This Document

This document shows how to configure RADWIN 2000-Plus Family radios.

For a detailed description of how to install RADWIN 2000-Plus Family radios, see the RADWIN 2000-Plus Family Installation Guide.

1.2. RADWIN 2000-Plus Family Overview

RADWIN 2000-Plus Family delivers up to 750 Mbps (depending on the specific model) in a point-to-point link and is the ideal choice for last mile enterprise connectivity and high-end applications that demand assured performance with guaranteed link bandwidth.

The RADWIN 2000-Plus Family has several models, each offering different characteristics. The main differences are shown below. Other differences are noted throughout this publication.

Table 1-1: RADWIN 2000-Plus Family Model Comparisons

Model Name	Max T-put (Mbps)	Input Voltage & Current	Form Factor	Enclosure Type	Oper. Temp	Hub Site Synchronization	AES 256 Support
RADWIN 2000 A-Plus	25	55VDC, 1A	Small (SFF)	IP67/Type 4	-35C to +60C	Ethernet, External GPS	No
RADWIN 2000 Alpha EMB	500	24-56VDC, 1A	Alpha Embedded	IP66/Type 4	-35C to +60C	Ethernet (HSS client only)	Yes ^b
RADWIN 2000 Alpha Integrated 5.x RADWIN 2000 Alpha Integrated 3.x	500	24-56VDC, 1A	Alpha Integrated	IP67/Type 4	-35C to +60C	Ethernet (HSS client only) Integrated GPS ^b	Yes
RADWIN Alpha Connectorized	500	24-56VDC, 1A	Alpha Connectorized	IP67/Type 4	-35C to +60C	Ethernet (HSS client only) Integrated GPS ^b	Yes
RADWIN 2000 C-Plus	250	48-57VDC, 1A	Large (LFF)	IP67/Type 4	-35C to +60C	Serial, Ethernet, External GPS	Yes ^a
RADWIN 2000 D-Plus	750	48-57VDC, 1A	Large (LFF)	IP67/Type 4	-35C to +60C	Serial, Ethernet, External GPS	No

a. (UNI and WPC regs only)

b. For new h/w of Alpha that contains GPS



Some options and models may not be available for your regulatory environment.

1.2.1. Radio Units

There are five types of outdoor radio units (ODUs):

- Large Form Factor (LFF) - With an integrated or external antenna.
- Small Form Factor (SFF) - As its name implies, this unit is smaller than an LFF unit but can also have an integrated or external antenna.
- RADWIN 2000 Alpha EMB **units** - Uses a smaller form-factor than that of the LFF or SFF. Can also have an integrated antenna, like the *Turbo Gain* antenna, which installs directly on the unit, or a separate, non-integrated, external antenna.
- RADWIN 2000 Alpha Integrated 5.x and RADWIN 2000 Alpha Integrated 3.x (integrated antenna) units - Uses a larger form-factor than that of the RADWIN 2000 Alpha EMB.
- Alpha Connectorized units - Uses its own form-factor. There is no integrated antenna, only external antennas are used.



With the exception of the frequency band, the RADWIN 2000 Alpha Integrated 5.x and RADWIN 2000 Alpha Integrated 3.x are identical in form factor and function. We will use the term RADWIN 2000 Alpha Integrated to refer to both units.

The RADWIN 2000 Alpha EMB and the RADWIN 2000 Alpha Integrated can be converted for use as an SU **PRO** EMB and SU **PRO** INT respectively. In addition, the Alpha Connectorized can be converted for use as an SU Connectorized.

Do this as follows:



1. Restore factory settings (recommended):
 - > RADWIN Manager: **Configuration -> Operations -> Restore Defaults**
 - > WebUI: **Operations -> Factory Default -> Restore**
 2. Verify that the unit to be converted is a “Slave ODU” (or Client). If not, change the ODU mode accordingly.
 3. Set the *Sector ID* the same as the *Sector ID* of the base station. This is called the *Link ID* in the 2000-Plus.
 4. Reset the unit.
-

1.2.2. Method of Work

- The radio units communicate with the service provider and users through PoE devices. The communication protocol for both the service provider and the users is Ethernet.

Although the link is symmetric, one unit is defined as a “Base Station” (RT-A(HBS)) and the other as a “Subscriber Unit” (RT-B(HSU)). Sometimes, these are also called the “Hub” and “Client” site. The differences are summarized here:

Table 1-2: RT-A(HBS) vs. RT-B(HSU)

RT-A(HBS)	RT-B(HSU)
Must be “activated” to work	Must be “registered” opposite an RT-A(HBS)
VLAN for services not available from the RT-A(HBS)	VLANs can be defined from the RT-B(HSU)
The “Dying Gasp” signal is not relevant.	Can emit a “Dying Gasp” signal, if it is active.

1.2.3. Management Tools

RADWIN Web Interface

The Web Interface enables you to carry out unit and/or link management functions using a Web browser. It is an easy way to rapidly configure and setup a link.

It may be used to -

- Set or change radio unit parameters in the field
- Establish a sector
- Check link parameters and make changes
- View the link Inventory
- Inspect the Recent Events logs

RADWIN Manager

The RADWIN Manager is an SNMP-based management application which manages a complete sector over a single IP address.



From RADWIN Manager release 11.0 and above, the Manager detects if the managed device supports the Web UI, and if so, redirects the user to use the Web UI instead of the RADWIN Manager.

1.3. Key features of the RADWIN 2000 Plus Family

- » Ethernet connectivity
- » Transparent to L2 protocols
- » Advanced OFDM & MIMO 2x2 for nLOS performance
- » Inter & intra site sync to reduce self-interference
- » Regulations supported - FCC/ISED/ETSI/WPC/MII/Universal (the product shipped to any given regulatory environment can only support those regulations)
- » Simple to deploy
- » Web Interface for link management
- » Fully integrated with RADWIN's family of solutions:
 - > Master ODU of RADWIN 2000-Plus Family can co-exist with other Master ODUs, as well as with base stations of all other RADWIN products
 - > Common RADWIN Manager
- » Separate uplink and downlink configurable Maximum Information Rate (MIR)

1.4. What's New in Release 5.1.42

- » IP & VLAN management on the same window
- » Enable / Disable maintenance without IP (for SU)
- »
- » Link Quality Indication

1.5. Notifications

Notifications consist of Notes, Cautions, and Warnings:



Caution: Risk of damage to equipment or of service degradation



Warning: Risk of danger to persons operating near the equipment



The purpose of a Note is to:

- Draw your attention to something that may not be obvious
 - Emphasize a special feature
 - Provide additional background
-

Chapter 2: RADWIN Manager Overview

2.1. Scope of this Chapter

This chapter shows you how to install the RADWIN Manager software on your managing PC, connect it to an operating radio unit and then log on. We then explain the use of the various objects on the RADWIN Manager main window.



From RADWIN Manager release 11.0 and above, the Manager detects if the managed device supports the Web UI, and if so, redirects the user to use the Web UI instead of the RADWIN Manager.

2.2. Installing the RADWIN Manager Application

2.2.1. Minimum System Requirements

Operating system specific PC resources required by the application are set out in [Table 2-1](#) below:

Table 2-1: PC Requirements for the RADWIN Manager Application

	Windows Version		
	XP Pro	Vista/7/8/10	
		32 bit	64 bit
Memory	512 Mb	1 Gb	2 Gb
Processor	P IV	P IV Dual Core	

Requirements common to all systems are:

- Hard disk: 1 GB free space
- Network: 10/100BaseT NIC
- Graphics: 1024x768 screen resolution with 16-bit color
- Any modern Web browser to view additional material or get help from the RADWIN website

2.2.2. Installing the Software

Any PC running the RADWIN Manager application can be used to configure a RADWIN 2000 Plus Family sector.

➤ **To install the RADWIN Manager application:**

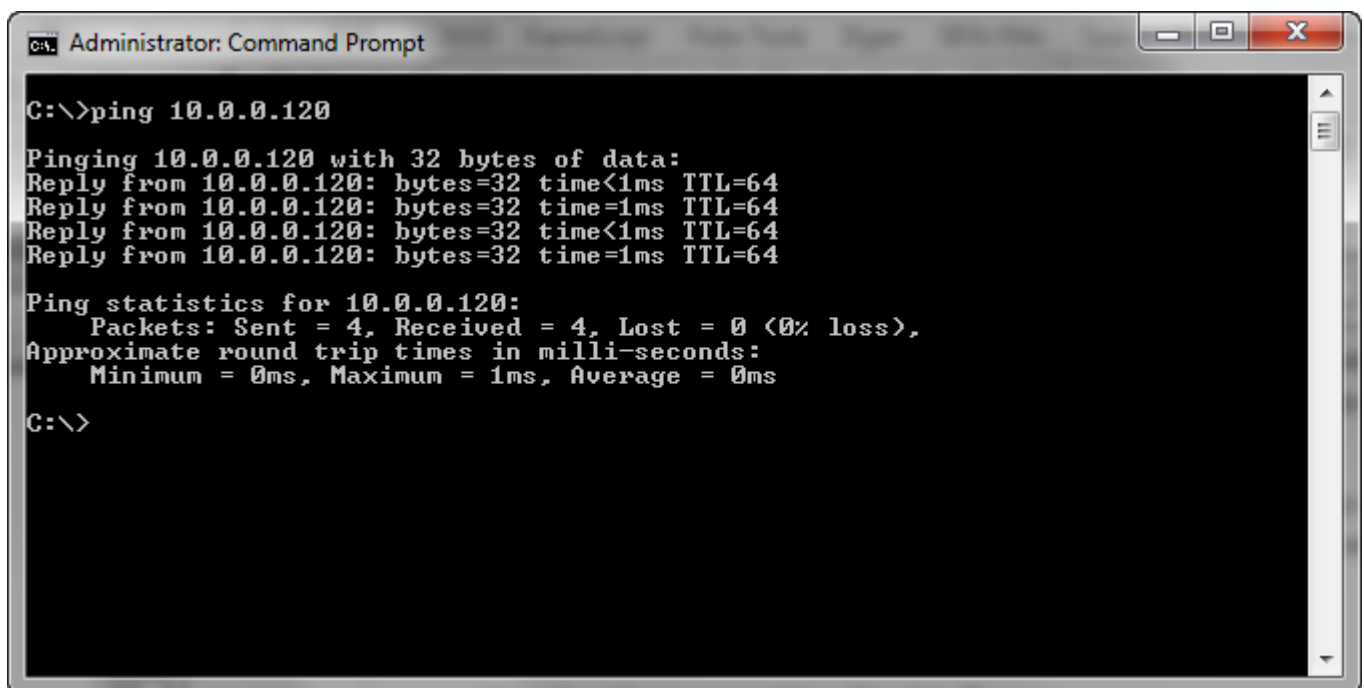
Download the RADWIN Manager application from the website, and follow the wizard's instructions to install the application.

2.3. Initial Connection and Logon

1. Check that you have connectivity to the radio. You can do this by opening up a command line session (Start|Run and then type, cmd). At the command prompt, type

```
ping
10.0.
0.120
```

You should see something like this:



```
Administrator: Command Prompt
C:\>ping 10.0.0.120
Pinging 10.0.0.120 with 32 bytes of data:
Reply from 10.0.0.120: bytes=32 time<1ms TTL=64
Reply from 10.0.0.120: bytes=32 time=1ms TTL=64
Reply from 10.0.0.120: bytes=32 time<1ms TTL=64
Reply from 10.0.0.120: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.0.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Figure 2-1: Pinging a radio unit

Any other response from ping means that the radio is not connected properly. You can try each one of these steps, then ping again:

- Check that you are using the correct IP address
(It may have been changed from the default value shown above)
- Check your Ethernet connection
- Check the physical connection of the radio in the field
- If you do not succeed using these steps, seek assistance from RADWIN Customer Service.

2. Dismiss the command line session.
3. Open the RADWIN Manager from the desktop icon, or click Start | Programs | RADWIN Manager | RADWIN Manager.

The Log-on dialog box appears.



Figure 2-2: Log-on window - Local Connection



Figure 2-3: Log-on window using an IP address

4. Log on with IP address 10.0.0.120 and default password *wireless*.
5. If the log-on was successful, you should see the initial RADWIN Manager screen (see [Figure 2-11](#)).

2.3.1. Log-On with Local Connection

Alternatively, you can log on using Local Connection (Figure 2-2) without having to change your Network Interface Card address.

- The Local Connection method uses broadcast packets to “discover” the attached radio unit.
- If you log on using Local Connection, but your physical connection is not local, then any configuration you carry out may affect other links in the network. Do not do this!
- Do not carry out this procedure using a multi homed managing computer also connected to a network. It will flood the network with broadcast packets. Further, it will throw any other links on the network into Installation or Inactive mode.



- As a precaution, default log-on over Local Connection is read-only mode. Check the Read/Write enable box to carry out installation procedures.
- Network log on (IP address to the radio unit) is recommended.

2.3.2. Log-On Changes from Previous Release

If you have a system that was upgraded from a release before 4.9.75, note that the User Type when logging on via SNMPv1 is no longer relevant, and the drop-down menu does not appear.

- If your User Type was *Installer*, use the same password that you used before.
- If your User Type was *Observer* or *Operator*, the password is reset to the default password (*wireless*), and the activities you can perform are the same as an Installer.
- This relates to logging on to the RADWIN Manager only.

If you are working with SNMPv3, user types are still relevant. Note the additional instructions for logging on below:

2.4. Other Log-on Options

The 2000-Plus supports many alternative log-on options.

- **SNMPv1 log-on:** Make sure the SNMP Version shows as V1 and enter the password. No other actions are needed.
- **SNMPv3:** Make sure that the SNMP Version shows V3. This can only be changed once you have already logged in to the RADWIN Manager (See [Protocols - LFF and SFF units](#)). Click on **Settings <<**, and the right extended window will open, as shown. Make sure V3 appears under SNMP version. Also, make sure that the correct Authentication method appears under SNMPv3/RADIUS Parameters (MD5 or SHA1, as set when SNMPv3 was configured). The username and password here don't normally need to be changed (See [Table 4-2, SNMPv3 Predefined Users](#) for a list of usernames and passwords). Click << or **Settings <<** to close the right window.



Figure 2-4: Extended log-on window

Figure 2-5 shows the difference between SNMPv1 and SNMPv3 at log-on time. You may choose the SNMP version. If your firewall blocks SNMPv3 messages and for security reasons

cannot be changed, use SNMPv1. To log on under SNMPv3, click Settings from the extended log-on window:

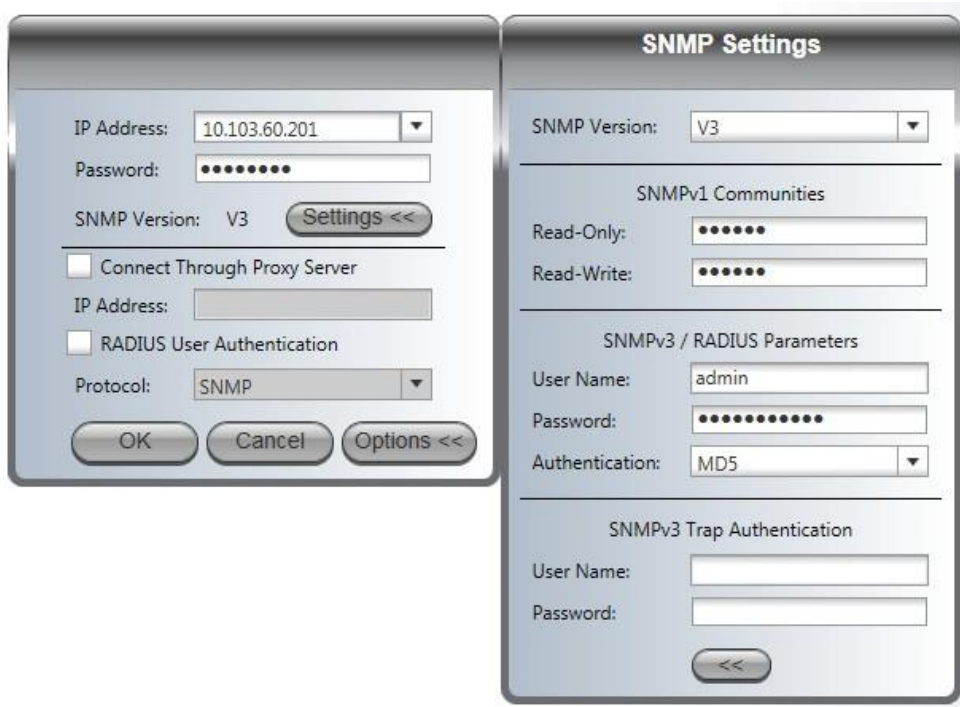


Figure 2-5: Log on window showing SNMP settings

- If you are using Trap Authentication, enter the username and password. The allocation and association of a trap address with a user is described in [Managing the Link](#).
- The Network Manager should change the default password as soon as possible, particularly if SNMPv3 is to be used.

Connect using RADIUS - If your system uses RADIUS authentication (Management -> RADIUS User Authentication. For more detail, see [RADIUS User Authentication](#)), place a checkmark here, make sure SNMP Version is V3, and select the protocol used (SNMP or Telnet).
- Under Password in the main window, use the standard password for the RADWIN Manager.
- Under the Username and Password for SNMPv3/RADIUS Parameters in the right extended window, use the username and password given to you by your network administrator. Note that your username will have certain permission levels according to its definition (see [RADIUS User Authentication](#) for more details).
When you are ready, click **OK**.

- **Connect Through Proxy Server:** If the unit is not directly connected to the managing computer or does not have a direct route, you can log on via a different entity whose IP address is known. If you wish to do this, click Options >>, and the lower extended window opens. This option works with SNMP V1 or SNMP V3.



Figure 2-6: Log-on Window: lower extended window "Options >>"

Once you have set all fields properly, click OK. The RADWIN Manager main screen (Figure 2-11) should appear.

2.5. Log-on Errors and Cautions

2.5.1. Unsupported Device

Attempting to connect to an unsupported device on an otherwise valid IP address (for example, a LAN printer) will result in the following error message:



Figure 2-7: Unsupported device message

2.5.2. Incorrect IP Address

If the IP address chosen is invalid or the sector is unreachable, the following error message will be displayed:



Figure 2-8: Unreachable device message

2.5.3. Incorrect Password

If you type an incorrect password in the Login window, the following message will be displayed:



Figure 2-9: Invalid user type or password

2.5.4. SNMP Issues

Invalid read/write community strings or SNMPv3 passwords, and incompatible versions or authentication versions, will result in a message similar to this:



Figure 2-10: SNMP Issues

- **Contact your IT department to unblock SNMP via the firewall**
- **Make sure you are using the correct SNMP version**
- **If you are logging in immediately after changing the authentication mode:**
 - Make sure that the mode chosen in the **Authentication** pull-down menu on the log-on window (see “[Log on window showing SNMP settings](#)”) is the same as the one you chose when you changed the authentication mode (See [Protocols - LFF and SFF units](#)).
- **To deal with lost or forgotten Community Strings:**
 1. Send an email request for to RADWIN Customer Service for an alternative key. Your email must include the radio unit serial number shown on the adhesive sticker on rear of one of your radio units.
 2. The reply will contain an alternative key, which functions as a temporary master Community String. Copy/paste the supplied alternative key to both the Read-Only and Read-Write fields in the log-on window ([Figure 2-4](#)). This gets you to the RADWIN Manager main window.
 3. To enter new Community Strings, See [Security](#).

2.6. The Initial RADWIN Manager Main Window

Upon successful login, the main window is displayed:

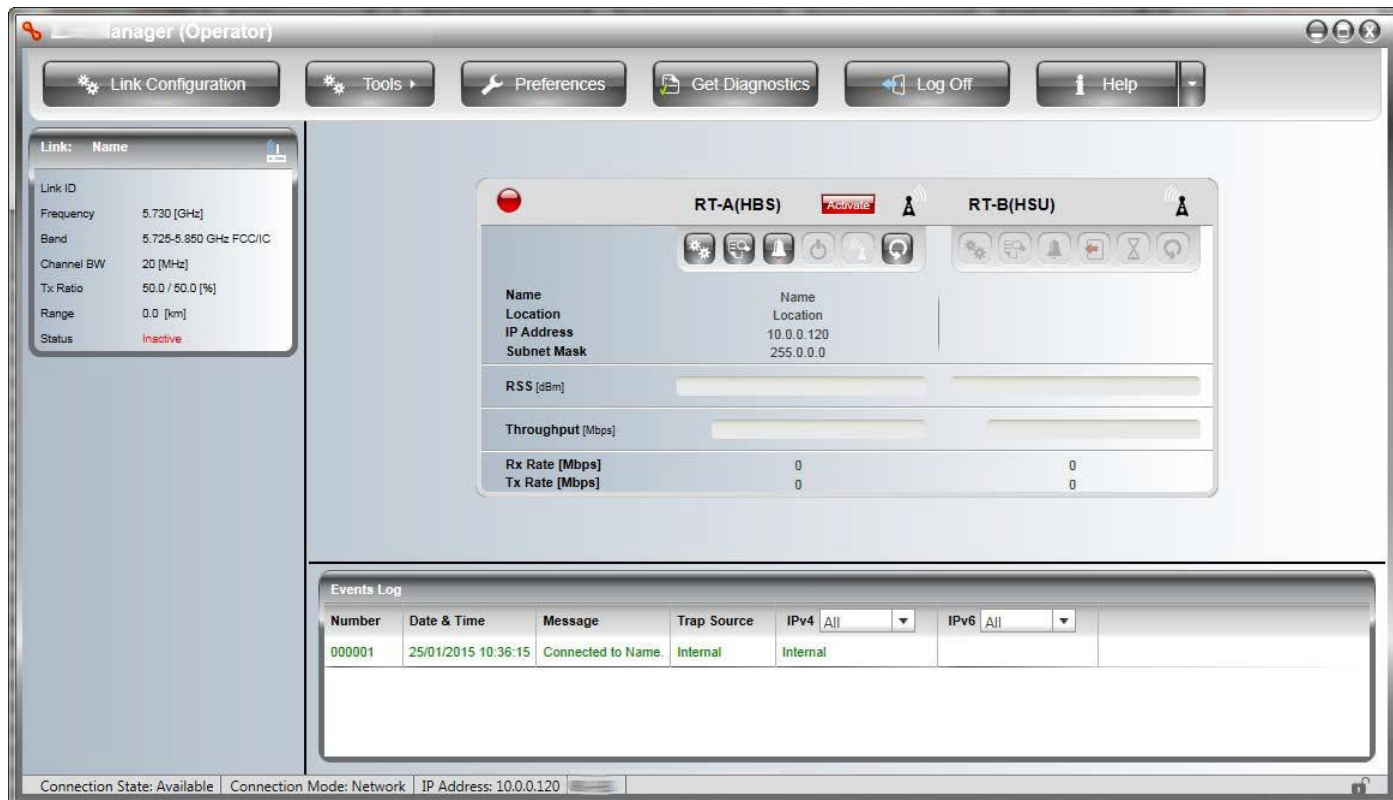


Figure 2-11: Main window prior to link configuration

2.7. Master ODU vs. Slave ODU

In a point-to-point link, one radio unit functions as the “dominant” unit. This unit is called either the Master ODU, the *Radio Terminal A* RT-A(HBS), or the Hub unit. The other unit is called the Slave ODU, the *Radio Terminal B* RT-B(HSU), or the Client unit. This terminology describes their relative roles.

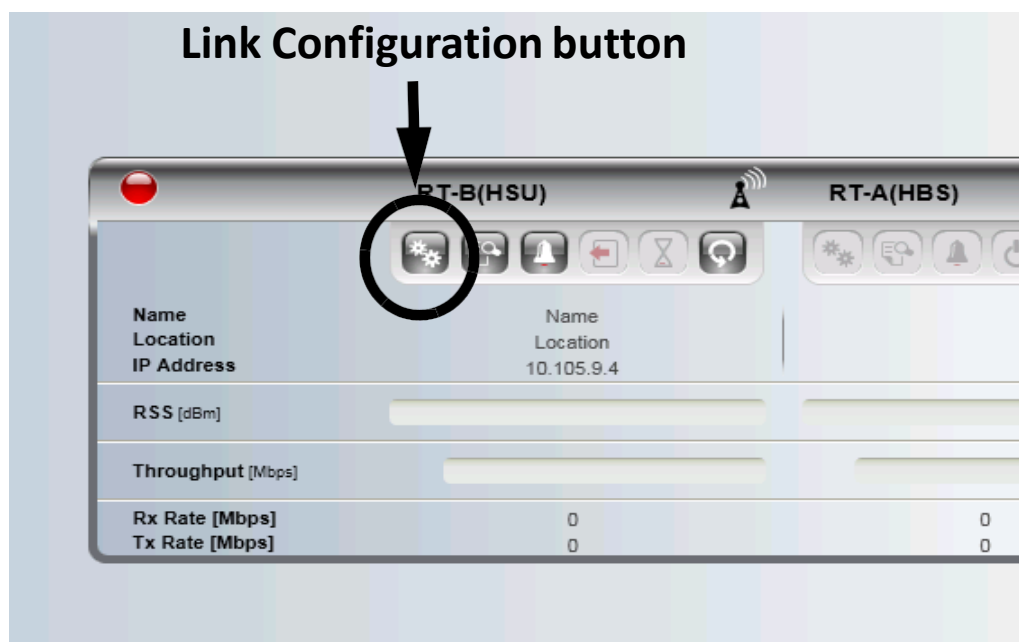
All 2000-Plus radios are shipped from the factory defined as Slave ODUs. You must re-define one as a Master ODU. For instructions on doing this, See [Define One Unit as an RT-A\(HBS\)](#).

Although any side can be a Master ODU or Slave ODU, take the following into consideration when determining which side will be defined as either:

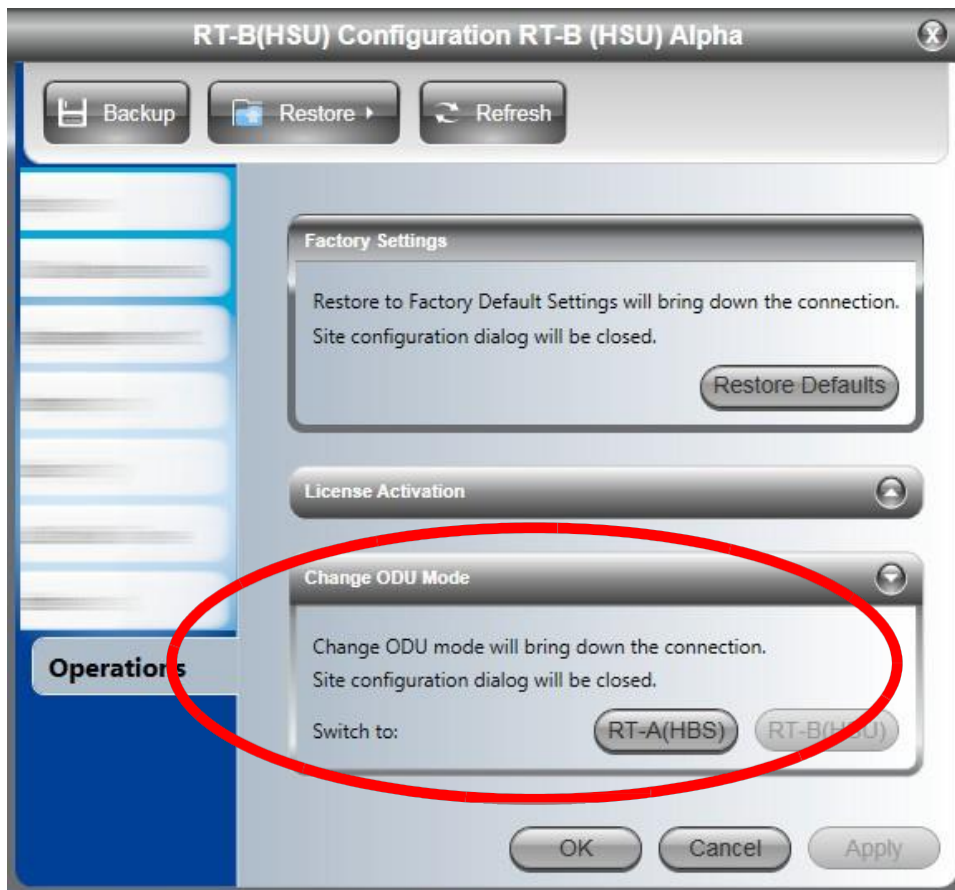
- > Hub Site Synchronization: Only Master ODUs can be synchronized with other units to avoid interference. You may require more equipment to fully implement Hub Site Synchronization. See the RADWIN 5000 *Hub Site Synchronization* application note for a description of hub site synchronization.
- > VLANs: VLANs can be defined from Slave ODUs only. See [Chapter 7, VLAN Functionality](#) for a description of how VLANs are defined.

2.7.1. Define One Unit as an RT-A(HBS)

1. Make sure that the managing computer is connected to the unit that will be defined as a Master ODU.
2. Install the RADWIN Manager and log on to the unit (see [Installing the RADWIN Manager Application](#)).
3. Click the Link Configuration button on the left unit in the central part of the main window.



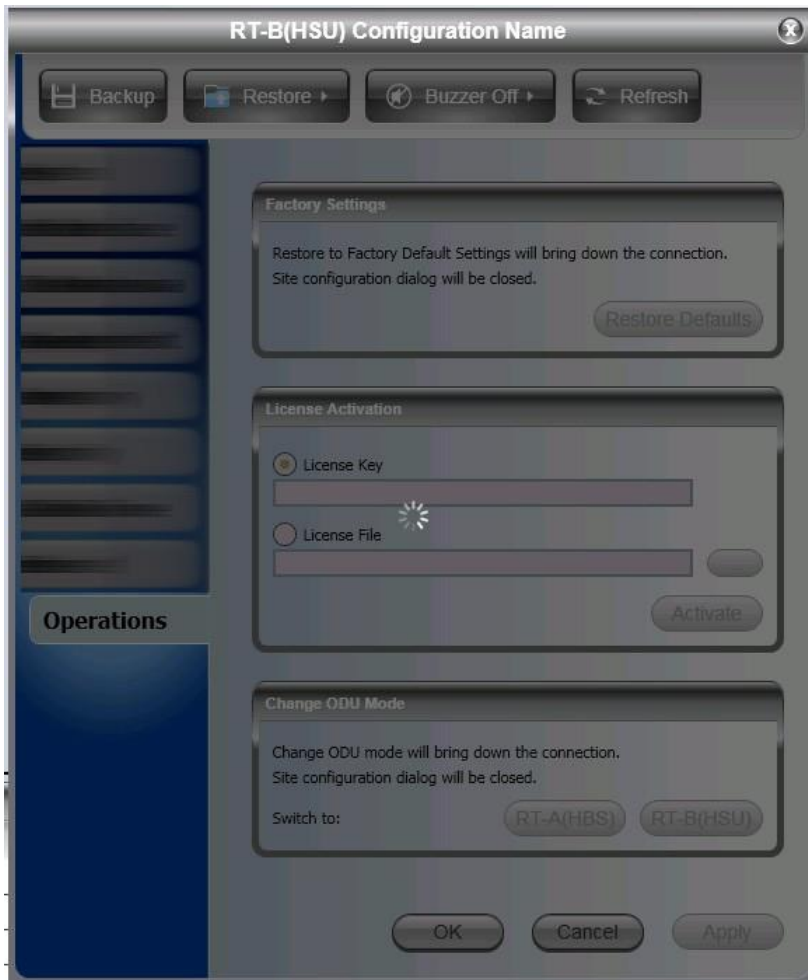
4. The Configuration window appears. Click Operations:



5. From Change ODU Mode, click RT-A(HBS).
6. A warning message will appear. Click OK.



7. The screen will be grayed-out while the system is re-configuring. No action is necessary on your part.



8. A warning message appears stating that connection to the unit was lost. This is normal, and of no concern. No action is necessary on your part.
9. After a few moments, the Main Window appears as follows:

The screenshot shows the RADWIN Manager software interface. At the top, there are menu buttons: Link Configuration, Tools, Preferences, Get Diagnostics, Log Off, and Help. Below these is a 'Site Surveyor' button. On the left, a 'Link' configuration panel shows details for a link with ID, Frequency (3.656 GHz), Band (3.000-3.700 GHz FCC/C), Channel BW (20 MHz), Tx Rate (50.0 / 80.0 %), Range (0.0 km), and Status (Inactive). The main area displays two device panels: RT-A(HBS) and RT-B(HSU). RT-A(HBS) is the Master ODU and RT-B(HSU) is the Slave ODU. Both show fields for Name, Location, IP Address, RSS [dBm], Throughput [Kbps], Rx Rate [Mbps], and Tx Rate [Mbps]. At the bottom, an 'Events Log' table shows a series of events:

Number	Date & Time	Message	Trap Source	IPv4	IPv6
000001	15/06/2015 14:09:02	Connected to Name.	Internal	Internal	
000002	15/06/2015 14:11:43	Read-Only mode activated.	ODU	Internal	
000003	15/06/2015 14:12:01	Device unreachable!	Internal	Internal	
000004	15/06/2015 14:12:39	Connected to Name.	Internal	Internal	
000005	15/06/2015 14:12:39	Read-Only mode deactivated.	ODU	Internal	
000006	15/06/2015 14:17:06	Read-Only mode activated.	ODU	Internal	
000007	15/06/2015 14:18:03	Device unreachable!	Internal	Internal	
000008	15/06/2015 14:18:08	Connected to Name.	Internal	Internal	

At the bottom of the interface, a status bar shows: Connection State: Available | Connection Mode: Network | IP Address: 10.105.9.4

The left unit is now defined as a Master ODU (or RT-A(HBS), the right unit as a Slave ODU (or RT-B(HSU)).

- From this point, you can activate, register, and then configure each unit. Instructions for doing this are found in [Chapter 3, Initial Link Configuration](#).
- However, we recommend you first set certain preferences when working with the RADWIN Manager.

2.8. Setting RADWIN Manager Preferences

The Preferences tabs appearing on both the RT-A(HBS) and RT-B(HSU) relate entirely to the way the Manager displays certain items for the connected unit. They are completely local to the managing computer. They are identical for both the RT-A(HBS) and RT-B(HSU).



Each managing computer (typically a laptop) should be set up with its own preferences.

2.8.1. Preferences: Monitor

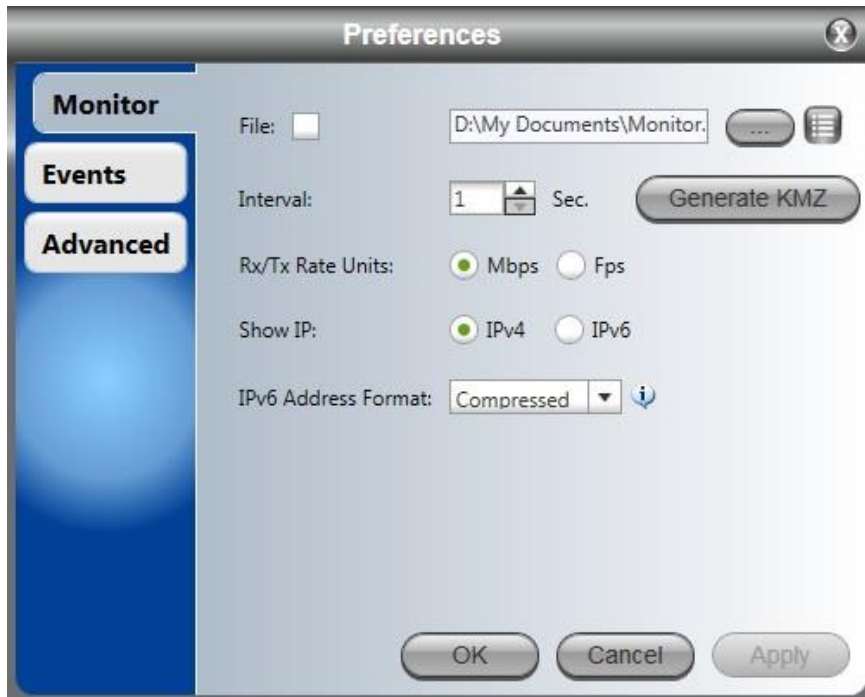



Figure 2-12: Monitor Preferences

File: Place a checkmark here to save traffic and identification information to the *Monitor file*. The content of the Monitor file is described in detail in [Chapter 5, Monitoring and Diagnostics](#).

Click the explorer button  to select the location of this file.

Click the select headers button  to select the categories of data to be saved in the Monitor file.

From the screen that appears, place a checkmark next to each category of data you wish to be saved in the Monitor file¹. Click OK to accept your choices.

Interval: Save the data every X seconds to the Monitor file (and the Utilization file if relevant). X can be an integer value only, and from 1 to 60. This file can be very large very quickly, so if you want to store data for a lengthy period of time, choose a large number.

The Generate KMZ button is not functional here and can be ignored.

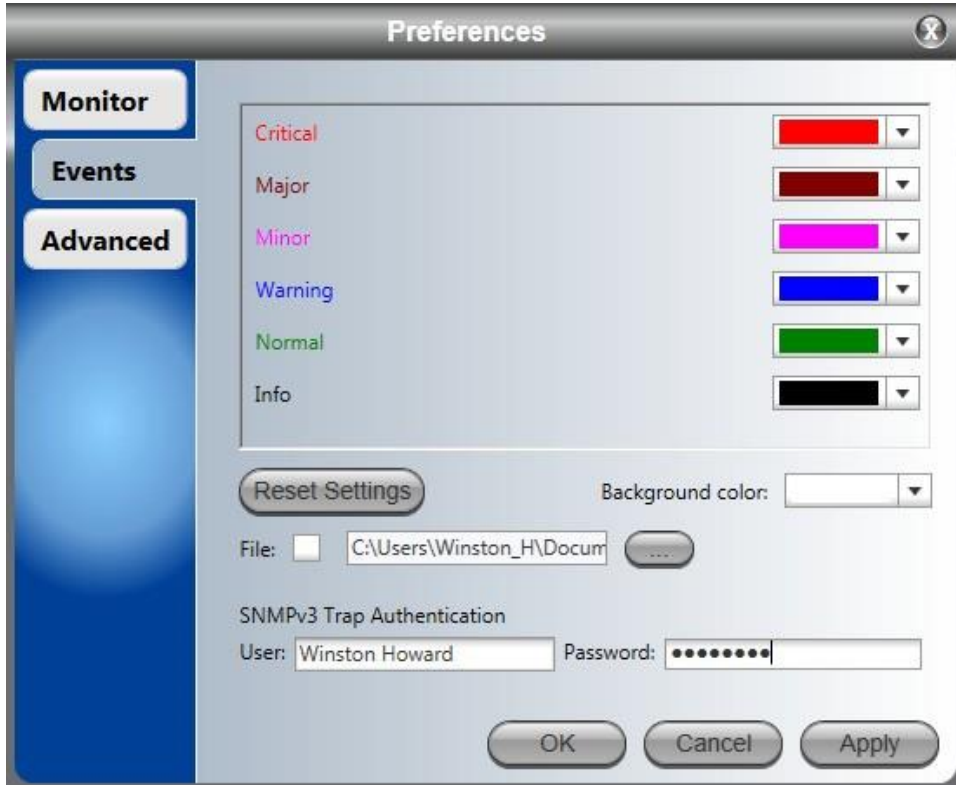
Rx/Tx Rate Units: Choose Megabits per second (Mbps), or Frames per second (Fps).

Show IP: Determine which IP address format to show on the main window for each unit: IPv4 or IPv6. The IPv6 option will work only if you have defined an IPv6 address for the unit (IPv6 is not available for the RADWIN 2000 Alpha EMB/RADWIN 2000 Alpha Integrated).

IPv6 Address Format: If showing IPv6 addresses, choose Compressed or Expanded.

¹ There may be categories listed that are not relevant for the specific radio model you are working with. Ignore those categories.


2.8.2. Preferences: Events



Critical ... Info: Choose your own color coding for the Recent Event display (see [Monitoring and Diagnostics](#)).

Reset Settings: Restore the color coding to the default values.

Background color: Choose the background color for the Recent Event display (see [Monitoring and Diagnostics](#))

File: Place a checkmark here to save a file for events logs and click the explorer button  to select the location of this file. These settings are per individual radio unit.

SNMPv3 Trap Authentication: Choose the username and password for SNMPv3 trap authorization. The SNMPv3 User and Password are relevant if you are using SNMPv3. In this, case trap messages are keyed to the username and password and not visible to anyone else. The preferences entered here relate to trap messages sent to the specified user, if specified, or to all trap messages.

2.8.3. Preferences: Advanced

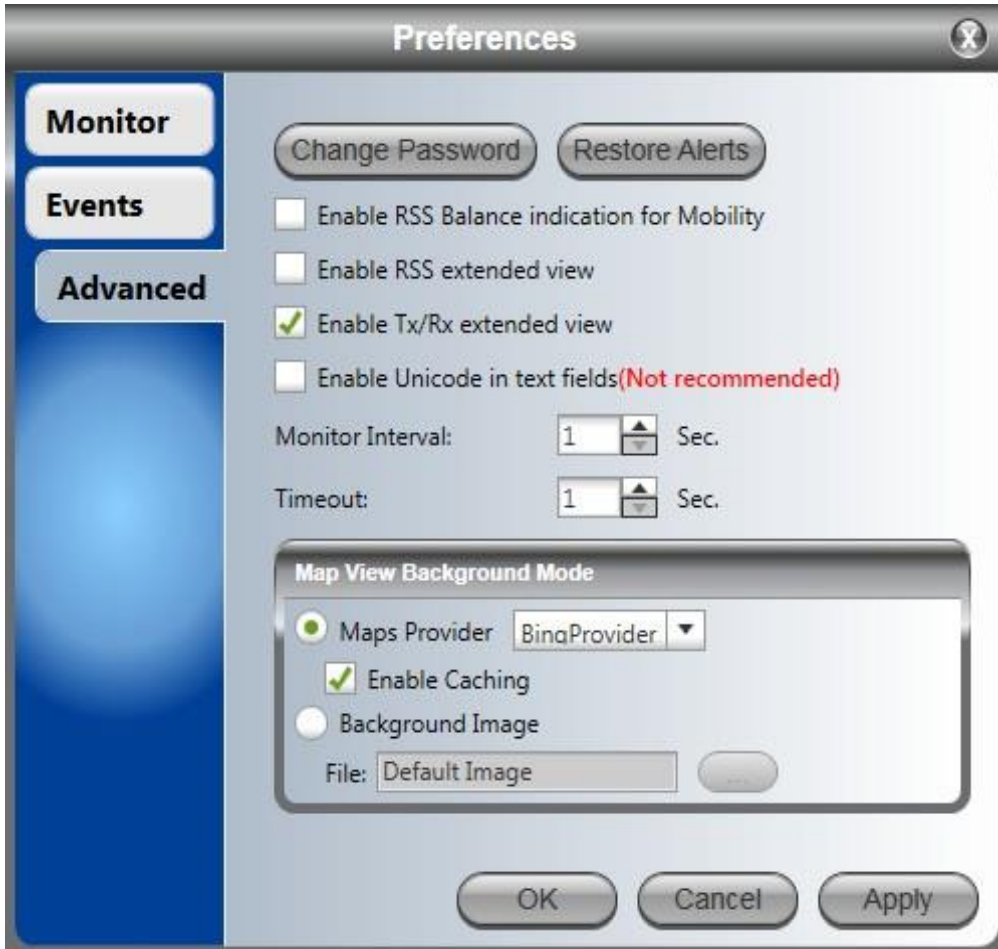


Figure 2-13: Advanced Preferences

Change Password: You may change your log-on password here from the default value.

Restore Alerts: Many alert messages in the RADWIN Manager have an option of the form “Do not show this message again”. These alert messages can be reverted to their default state (shown) by clicking this button. You will be asked to confirm:



Enable RSS Balance Indication for Mobility: This item is not functional for PtP links and may be ignored.

Enable RSS Extended View: Checking this box enables a dual chain view for RSS. When disabled, the RSS is shown as a single bar for each radio. The effect is visible immediately.



Figure 2-14: RSS Extended view enabled



Figure 2-15: RSS Extended view disabled

Enable Tx/Rx Extended View: Place a checkmark here to enable viewing the Rx and Tx rate of *each* LAN line attached to the unit. When disabled, the rate shown is an aggregate rate for both LAN lines.

This will appear in all cases but will only have meaning if your unit has more than one LAN line, and if they both are connected. See the RADWIN 2000-Plus Family Installation Guide for the external connections of the unit you are using.

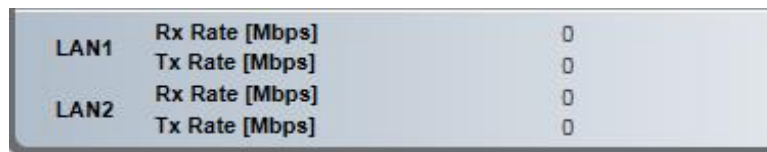


Figure 2-16: Tx/Rx Extended View enabled

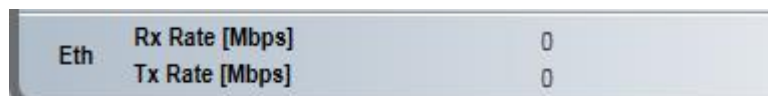


Figure 2-17: Tx/Rx Extended View disabled

Enable Unicode in Text fields: This allows you to write non-standard text in the various fields you use. We do not recommend this because it would be difficult or impossible to coordinate with systems and equipment that may not be able to detect this text, and you could therefore lose connections.

Chapter 3: Initial Link Configuration

3.1. Scope of this Chapter

This chapter covers the two phases of Link configuration:

1. Link establishment: Initial setup
2. Link maintenance: Fine tuning and special functions

Link establishment is typically a once-only task. Link maintenance is required for fine-tuning the link and configuring special features such as VLAN, Quality of Service and more.

3.2. Link Establishment

3.2.1. Link Configuration Workflow

As soon as power and network connections are supplied to the radio unit, it will commence transmitting and receiving packets related to management only - that is, no service traffic will be sent or received.

Activation: For the RT-A(HBS) to carry out service, it must be activated. Activation and Deactivation are affected quite simply by clicking a toggle button.

Discovery: Assuming that the radio unit intended as the RT-B(HSU) (Slave ODU) is mounted, aligned, and powered up, it will discover the RT-A(HBS) establishing a link for management only. At this point, the RT-B(HSU) may be managed over the air.

Registration: Having Identified the Link RT-B(HSU), the latter must be registered to the RT-A(HBS) to enable traffic between them.

Following registration, you can set separately,

- MIMO mode
- Transmission ratio between uplink and downlink

- Uplink and downlink Maximum Information Rate (MIR) in Mbps
- VLAN parameters
- Quality of Service parameters

In what follows, we assume that you are logged on to RT-A(HBS) on IP address as shown in the previous chapter. Here is the opening situation:

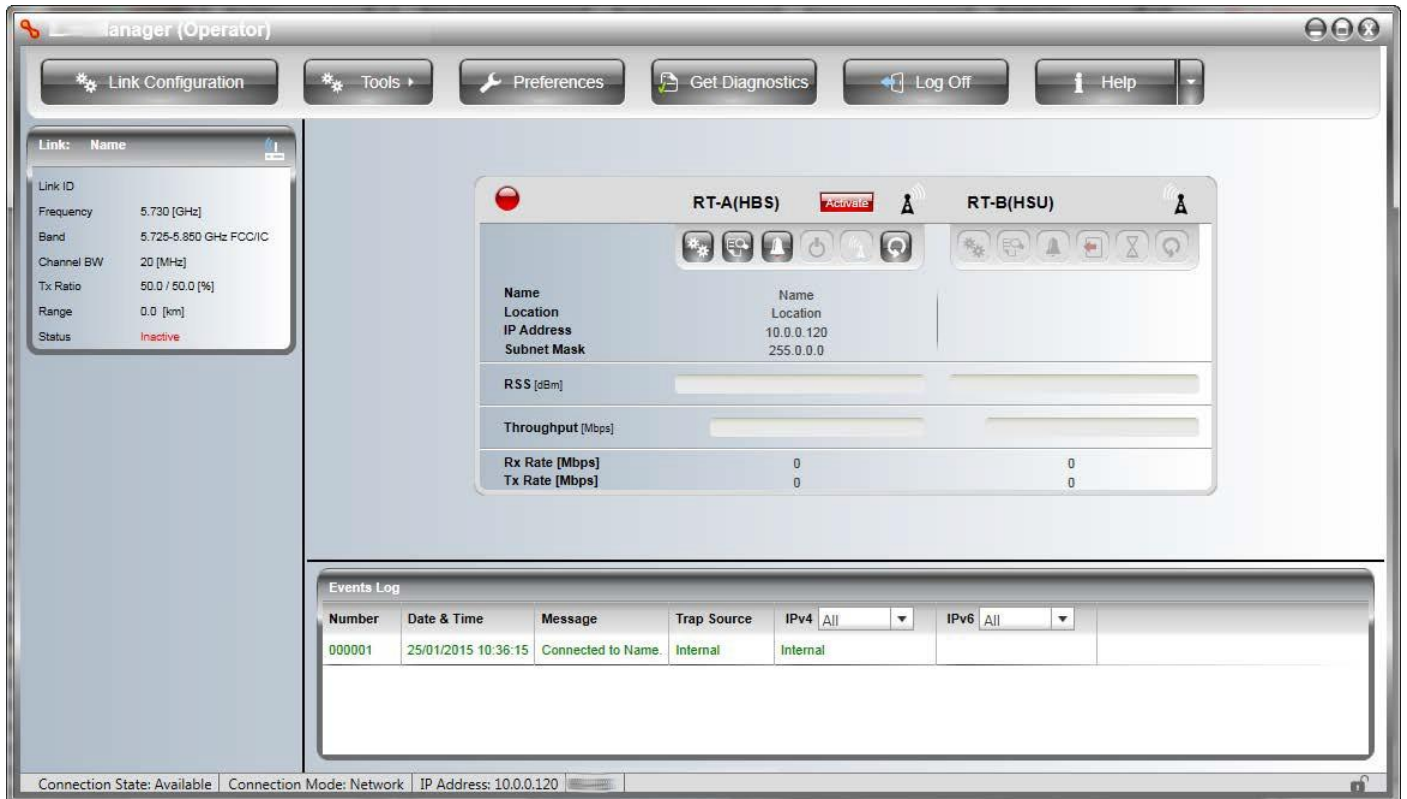


Figure 3-1: Main window prior to link configuration

3.2.2. Activating the RT-A(HBS)

All units are shipped from the factory defined as an RT-B(HSU). You must define one as an RT- A(HBS) before you can activate it. See [Define One Unit as an RT-A\(HBS\)](#) for instructions.

➤ **To activate the RT-A(HBS):**

1. Click the Activate button. The Activation Wizard opens.



2. Click Next:



3. Enter the Link ID/Sector ID, Name and Location. All fields are mandatory.



- The entries are case-sensitive
- You may use only characters in the Latin alphabet but , ; % are not allowed
- Max number of characters is 30, except for Link ID/Sector ID, which is 24
- The first four digits of the Link ID is the “Network ID”. This is important especially if the Secured Sync Type is configured as Secured Network ID (See [Secured Sync Type](#))

Here are the entries for our demonstration link:

RT-A(HBS) Activation Wizard

Link ID: EBG_20560334

Link Name: Jack@A

Location: A

Link Password: *****

Buttons: Coordinates..., Change..., Prev, Next, Cancel



You may also ignore the Coordinates button.

- The Link Password may also be changed by clicking Change:

Change Link Password

Current: []

New: []

Confirm: []

Hide Characters

Buttons: Forgot Link Password?, OK, Cancel

Full details for changing the Link Password may be found in [Changing the Link Password](#). It is best left as is if there is no pressing need to change it.



Location

If you skipped an entry, it will be framed in red like this:

- From the previous Activation Wizard window, click Next.

The screenshot shows the 'RT-A(HBS) Activation Wizard' window. At the top, the title bar reads 'RT-A(HBS) Activation Wizard'. Below the title bar, there is a dropdown menu for 'IP Version' set to 'IPv4 Only'. Underneath, there are two sections: 'IPv4' and 'IPv6'. The 'IPv4' section contains three input fields: 'IP Address' with the value '10.0.0.120', 'Subnet Mask' with '255.0.0.0', and 'Default Gateway' with '0.0.0.0'. The 'IPv6' section contains three input fields: 'IPv6 Address' (empty), 'Subnet prefix length' with '64', and 'Default Gateway' (empty). At the bottom of the window, there are three buttons: 'Prev', 'Next', and 'Cancel'.

Enter the IP details. Here are our demonstration IP details:

This screenshot shows the same 'RT-A(HBS) Activation Wizard' window, but with updated IP details. The 'IP Version' dropdown remains 'IPv4 Only'. In the 'IPv4' section, the 'IP Address' field now contains '10.1043.2', the 'Subnet Mask' field contains '255.255.0.0', and the 'Default Gateway' field contains '10.104.10.21'. The 'IPv6' section remains the same as in the previous screenshot, with empty fields for 'IPv6 Address' and 'Default Gateway', and '64' for 'Subnet prefix length'. The 'Prev', 'Next', and 'Cancel' buttons are still present at the bottom.

To continue, click Next.

6. The next window is used to set the frequency and channels.



The default frequency is the lowest available in the operating band.



Note

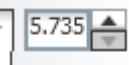
The frequency range and bandwidths available depend on the specific model in the RADWIN 2000-Plus Family you are working with. The values shown in the screenshot above are for illustrative purposes only.

7. Click Other to see other available bands for this radio unit.



8. For our purposes, we choose 5.820 GHz:



Observe that the right-hand spin-wheel  is no longer displayed. Had you left Other enabled, you could have chosen a frequency by working through those available in 5MHz increments.

9. Choose the required Channel Bandwidth:



Note

For the RADWIN 2000 C-Plus, RADWIN 2000 D-Plus, and RADWIN 2000i, choose at least 40 MHz Channel Bandwidth to enable the supported net aggregate capacity.

The RADWIN 2000-Plus Family has Dynamic Bandwidth Selection (DBS): If you choose the maximum value available for the bandwidth, the link may dynamically

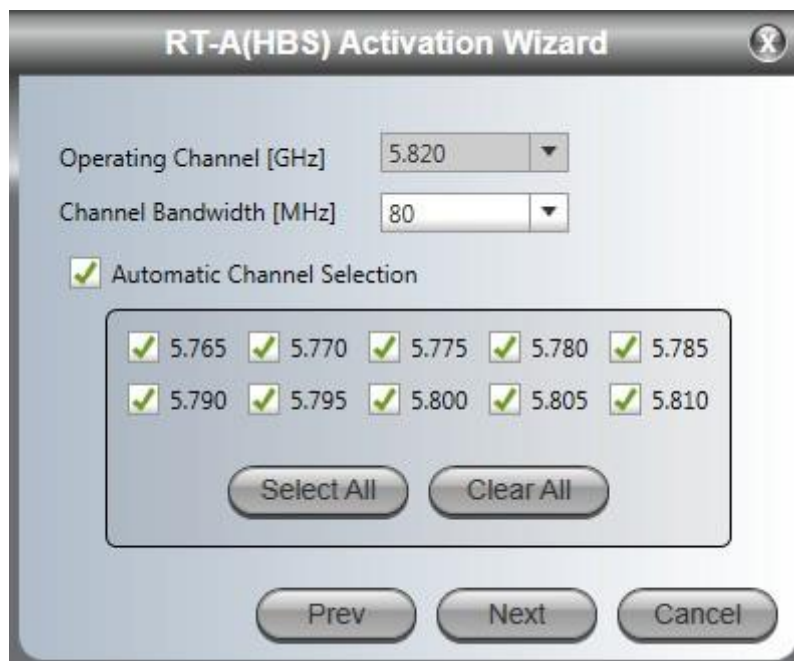
switch between the maximum value and values as low as 20MHz to ensure the best throughput. Selecting 20, 10 or 5 MHz CBW sets your choice as the fixed CBW for the link.

10. Using ACS:

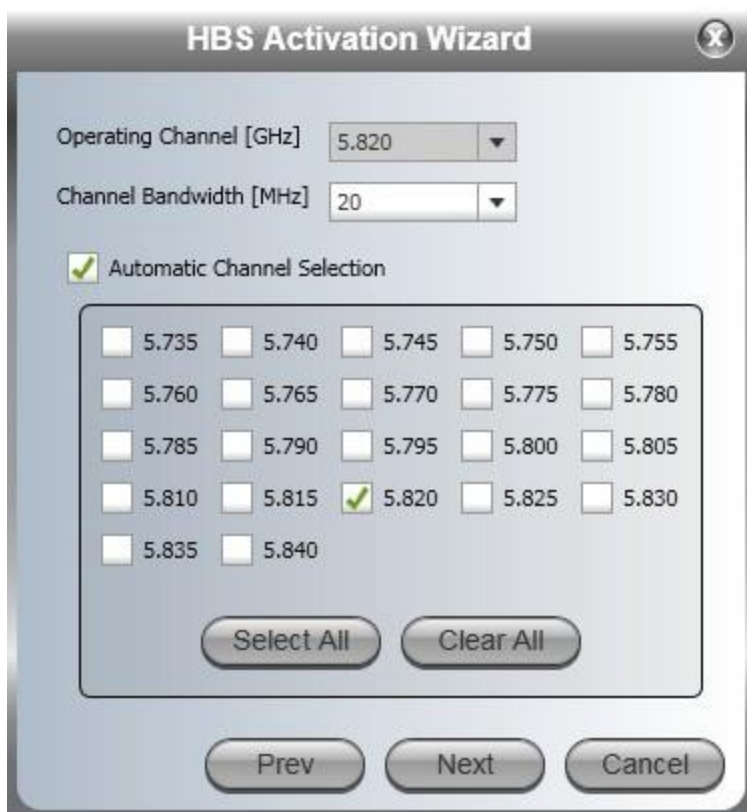
- > Choosing 40 or 80 MHz (if available) CBW automatically enables ACS. All that you may do is remove some of the channels:



Do not use ACS prior to antenna alignment.



- > For CBW 20MHz or less, enable ACS by checking the Automatic Channel Selection box:



You can perform a customized channel selection or click Select All to check all the channel boxes as shown:



11. Click Next. The Antenna type and Tx Power window is presented:

The choice of Tx Power, antenna gain and cable loss (between the radio and the antenna) determines the EIRP and is affected by such considerations as radio limitations and regulatory restrictions.

Before completing antenna installation, you might like to consider the background information about setting antenna parameters, in [Setting Antenna Parameters](#).

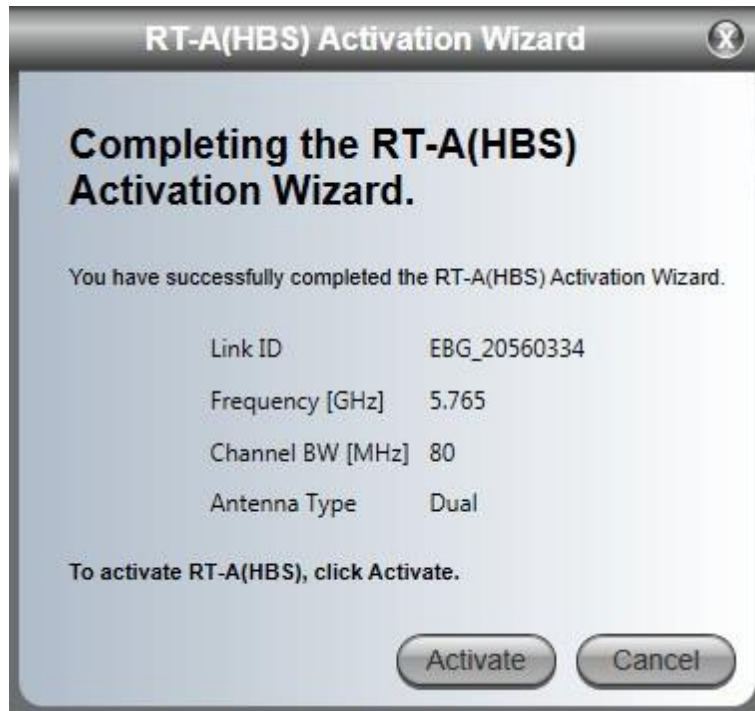


Caution

You can change the antenna gain, cable loss, or Tx power only if your user type is Installer. Changing these values can cause a violation of local regulations. You must check your local regulations if you plan to change these values.

Choose your Antenna Type, Required Tx Power, Antenna Gain and Cable Loss. We will set Required Tx Power to 5 dBm for our example. Click Next.

12. The Summary window of the Wizard is displayed.



Check that all information showed is correct and click Activate. After a few moments, the RT-B(HSU) will be displayed in the Manager main panel, as shown in the next figure:

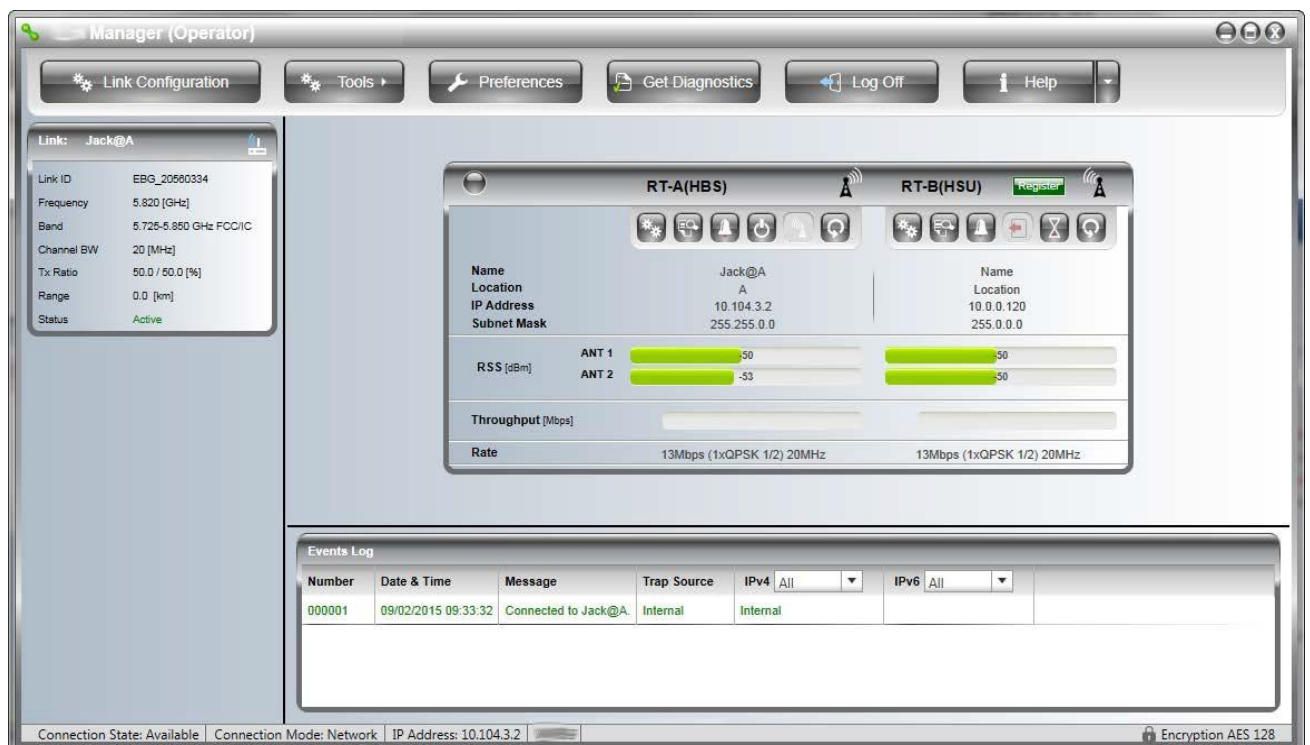


Figure 3-2: Main window: RT-A(HBS) activated; RT-B(HSU) ready for registration

Notice the Rate line shown enlarged:

Observe that under management mode (no traffic), the throughput and MCS is minimal to support a link and the CBW is also at its minimum for DBS.

13. If you are using a local connection, log out and log back into the RT-A(HBS) on its IP address.

You may have observed that the operating frequency 5.770 GHz shown is not what we chose (5.820 GHz). The RT-A(HBS) tries to optimize the frequency to minimize interference effects.

We next register and configure the RT-B(HSU). Many of the configuration and service parameters may be set prior to registration. During link establishment, the order does not matter. However, many configuration changes to a link after registration will affect traffic or even reset the link.

3.2.3. Registering the RT-B(HSU)

After few moments, the registration process completes. Here is the status of the link:



Figure 3-3: Main window: Link Master ODU activated, Slave ODU registered

3.2.4. Basic Configuration for Operations

Several basic parameters should be configured for both link sites. Use the appropriate site

Configuration button:



RT-A(HBS)

Go to Configuration | System and change the Contact to something other than the default entry, "Person":

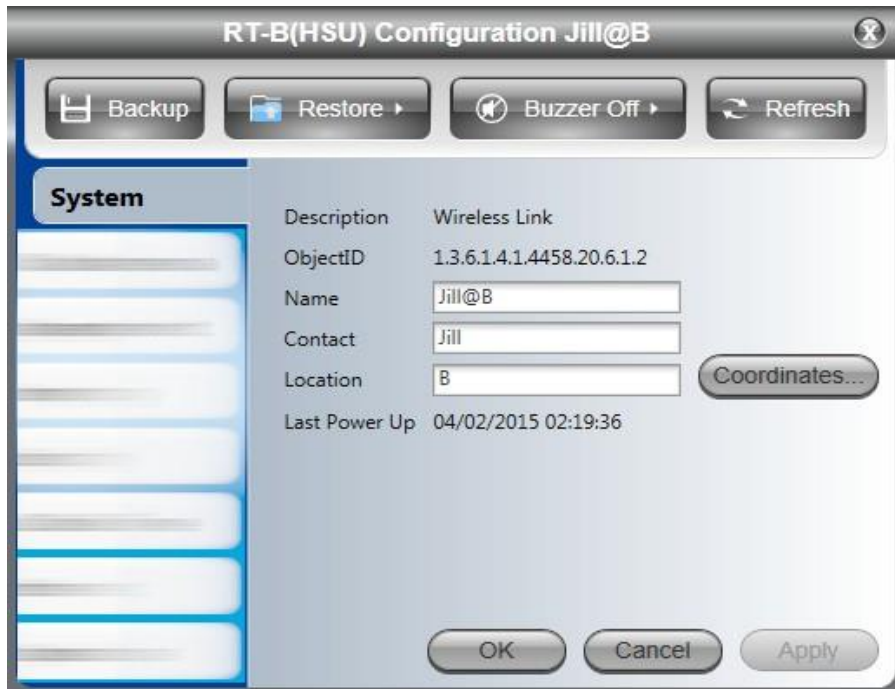


This only affects reports.

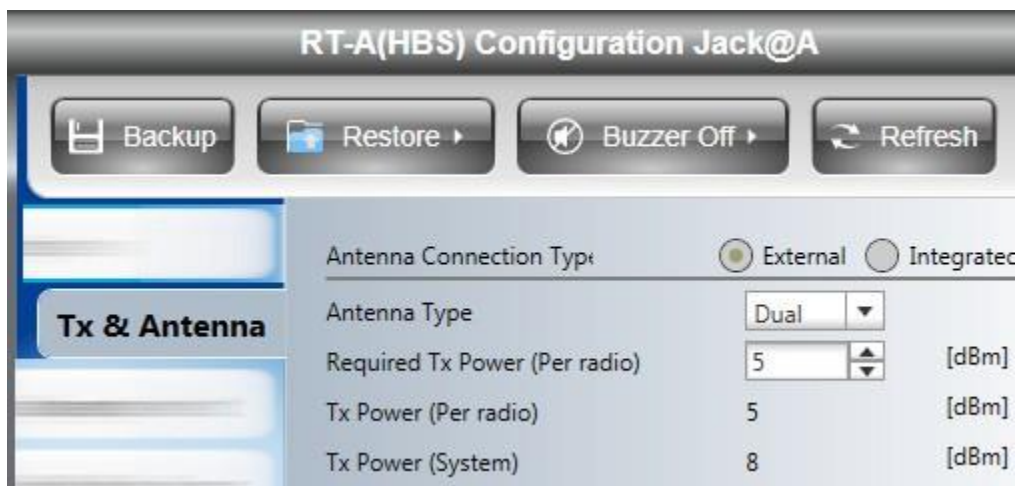
RT-B(HSU)

➤ To complete the basic configuration of the Slave ODU:

1. Go to Configuration | System and change the Name, Contact and Location fields to meaningful values:



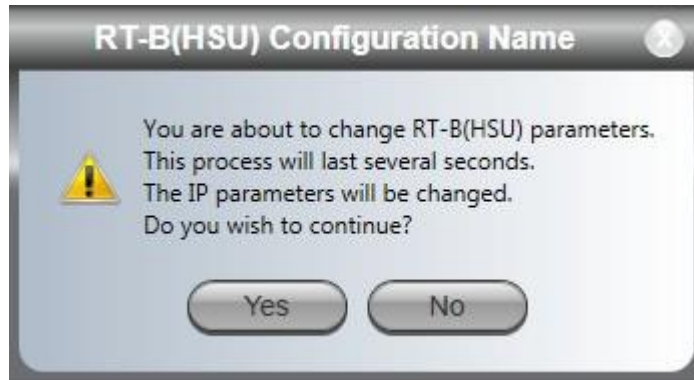
2. In the Tx & Antenna tab, ensure that the Tx Power is set appropriately. For our demonstration link, we reduce it to 5dBm:



3. Open the Management tab and set the IP address, Subnet Mask and Default Gateway to their required values. Here are ours:



- Click OK on the Configuration window to save your changes. You are asked to confirm:



- Accept the changes. Here is the status of the Link:

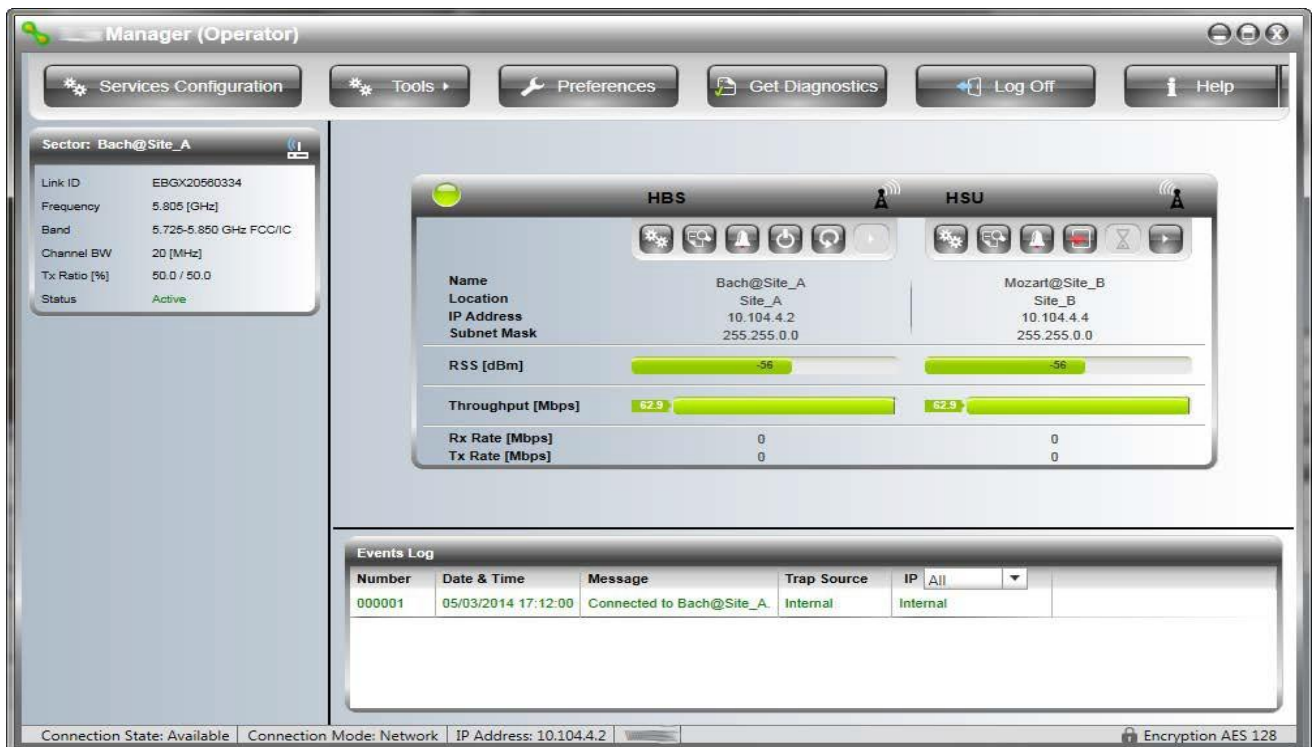
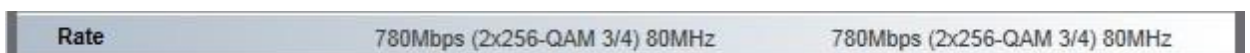


Figure 3-4: Main window: Link fully operational

Notice the Rate line shown enlarged:



Observe that in traffic mode, the throughput and MCS are at their maximum and the CBW is also at its maximum. Under adverse conditions, such as high interference, DBS would cause these parameters to fallback for best throughput.

3.3. Advanced Link Configuration

The link, as configured so far, is sufficient to provide basic service. Additional link-level services that can be configured from the Link Configuration tab on the top left of the main window.

3.3.1. Air Interface

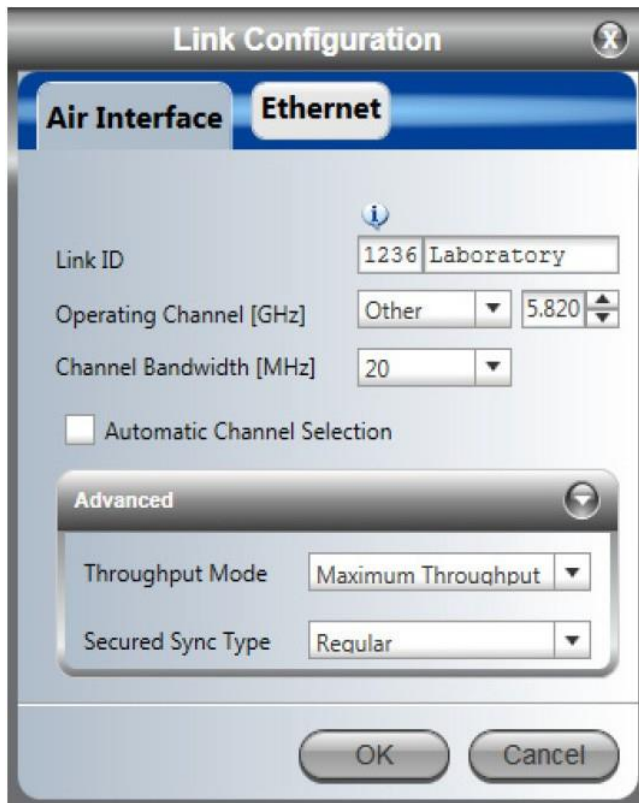


Figure 3-5: Link Air Interface parameters - no ACS

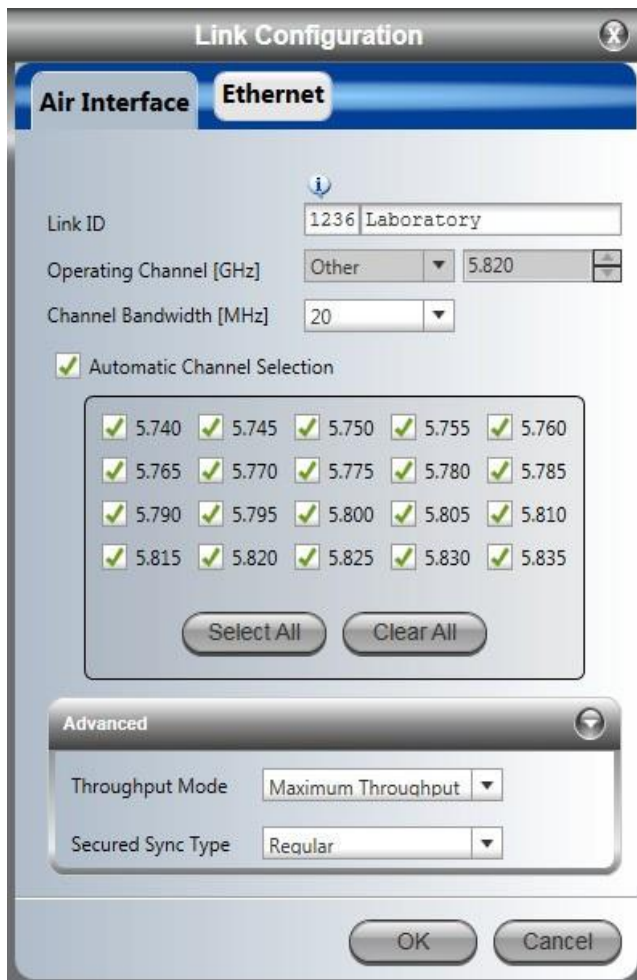


Figure 3-6: Link Air Interface parameters - ACS enabled

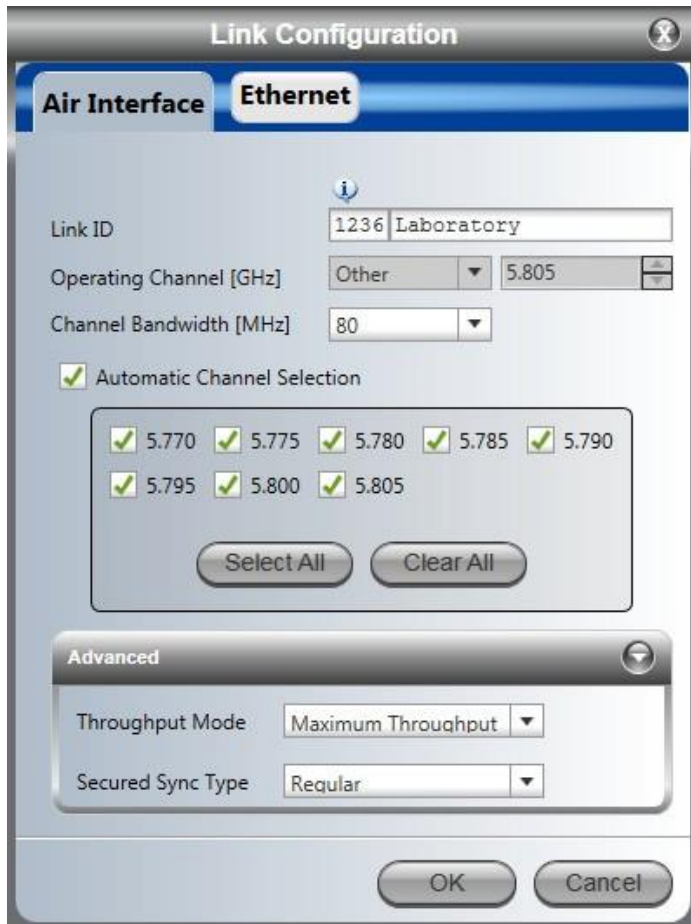


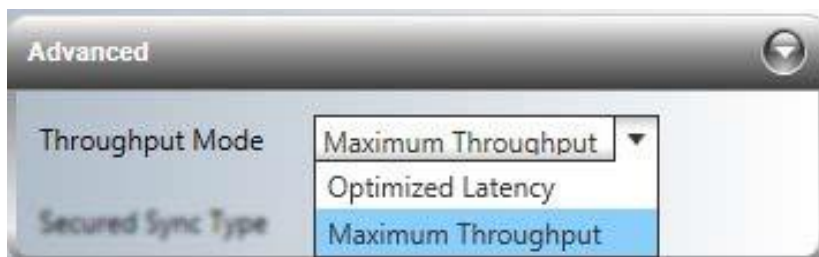
Figure 3-7: Link Air Interface parameters - DBS enabled, ACS on by default

Figure 3-5 to Figure 3-7 contain a subset of the Activation Air Interface settings. You may only change the Operating channel with ACS disabled.

These parameters are automatically inherited by the RT-B(HSU) when you click OK.

Throughput Mode

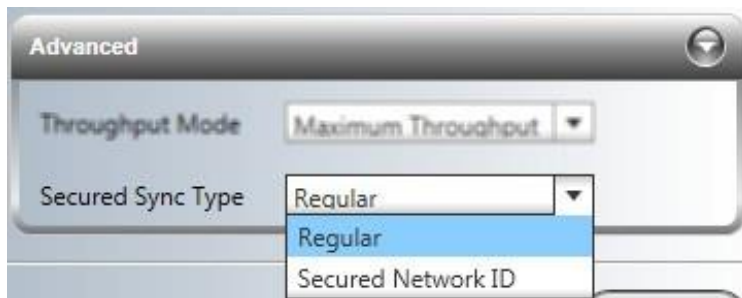
From the Advanced button, you can choose a throughput mode:



Throughput Mode determines how the Adaptive Modulation mechanism works. Maximum Throughput (default) should be chosen if throughput is more important than higher delay. Conversely, Reduced Latency minimizes delay at the expense of lower throughput.

Secured Sync Type

From the Advanced button, you can choose a secured sync type.



Secured Sync Type determines whether or not the RT-B(HSU) must have the same Network ID as the RT-A(HBS) to establish a link. The Network ID is the first 4 digits of the Link ID.

- To enable this option, select **Secured Network ID** from the pull-down menu.
- To disable this option, select **Regular** from the pull-down menu.



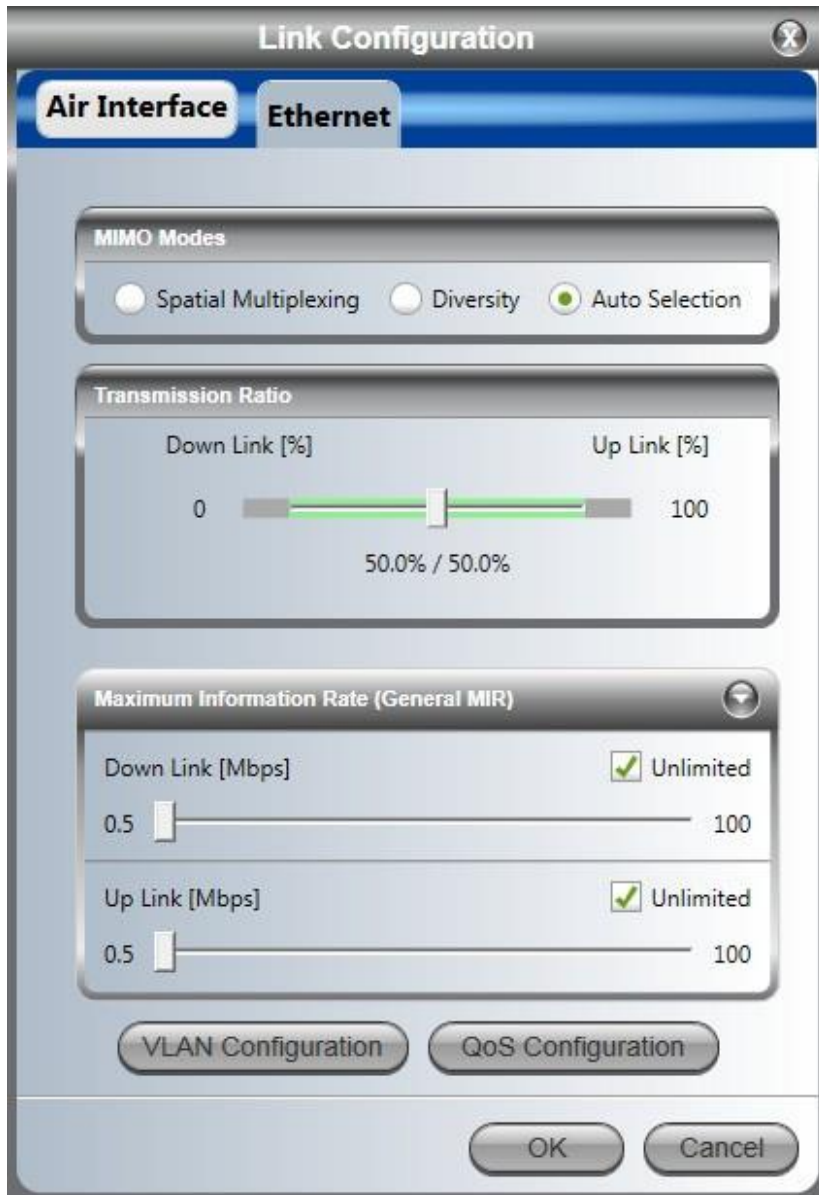
If the Secured Sync Type is Secured Network ID, and the wrong Network ID was entered in the RT-B(HSU), the unit will not establish a link and will be prevented from doing so for 10 minutes. Correct the Network ID, and at the end of this 10-minute period, the RT-B(HSU) will be able to synchronize with the RT-A(HBS).

Link ID

You may change this to any convenient string, but you are limited to 24 characters in the Latin alphabet and cannot use , ; and % . After you click OK, the RT-B(HSU) will be immediately updated over the air without interruption to service.

Changing the Link ID will also cause a change in the Network ID. Be careful if doing this when the Secured Sync Type is configured as Secured Network ID.

3.3.2. Ethernet



Link Configuration: MIMO Modes

If you are using dual antennas, you may check a MIMO Mode. Spatial Multiplexing (default) splits the data in to two streams on transmission and recombines it on reception providing maximum throughput. Diversity transmits the same data on both antennas and checks for correctness on reception. For further details about MIMO antenna modes, see [Initial Link Configuration](#).

Link Configuration: Transmission Ratio

The Transmission Ratio shows the allocation of throughput between downlink and uplink traffic at RT-A(HBS).

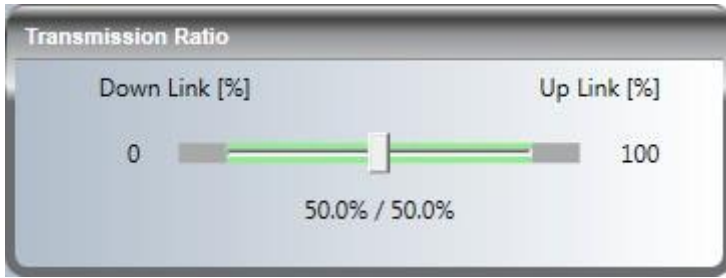


Figure 3-8: RT-A(HBS) Collocated client or independent unit

The permissible Transmission Ratio is also dependent on RT-A(HBS)'s HSS (collocation) status. (For further details about configuring and using HSS, see the *Hub Site Synchronization* application note.)

If the RT-A(HBS) is an HSS master¹, you will see something like this:

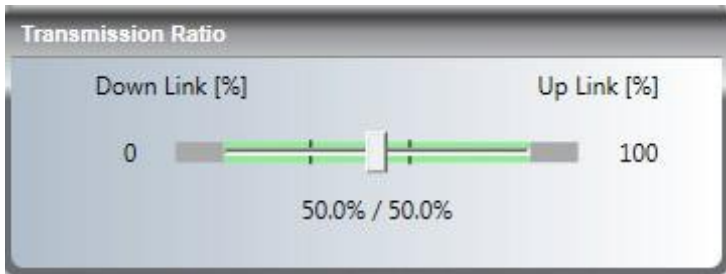
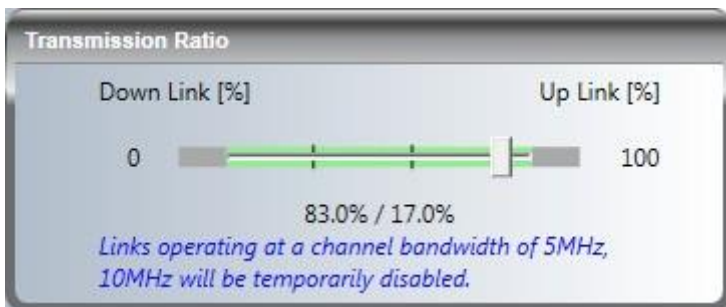
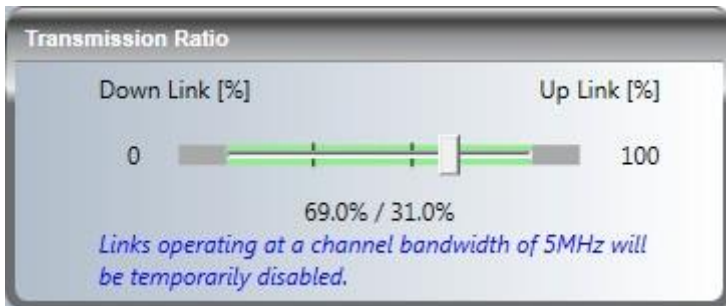


Figure 3-9: RT-A(HBS) Co-located master

Moving the slider to the right in stages yields the following:

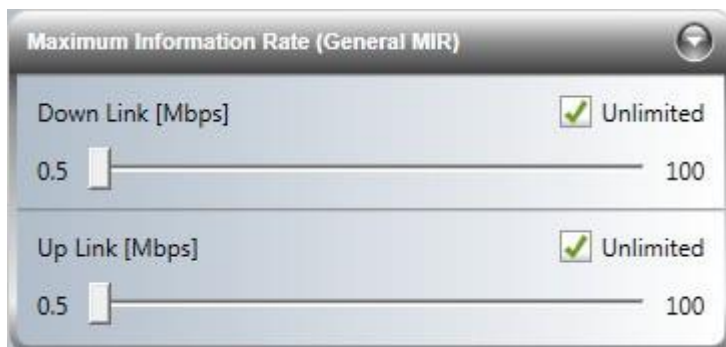


The effective available range for Asymmetric allocation is determined by channel bandwidth, as shown, as well as link distance.

1. Note that not all models can be an HSS master. See the RADWIN 5000 Hub Site Synchronization Application Note for more details.

Link Configuration: Maximum Information Rate

You can separately set the uplink and downlink Maximum Information Rate (MIR) in Mbps or leave it as Unlimited. The MIR acts as a throttle; leaving the uplink or downlink as Unlimited commits the link to operating at best effort.



VLAN and Quality of Service

These services are covered respectively in [VLAN Functionality](#) and [Quality of Service](#).

3.3.3. Changing the Link Band

Changing the Band in use is always carried out at the link level (not per installed radio unit). To change the Link Band, you must be logged on to the RT-A(HBS) as Installer. In Installer mode, the Tools drop-down menu has an extra function, Change Band.

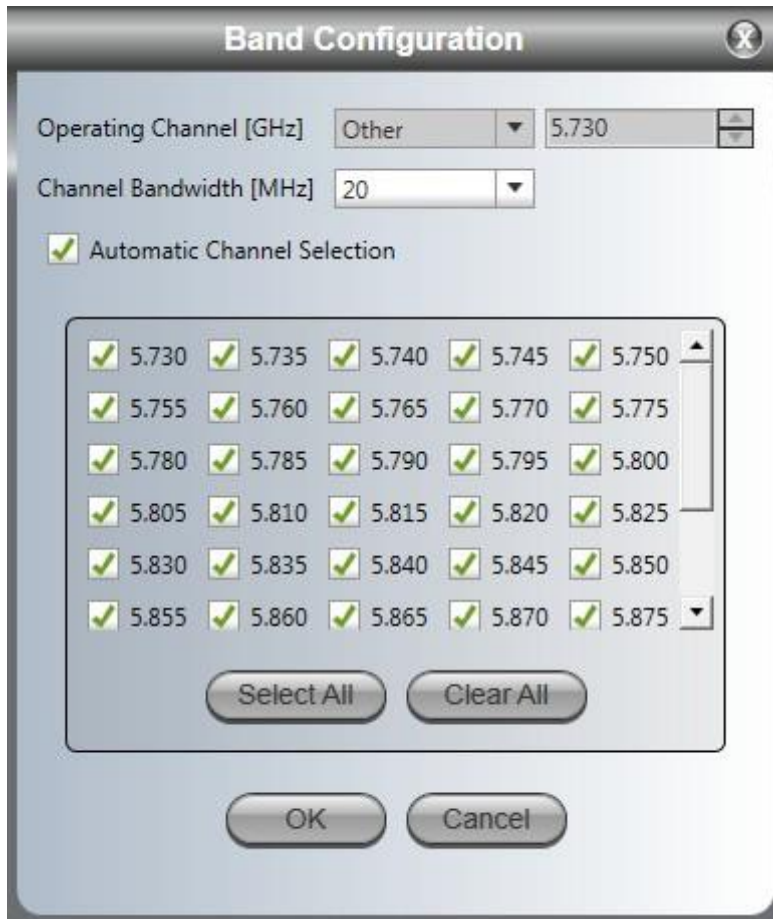
➤ **To change the Link Band:**

1. Click Change Band. A list of available Bands is displayed.

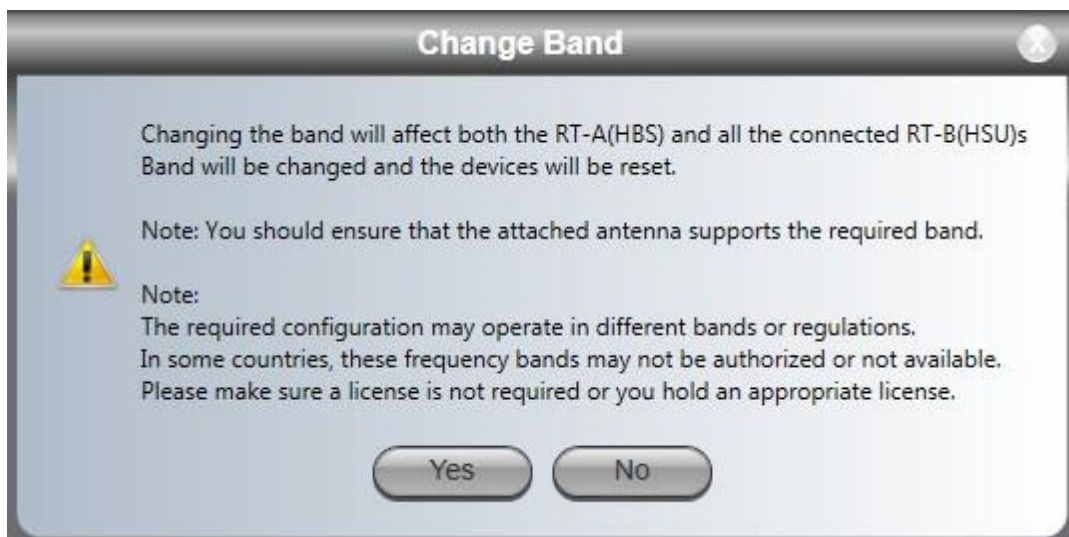


Figure 3-10: Change or Add Bands

2. Select the required Band and click OK. The band is highlighted, and right button is enabled.
3. Click the right button (🔧). The following window opens:



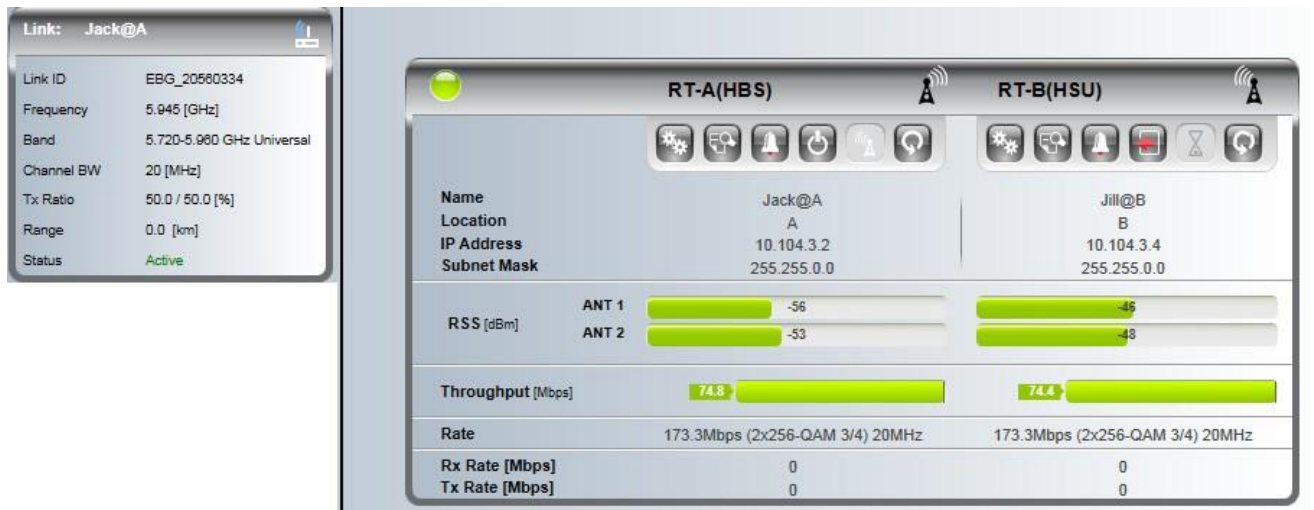
4. Here you may choose the working channel bandwidth and channel selection as in the activation process. (We will set CBW to 80 MHz and ACS fully selected.) Click OK to accept your choice. You are returned to the list of available bands.
5. Click OK again. The following cautionary message is displayed:



6. Click Yes to continue. After a short delay, you are offered a final confirmation:



7. Click OK. A link re-sync follows. Here is the final result:



Having set the channel bandwidth and operating channels earlier, there is no need for de-activation and re-activation.

You may also add new Bands by clicking the Add Bands button. There are several provisos to this:

- Additional Bands must be available for your hardware
- Such additional Bands must be available within the framework of your local regulations

The foregoing applies to both regulated and unregulated Bands.

➤ **To obtain and install additional bands:**

1. As Installer, open the window of [Figure 3-10](#) above, and click Add Bands. The following instruction panel is displayed:

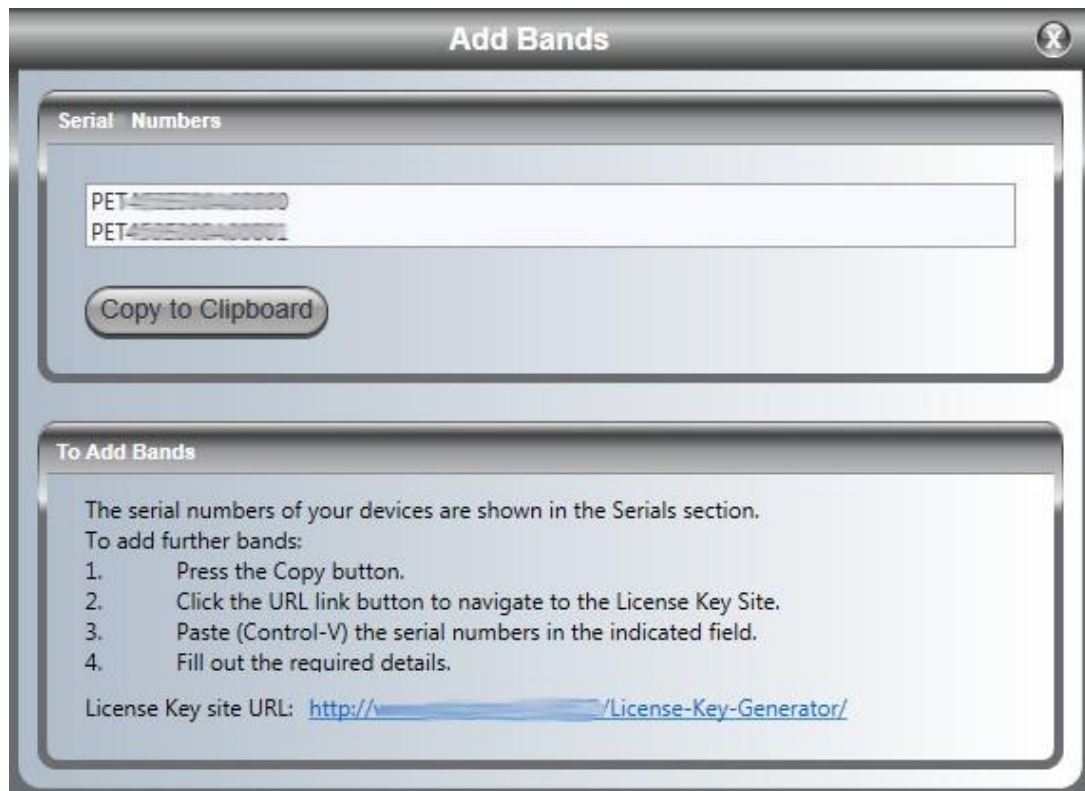


Figure 3-11: Add Bands Instructions Panel

The serial numbers displayed are those of the ODUs in the link. Click Copy to Clipboard.

2. Now carry out steps 2 to 4 in [Figure 3-11](#). Step 2 will take you to a Web page, which contains a form like this:

Fill out the form below to generate your License Key. After submitting the form you will receive an email with the new License Key. License Key generation is per serial number, you may enter several serial numbers. Required fields are marked with *. The Reference field is for your own records.

Personal details

End-User Full Name:*	<input type="text"/>	Company:*	<input type="text"/>
Address:*	<input type="text"/>	Phone:*	<input type="text"/>
End-User Email Address:*	<input type="text"/>	Confirm Email:*	<input type="text"/>
Reference:	<input type="text"/>	Enter Code (6344):*	<input type="text"/>

Link details

Required Band:*	<input type="text" value="2.4 GHz FCC/IC"/>	Serial Numbers:*	<input type="text"/>
Installation Country:*	<input type="text" value="Please Select..."/>		

Get Key

3. Fill out the requested details. Remember to terminate the dialog by clicking the Get Key button.
4. The results of your request will be displayed with further instructions.

No.	Serial	Status
1	PET4-XXXXXXXXXX	Serial Found
2	PET4-XXXXXXXXXX	Serial Found

Close

You will receive an automated email during the next few minutes. If it does not arrive, please check that it was not caught by your junk/spam filter.

A few minutes later, you should receive an email containing a list of license keys.



You may see error messages in the Status Column, such as “Band not supported” or “Serial not found”. Supported bands typically reflect your local regulations. Check missing serial numbers with the RADWIN Customer Service.

5. Copy and Paste the license keys into a plain text file and save it to a safe known place.
6. Open the Configure | Operations tab for either radio unit.



Figure 3-12: Using the Master ODU (HBS) Configuration button for licensing

Check the License File button and navigate to the file you saved in the last step.

7. Click Activate. The next time you enter the Change Bands tab, the new bands will be available.

3.3.4. Configuring AES 256 Encryption Support

AES 256 support is available for Alpha unit running release 5.1.30 and above and RADWIN 2000 C-Plus only, and only for the UNI and WPC regulatory environments.

In Alpha PtP link mode, the AES 256 is automatically enabled if the client side also support AES 256. The encryption mode (128 or 256) is displayed on the main screen after login to the web interface of the Alpha. For RADWIN 2000 C+, AES 256 support is enabled from the RT-A(HBS).

➤ To enable AES 256 Encryption support for a sector:

1. Ensure that the RT-A(HBS) is hardware ready for AES 256: From the HBS Configuration button, open the Inventory page and check that the hardware version is 9 or higher. Open a text file and copy/paste the serial number of the RT-A(HBS) to it.
2. Repeat step 1 for the RT-B(HSU).
3. Save the text file and send it to your equipment supplier with your license purchase order.
4. You will receive by return email a text attachment showing serial number and license key. Save the file to a known safe location.
5. At either ODU, open the Configuration | Operations tab. Check the License File

button and navigate to the file you saved in the previous step.

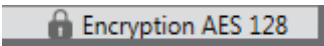
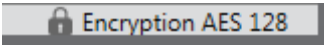
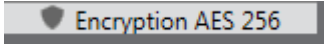
- Click Activate. You can confirm activation by opening the Security tab. The AES 256 check box, previously grayed out, is now available.



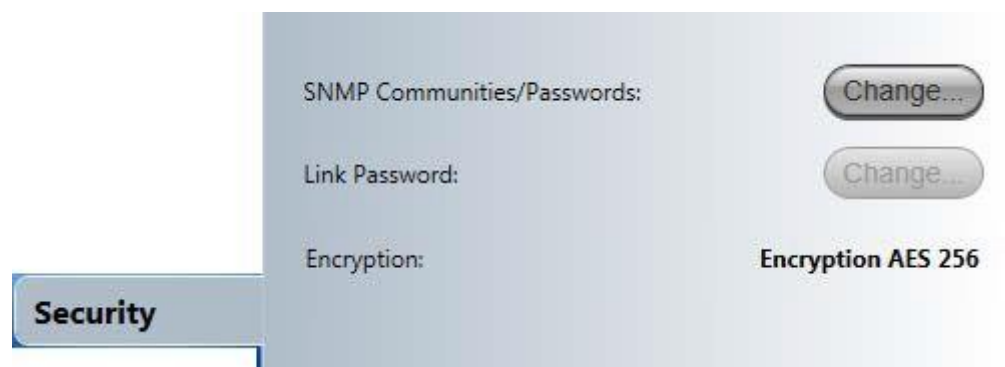
Check it to commence AES 256 Encryption.

You can confirm AES 256 support per ODU by looking at the Encryption icon at the bottom right-hand corner of the main window as shown in the following tables:

Table 3-1: AES Indicators for a link

AES Level Supported	Licensed for AES 256	RT-B(HSU) Encryption Icon
128	N/A	 Encryption AES 128
256	No	 Encryption AES 128
	Yes	 Encryption AES 256

In addition, the Security tab on the RT-B(HSU) Configuration widow (from the RT-A(HBS) or direct logon) will indicate when appropriate, that AES 256 is enabled:



3.4. Configuration with Telnet

3.4.1. Telnet Access to Either ODU

A Telnet terminal can be used to configure and monitor the RADWIN 2000-Plus Family radio units, with the exception of the RADWIN 2000 Alpha EMB/RADWIN 2000 Alpha Integrated.

To start a Telnet session on the RT-A(HBS), use telnet <ODU_IP>. For example, if you run Telnet as follows, telnet 10.104.3.2

you will be asked for a username and password.

The Telnet log on username is the password that you used to enter the RADWIN Manager (for example, the default: *admin*). The Telnet password is the corresponding Community string (default: *netman*).

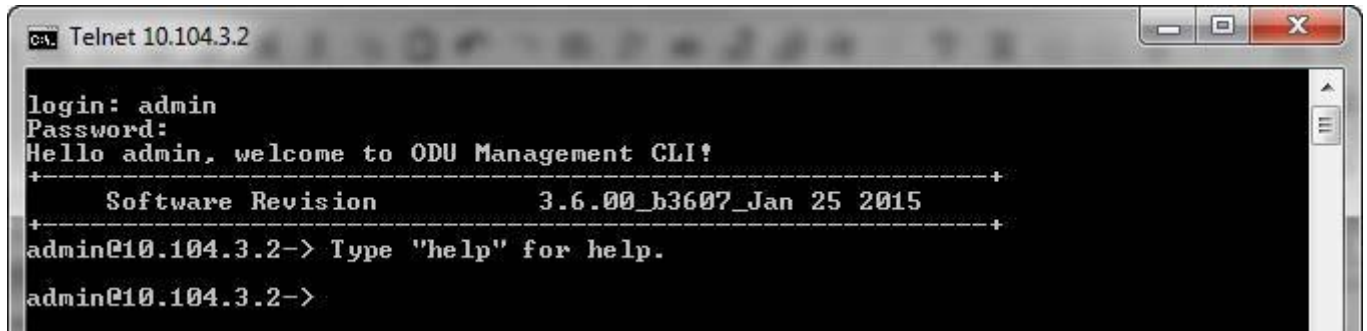


Figure 3-13: Telnet session log on to the RT-A(HBS)

A Read-Only Community string allows you to use display commands only whereas a Read-Write Community string allows you to use display commands and execute set commands.

Supported radio unit (ODU) Telnet commands are shown in [Table 3-2](#) to [Table 3-4](#). They apply to both RT-A(HBS) and RT-B(HSU)

Table 3-2: ODU Telnet - Display Commands

Command	Explanation
display inventory	Displays radio unit product name, Name, Location, hardware and software revisions, uptime, MAC address.
display management	Displays IP, subnet, Gateway, Traps table
display link	Displays all static details about the link
display ethernet	Displays Port table (State, Status and action)
display ethernet_errors	Displays Cable statistics

display ntp	Displays Time, Server and Offset
display PM <interface:AIR,LAN1> <interval:current,day,month>	Shows the performance monitor tables for each interface according to user defined monitoring intervals
display bands	Displays available bands
display ldpc_mode	On or off; default off

Table 3-3: ODU Telnet - Set Immediate Commands

Command	Explanation
set ip <ipaddr> <subnetMask> <gateway>	Set the radio unit IP Address, Subnet Mask and Gateway. The user must reset the radio unit after the command completion
set trap <index:1-10> <ipaddr> <port:0-65535>	Set a specific trap from the traps table (e.g., set trap 3 192.168.101 162)
set readpw <oldpasswd> <passwd>	Set the read access password (Read Community)
set writepw <oldpasswd> <passwd>	Set the read-write access password (Read-Write Community)
set trappw <oldpasswd> <passwd>	Set the trap Community string
set buzzer <mode>	mode: 0 = off, 1 = auto, 2 = on
set tpc<power:Value between minimal Tx power, and maximal Tx power>	Set the radio unit Tx Power. If a wrong value is entered, both min and max values shall be displayed in the error reply
set name <new name>	Set the name of the link
set location <new location>	Set the name of the location
set contact <new contact>	Set the name of the site manager
set ethernet <port:LAN1> <mode:AUTO,10H,10F,100H,100F,D ISABLE>	Set the mode and speed of the Ethernet port
reboot	Resets the radio unit. The user is warned that the command will reset the radio unit. A new Telnet session to the radio unit may be opened after the reset is complete.
help	Displays the available commands

Table 3-4: ODU Telnet - Set Commands requiring Reset

Command	Explanation
set seclid <SectorID>	Set new sector ID
set ldpc_mode <mode:on,off>	Sets ldpc mode

Chapter 4: Managing the Link

4.1. Scope of this Chapter

In this chapter, we describe how to manage and configure a link, noting differences between the RT-A(HBS) and RT-B(HSU).

4.2. Link Tool Bar

Here are the link tool bars and their functions:



Figure 4-1: Link Tool Bars

Table 4-1: Link Buttons - Description








Menu Button	Applies to which side of the link?	Purpose / Reference
	Both	Open the Link Configuration Window
	Both	Recent Events
	Both	Active Alarms
	RT-A(HBS)	Deactivate RT-A(HBS)
	Both	Reset the ODU

Table 4-1: Link Buttons - Description

Menu Button	Applies to which side of the link?	Purpose / Reference
	RT-B(HSU)	Deregister RT-B(HSU)
	RT-B(HSU)	Suspend a Deregistered RT-B(HSU)

4.3. Link Configuration Window

4.3.1. Link Configuration Tool Bar

Backup and Restore

The Backup and Restore buttons provide for backup and restore of the ODU software. For further information about the Backup and Restore, see [Backup, Restore, and Upgrade](#).



Buzzer

The Buzzer button sets or mutes the buzzer.



The buzzer tone is primarily used for ODU antenna alignment. The default setting is Auto.

Off - Turn off buzzer

On - Turn on buzzer

Auto - Buzzer responds according to signal strength. This is the setting used for antenna alignment. For details, see the RADWIN 2000-Plus Family Installation Guide.

Advanced Auto - Buzzer on while link down, and remains on for an extra two minutes.



There is no buzzer, nor buzzer button for the RADWIN 2000 Alpha EMB/RADWIN 2000 Alpha Integrated. For details on aligning this unit, see the RADWIN 2000-Plus Family Installation Guide.

Refresh

The Refresh button restores the current window to its previous state abandoning any changes you made, provided that you did not click Apply or OK.

4.3.2. Link Configuration for RT-A(HBS) vs. RT-B(HSU)

The Link Configuration windows are slightly different for the RT-A(HBS) and RT-B(HSU).



Figure 4-2: Link Configuration window - RT-A(HBS)

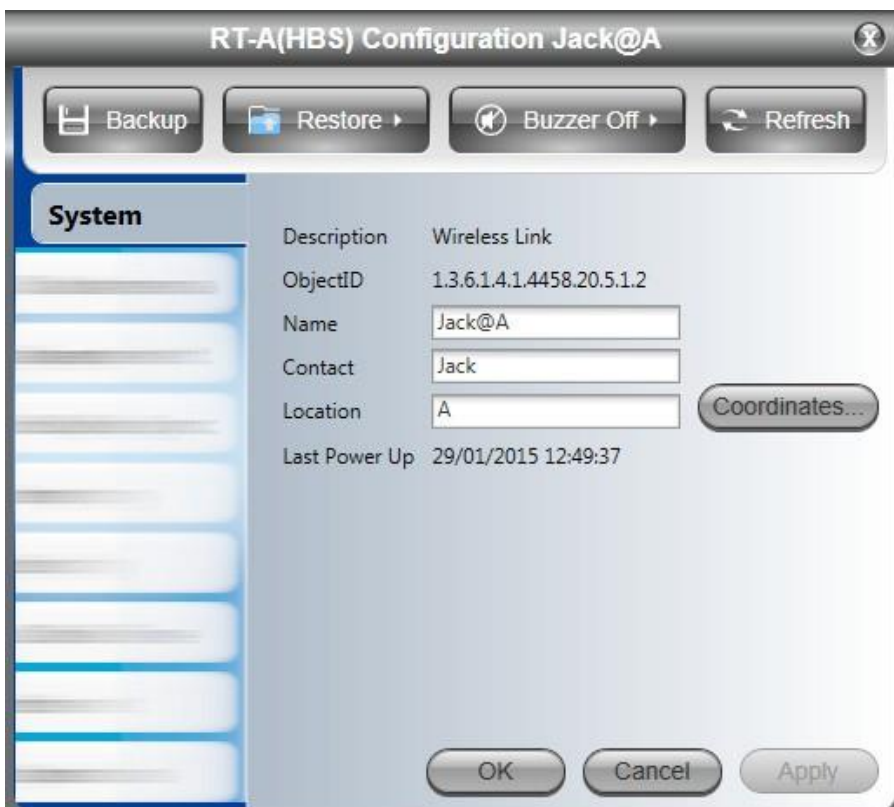
The RT-A(HBS) side has a tab to configure HSS. Otherwise, the side tabs have identical functionality for both sides. Further, the tool bars are common to both, and have identical functionality.



Figure 4-3: Link Configuration window - RT-B(HSU)

4.4. Configuration Tabs

4.4.1. System



The Name, Contact and Location fields are limited to 30 alphanumeric/Latin characters, and

cannot include , ; or %.

4.4.2. Tx & Antenna

You may use this tab at either side to further fine-tune Tx Power parameters set at Activation time.

Parameter	Value	Unit
Antenna Connection Type	<input checked="" type="radio"/> External <input type="radio"/> Integrated	
Antenna Type	Dual	
Required Tx Power (Per radio)	5	[dBm]
Tx Power (Per radio)	5	[dBm]
Tx Power (System)	8	[dBm]
Antenna Gain	28.5	[dBi]
Cable Loss	0.0	[dB]
Max EIRP	30.0	[dBm]
EIRP	30.0	[dBm]

Changing the Tx and Antenna parameters will take immediate effect without service interruption.



It is impossible to change the parameters of an EIRP to go beyond what is permitted in your regulatory environment.

4.4.3. Management

IP Addresses

Here is a typical IPv4 configuration:

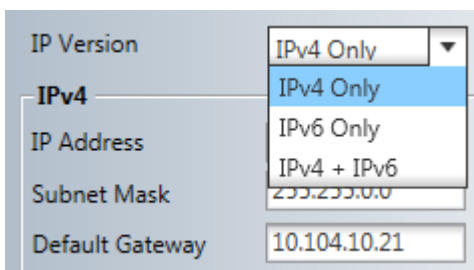


The screenshot shows the configuration window for RT-A(HBS) Configuration Hub_Site_1. It features a sidebar with a 'Management' tab. The main area contains the following settings:

- IP Version: IPv4 Only (dropdown)
- IPv4 section:
 - IP Address: 10.103.60.201
 - Subnet Mask: 255.255.0.0
 - Default Gateway: 10.103.10.1
- IPv6 section:
 - IPv6 Address: ::11.0.0.0
 - Subnet prefix length: 64
 - Default Gateway: ::10.0.0.0
- SysLog server IP Address: 0.0.0.0
- Trap Destination, VLAN, and Protocol buttons.
- OK, Cancel, and Apply buttons at the bottom.

IP Version

You may configure a link for IPv4, IPv6¹ or both:



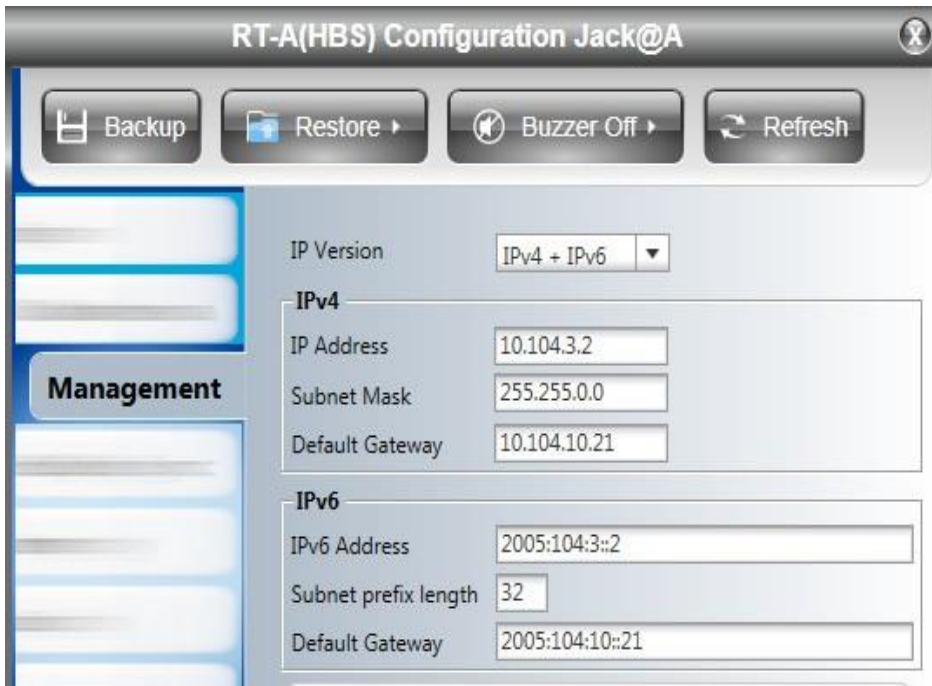
This close-up shows the 'IP Version' dropdown menu with the following options:

- IPv4 Only (selected)
- IPv6 Only
- IPv4 + IPv6

The background shows the IP Address field with the value 10.104.10.21 and the Subnet Mask field with the value 255.255.0.0.

Here we choose both and enter the IPv6 addresses:

¹ IPv6 is not available for the RADWIN 2000 Alpha EMB / RADWIN 2000 Alpha Integrated.



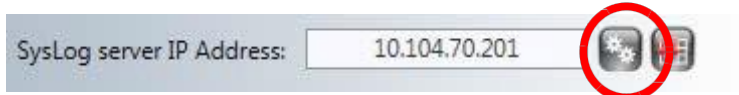
Using both IP versions is useful in conjunction with applications that do not fully support IPv6. Here are the results of setting IPv6 addresses for both sides and enabling Show IP to IPv6 in Preferences | Monitor:



Syslog server IP address

This field shows the IP address of a Syslog server to which the specific radio unit sends Syslog messages. This is configured per individual unit.

- **To change a Syslog server IP address:**
 1. Open an entry with its edit button:



The following entry window is displayed:



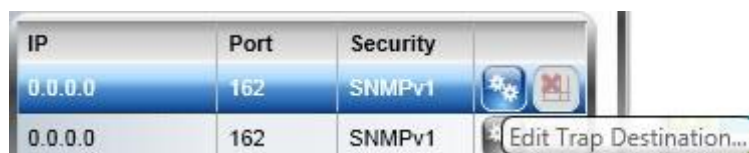
2. Enter the Syslog destination IP Address and click **OK**. It could be the IP address of the managing computer. The Syslog events will be stored at the address chosen.

Trap Destinations

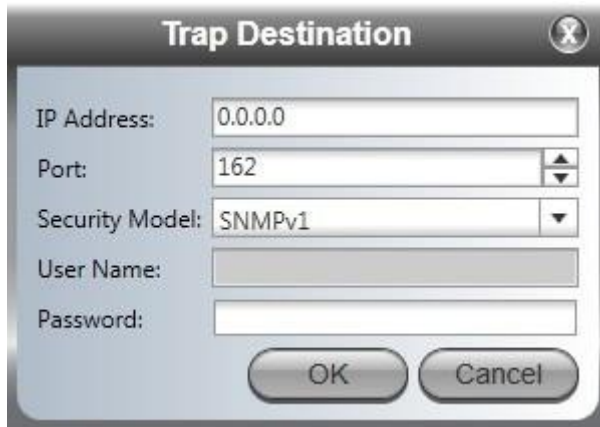


➤ **To change a trap IP address:**

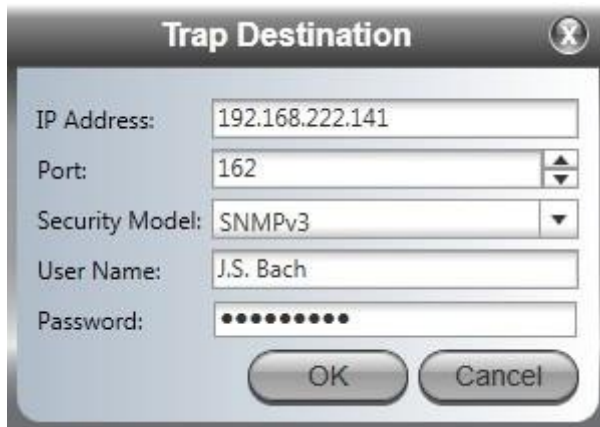
1. Open an entry with its edit button:



The following entry window is displayed:

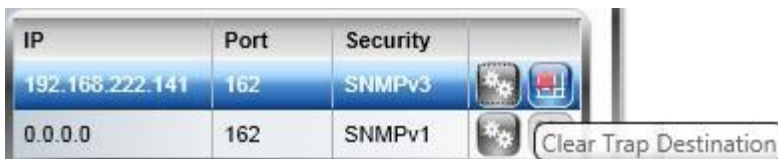


2. Enter the Trap Destination IP Address (IPv4 or IPv6)¹ and Port. It could be the IP address of the managing computer. The events log will be stored at the addresses chosen.
3. For Security model you may choose between SNMPv1 or SNMPv3. The choice is site dependent. If you choose SNMPv1, you may only enter an IP address and port number. For SNMPv3, you should supply a username and password:



4. Click OK to save your choice.

Note that for each active trap destination, the Clear Trap Destination button is enabled:



¹ IPV6 is not available for the RADWIN 2000 Alpha EMB/RADWIN 2000 Alpha Integrated.

VLAN for Management

Management VLAN Configuration



Figure 4-4: VLAN for Management



Caution

VLAN IDs are used by RADWIN products in three separate contexts: Management VLAN, Traffic VLAN and Ethernet Ring. It is recommended that you use different VLAN IDs for each context.

VLAN Management enables separation of user traffic from management traffic whenever such separation is required. It is recommended that each member of a sector be configured with different VLAN IDs for management traffic. (This reduces your chances of accidentally locking yourself out of the link.)

➤ To enable VLAN for management:

1. In the window of [Figure 4-4](#), check the Enabled box.
2. Enter a VLAN ID. Its value should be between 2 and 4094.

After entering the VLAN ID, only packets with the specified VLAN ID are processed for management purposes by the radio unit. This includes all the protocols supported by the radio unit (ICMP, SNMP, Telnet and NTP). Using VLAN for management traffic affects all types of management connections (local, network and over the air).

3. Enter a Priority number between 0 and 7.

The VLAN priority is used for the traffic sent from the ODU to the managing computer.

4. Change the VLAN ID and Priority of the managing computer NIC to be the same as those of steps 2 and 3 respectively.
5. Click Apply or OK.

Lost or forgotten VLAN ID

If the VLAN ID is forgotten or there is no VLAN traffic connected to the ODU, then reset the relevant ODU.



Caution

If the managing computer is directly connected to an ODU, and once you enable the management VLAN, you will lose connectivity. To log on again, you will need to configure the managing computer NIC to use the management VLAN number.



During the first two minutes of connection, the ODU uses management packets both with and without VLAN. You may use this period to reconfigure the VLAN ID and priority.

Protocols - LFF and SFF units

Supported protocols for all products except the RADWIN 2000 Alpha EMB / RADWIN 2000 Alpha Integrated are shown in [Figure 4-5](#):

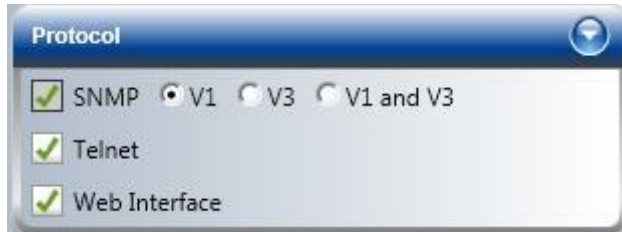
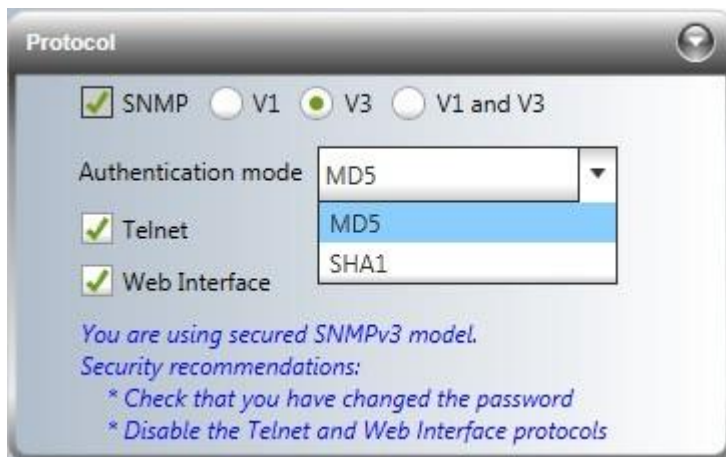


Figure 4-5: Supported protocols

Note that as of Rel. 4.9.75, the Web Interface is no longer available for LFF and SFF products. SNMP support is permanently enabled. You may choose between SNMPv1, SNMPv3 or both. If you choose SNMPv3, you will be offered the following cautionary message:



You can leave the default authentication mode for SNMPv3 as MD5 (message digest algorithm) or change it to SHA1 (secure hash algorithm).

For a link managed as part of a network, direct access using Telnet is considered to be a security breach. Telnet access may be enabled or disabled by clicking the Protocol tab and enabling/disabling Telnet access using the Telnet checkbox.

- For further details about Telnet access see [Section 3.4, Configuration with Telnet](#).

Telnet access mode, when available, is site specific. If, for example, you want Telnet access from a specific site, enable it for that site and disable it for others.

Conversely, if the Telnet access mode poses a general security risk, you must disable it for each site separately.

Protocols - RADWIN 2000 Alpha EMB / RADWIN 2000 Alpha Integrated

Supported protocols for the RADWIN 2000 Alpha EMB / RADWIN 2000 Alpha Integrated are shown in [Figure 4-6](#):



Figure 4-6: Supported protocols - RADWIN 2000 Alpha EMB/RADWIN 2000 Alpha Integrated

- SNMP and Web Interface support are permanently enabled
- Telnet is not available
- The Web Interface can be configured as HTTP or secured (HTTPS). It cannot be disabled. The options for the Web Interface are:
 - > HTTP: log on to the unit via a web browser using its IP address
 - > HTTP and HTTPS: log on to the unit via a web browser using its IP address or indicating explicitly HTTPS in the URL.
 - > HTTPS: log on to the unit via a web browser using its IP address, indicating explicitly HTTPS in the URL. If you do not write HTTPS in the URL (https://IP.address), then it will be put there automatically, and you will be logged on via HTTPS.
 - If you chose HTTPS, you can also choose “Strict Https” - next time you log on to the unit via a web browser, you must indicate explicitly HTTPS in the URL to log on
 - > Disabled: Not relevant for the RADWIN 2000 Alpha EMB/RADWIN 2000 Alpha Integrated.
- For further details about the Web Interface, see [Chapter 10, Using the Web Interface](#).

Multiuser Support under SNMPv3

If you chose SNMPv3 or both versions, you are asked to log on again:



For the first log-on under SNMPv3, use as password, the Username, *admin*.

The authentication will show as the mode you chose in the step before. Make sure you do not change it.

There is one change to the main window. The title bar now shows the SNMPv3 username:



Further, there is an additional button, SNMPv3/SSH Users, in the Management window:

IP Version: IPv4 Only

IPv4

IP Address: 10.104.50.1

Subnet Mask: 255.255.0.0

Default Gateway: 10.104.10.21

IPv6

IPv6 Address:

Subnet prefix length: 64

Default Gateway:

SysLog server IP Address: 0.0.0.0

SNMPv3/SSH Users

Trap Destination

VLAN

Protocol

OK Cancel Apply

Using the new button opens up the following entry list:

User Name	Password	Profile	Last Access time	
observer	*****	Observer		 
admin	*****	Admin		 
installer	*****	Installer		 
operator	*****	Operator		 
				 
				 

Table 4-2: SNMPv3 Predefined Users

Profile	Default Password	Function
observer	netobserver	Read Only
operator	netpublic	Can install and configure the sector but cannot change the frequency band/regulation.
installer	netinstaller	Functions as Operator, in addition to being able to change the operating frequency and frequency band /regulation, antenna gain and cable loss. Only an Installer can change the antenna gain and cable loss.
		Functions as Operator, in addition to being able

admin	netwireless	to change new users. Pre-defined users cannot be changed. Can change the operating frequency and frequency band/regulation, and the security mode (enhanced).
--------------	-------------	---

To change, delete, or add any user, you must be logged on as admin.

1. To add an SNMPv3 user:
2. Click the right hand edit icon on any empty line of the list:



3. An Edit window is displayed:

Figure 4-7: Add or Edit a user

4. Enter a username and password. Confirm the password as indicated.
5. Choose a Profile:

- Click OK to accept. Here is the result of adding one more Installer, Operator, and Observer user:



User Name	Password	Profile	Last Access time
observer	*****	Observer	
admin	*****	Admin	
installer	*****	Installer	
operator	*****	Operator	
Vivaldi	*****	Installer	
Teleman	*****	Operator	
Purcell	*****	Observer	

Figure 4-8: SNMPv3 users list

➤ **To edit an existing user:**

- Use the same procedure as above to choose a user for editing. For illustration, we will correct the spelling of Teleman's name:



User Name	Password	Profile	Last Access time
observer	*****	Observer	
admin	*****	Admin	
installer	*****	Installer	
operator	*****	Operator	
Vivaldi	*****	Installer	
Teleman	*****	Operator	
Purcell	*****	Observer	

- Click the edit button:



Edit User

User Name:

Password:

Confirm:

Profile:

OK Cancel

- Correct the spelling of the name:



4. Enter and confirm the user's password:



5. Click OK to finish. The change will be reflected in the display of [Figure 4-8](#).
6. Use the same method to change the user's profile.



Passwords are never displayed as clear text. If a user loses his password, the only way that the situation can be corrected is to delete the username and re-create the same username with another password.

Logging on as a SNMPv3 User

1. The default log-on dialog is shown below. Use the same password in the first Password window (on the upper left), but in addition, in the right-hand window, enter the SNMPv3 username and password.

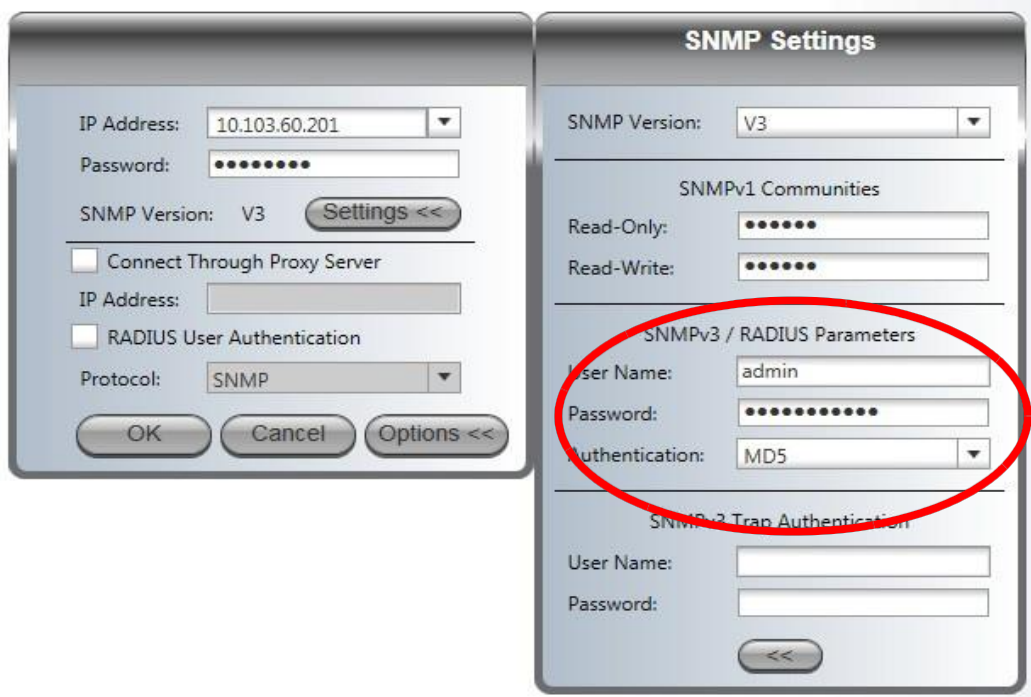


Figure 4-9: Default SNMP log-on dialog

In the main window, we see the username in the title bar:



4.4.4. Hub Site Sync (RT-A(HBS) Only)

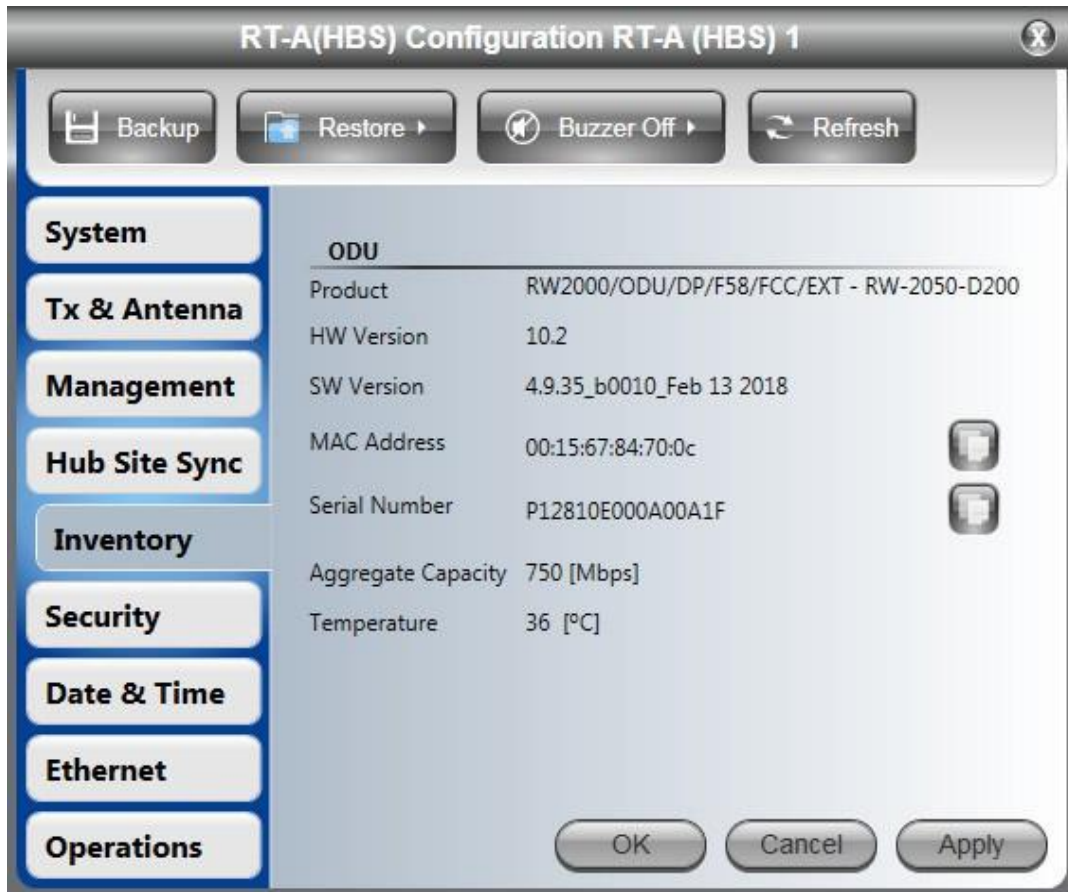
See the *Hub Site Synchronization* application note for details about configuring HSS.



Only RADWIN 2000-Plus Family RT-A(HBS) units can be co-located with other base stations. RT-B(HSU)s cannot be collocated.

4.4.5. Inventory

You might like to capture or copy the information here:



The information listed shows the parameters relating to the radio unit. Use the button to the right of the Serial Number field to copy the serial number to the clipboard. The Inventory information will be required by Customer Service should you require assistance.

4.4.6. Security



Figure 4-10: Sector Security settings - RT-A(HBS)

The Security dialog enables you to change the Link Password and the SNMP Community strings, as well as change the [Security Mode](#).

Changing the Link Password

This item is available as follows:

- At the RT-A(HBS)
- At an isolated RT-B(HSU)

Here are the details:

The default password is *wireless-p2mp*. Optionally, you can change the link password as explained here.

➤ To change the link password:

1. Open the Security tab ([Figure 4-10](#)).
The Change Link Password dialog box opens.



Use the Hide characters check box for maximum security.



Figure 4-11: Change Link Password dialog box

2. Enter the current link password (The default link password for a new ODU is *wireless-p2mp*).

If you have forgotten the Link Password, click the Forgotten Link Password button. The following window is displayed:



Figure 4-12: Lost or forgotten Link Password recovery

Follow the instructions to use the Alternative Link Password and click OK to finish. You are returned to the window in [Figure 4-11](#) above. Continue with the next step.

3. Enter a new password.
4. Retype the new password in the Confirm field.
5. Click OK.
6. Click Yes when asked if you want to change the link password.
7. Click OK at the *Password changed* success message.



Note

- A link password must contain at least eight but no more than 16 characters excluding SPACE, TAB, and any of ">#@|*?;,"
- Restoring Factory Defaults returns the Link Password to *wireless-p2mp*.

RADWIN Manager Community Strings

The ODU communicates with the RADWIN Manager using the SNMPv1 or SNMPv3 protocol. The SNMPv1 protocol defines three types of communities:

- Read-Only for retrieving information from the ODU
- Read-Write to configure and control the ODU
- Trap used by the ODU to issue traps.

The Community string must be entered at log on. You must know the password and the correct Community string to gain access to the system. You may have read-only privileges. It is not possible to manage the ODU if the read-write or the read Community values are forgotten. A new Community value may be obtained from RADWIN Customer Service for the purpose of setting new Community. You must also have available the serial number or the MAC address of the ODU.

The read-write Community strings and read-only Community strings have a minimum of five alphanumeric characters (bru1 and bru4097 are not permitted). Changing the trap Community is optional and is done by clicking the check box.

Editing SNMPv1 Community Strings

When editing these strings, both read-write and read-only communities must be defined.

Upon logging on for the first time, use the following as the current Community:

- For Read-Write Community, use *netman*.
- For Read-Only Community, use *public*.
- For Trap Community, use *public*

➤ To change a Community string:

1. Type the current read-write Community (default is *netman*).
2. Choose the communities to be changed by clicking the check box.
3. Type the new Community string and re-type to confirm. A community string must contain at least five and no more than 32 characters, excluding SPACE, TAB, and any of ">#@|*?;,"
4. Click OK to save.

Editing SNMPv3 Passwords

To commence the process, you must enter the current Read-Write Community password, as shown in the first field of [Figure 4-13](#) below. Change the Read-Write and Read-Only passwords as indicated. A password must be between 8 and 31 characters long. The same character restrictions for the SNMPv1 community strings also apply here.

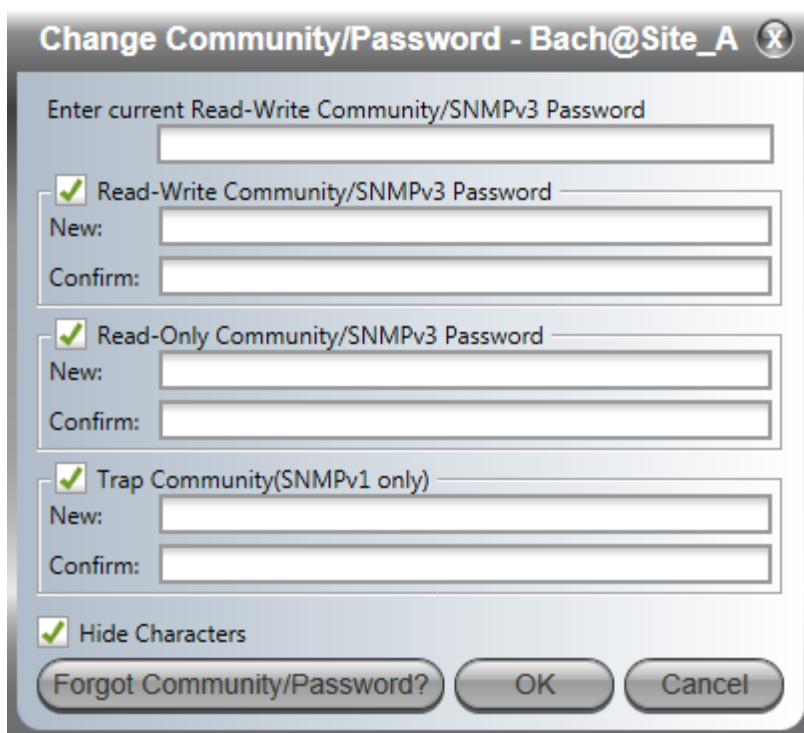


Figure 4-13: Changing the Community Strings/Passwords

Forgotten SNMPv1 Community String

If the read-write Community string is unknown, an alternative Community key can be used. The alternative Community key is unique per ODU and can be used only to change the Community strings. The alternative Community key is supplied with the product and should be kept in a safe place.

If both the read-write Community and the alternative Community key are unavailable, then an alternative Community key can be obtained from RADWIN Customer Service using the ODU serial number or MAC address. The serial number is located on the product label. The serial number and the MAC address are displayed in the Link Configuration inventory tab.

When you have the alternative Community key, click the **Forgot Community** button and enter the Alternative Community key (Figure 4-14). Then change the read-write Community string.



Figure 4-14: Alternative Community Dialog box

Security Mode

The 2000-Plus offers an enhanced version of its usual secured method of working, which offers extra protection against unauthorized access of the system.

It is performed on a unit-by-unit basis. However, if configured in one unit, its counterpart must also be configured for SNMPv3, but need not be configured with Enhanced Security.

Implement this mode as follows:

1. Change the SNMP management interface to SNMPv3:

Use the [Management](#) tab > [Protocols - LFF and SFF Units](#) pull-down menu

- a. Choose the SNMPv3 radio button. Choose SNMPv3 only, not “V1 and V3”
- b. Disable Telnet and the Web Interface (if working with LFF or SFF models)
- c. You can use either the MD5 or SHA1 authentication mode
- d. Click Apply. You will be asked to log in again (see [Logging on to the FibeAir Manager](#)). Make sure you have the proper SNMPv3 username and password.

2. Click the Security tab

3. Click the Security Mode pull-down menu. The screen will appear as follows:

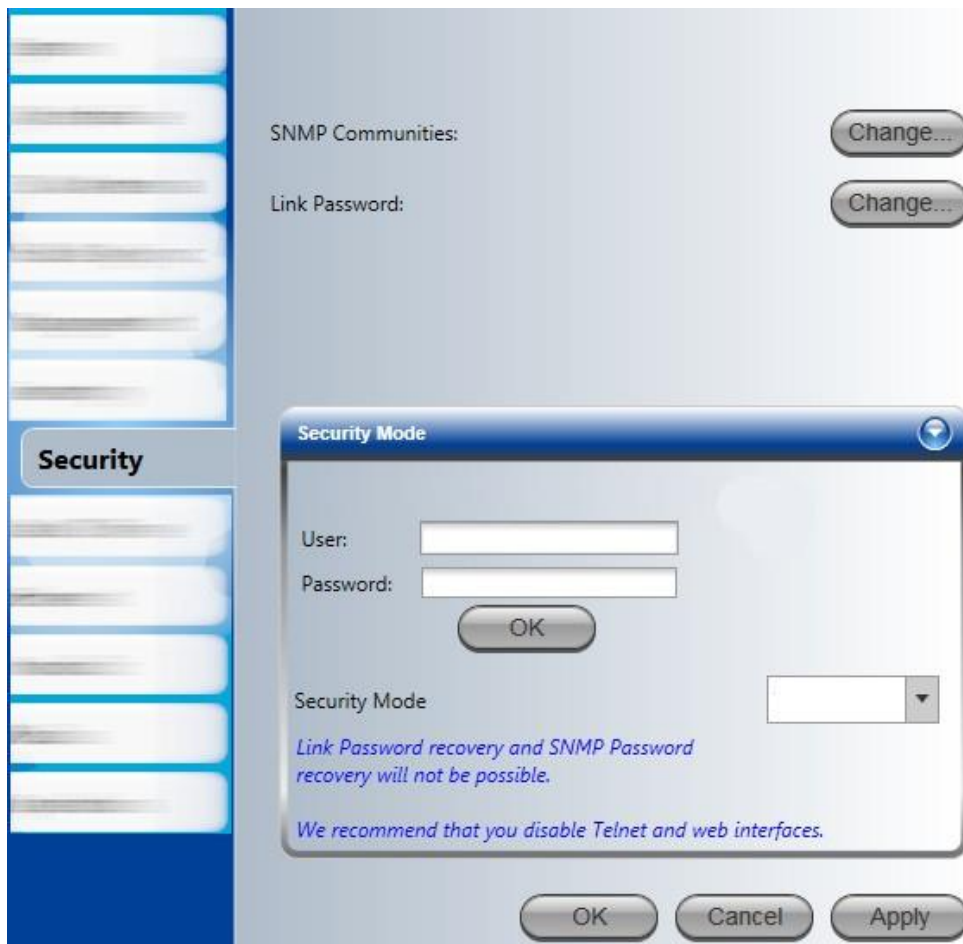


Figure 4-15: Security Mode settings

4. Enter the SNMPv3 username and password.
5. Click OK. The screen will appear as follows:



Figure 4-16: Choosing the Security Mode

6. From the Security Mode pull-down menu, select the security mode. There are three options:

Secured:	RADWIN 2000-Plus Family secured operation
-----------------	---

Immediately implement the enhanced security option.

When and if the unit is reset, there is a 2-minute grace

Enhanced Security*:

period where the enhanced security option is temporarily removed. After this time, the enhanced security option is re-established automatically.

Enhanced Security:	Immediately implement the enhanced security option.
---------------------------	---

7. Click OK or Apply.

Note the following when using the enhanced security mode:

- The SNMP management interface must be SNMPv3:
Use the [Management](#) tab > [Protocols - LFF and SFF Units](#) pull-down menu
- If configuring one unit for SNMPv3, its counterpart must also be configured for SNMPv3.
- The Local Connection feature is disabled (as it is based on SNMPv1)
- Alternative Community/Password is disabled
- Link Password is disabled
- VLAN recovery is disabled

4.4.7. Date & Time

The ODU maintains a date and time. The date and time should be synchronized with any Network Time Protocol (NTP) version 3 compatible server.

During the power-up, the ODU attempts to configure the initial date and time using an NTP Server. If the server IP address is not configured or is not reachable, a default time is set.

When configuring the NTP Server IP address, you should also configure the offset from the Universal Coordinated Time (UTC). If there is no server available, you can either set the date and time, or you can set it to use the date and time from the managing computer. Note that manual settings are not recommended since it will be overridden by a reset, power up, or synchronization with an NTP Server.



The NTP uses UDP port 123. If a firewall is configured between the ODU and the NTP Server this port must be opened.
It can take up to 8 minutes for the NTP to synchronize the ODU date and time.

➤ **To set the date and time:**

1. Determine the IP address of the NTP server to be used.
2. Test it for connectivity using the command, for example:
w32tm /stripchart /computer:216.218.192.202

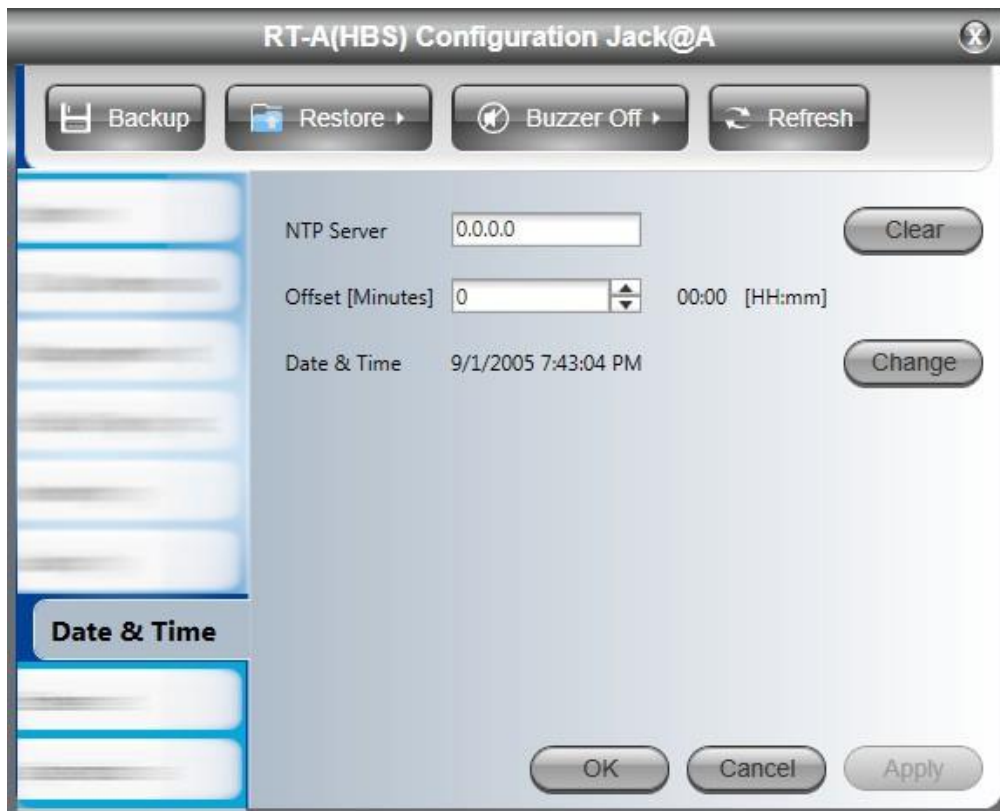


Figure 4-17: Date and Time Configuration

3. If entering an IP address for the NTP Server, click Clear, and then enter the new address.
4. Set the Offset value in minutes ahead or behind GMT¹.
5. To manually set the date and time, click Change and edit the new values.



Figure 4-18: Change Date and Time

6. Click OK to return to the Configuration dialog.

1. Greenwich Mean Time

4.4.8. Ethernet

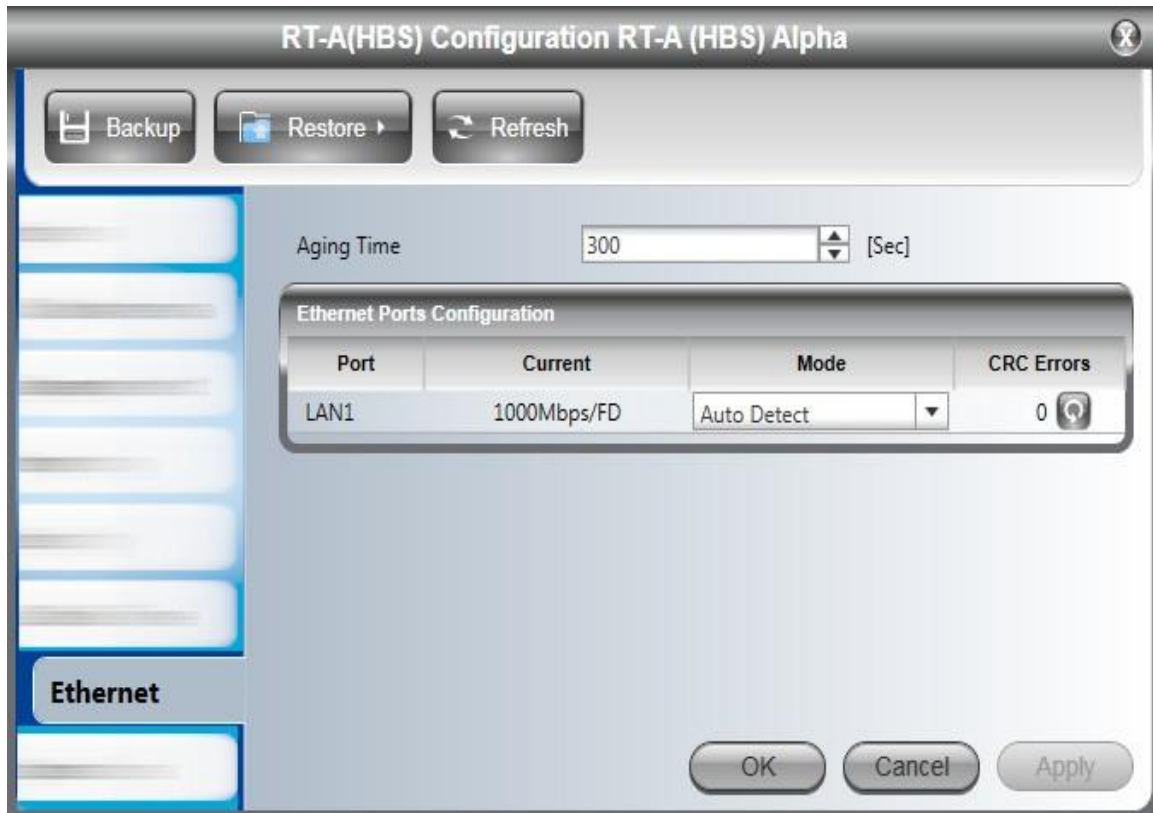


Figure 4-19: Setting Ethernet services

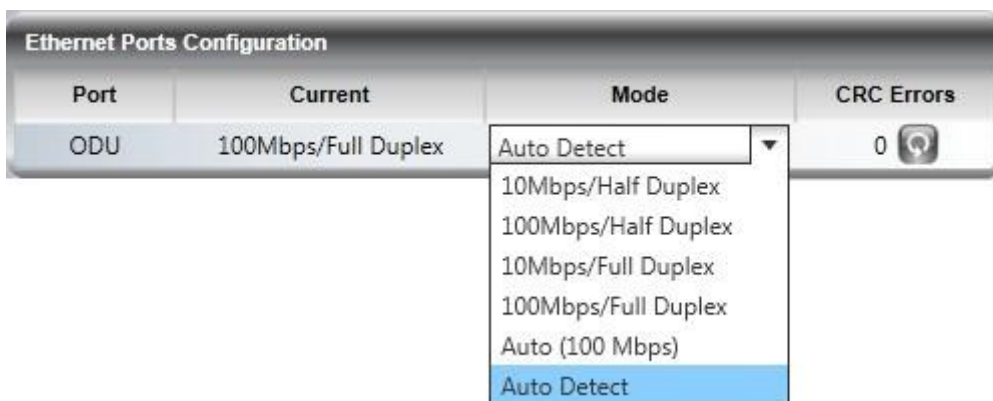
Aging Time

The RT-A(HBS) works in Bridge Mode. In Bridge mode, the ODU performs both learning and aging, forwarding only relevant packets over the sector. The aging time of the ODU is, by default, 300 seconds.

Ethernet Ports Configuration

The Ethernet port mode is configurable for line speed (10/100/1000BaseT) and duplex mode (half or full duplex).

Line speed 1000BaseT is only available if the ODU is connected to A GbE PoE device.



An Auto Detect feature is provided, whereby the line speed and duplex mode are detected automatically using auto-negotiation. Use the manual configuration when attaching external equipment does not support auto-negotiation. The default setting is Auto Detect. The icon next to the CRC error count may be clicked to reset the counter to zero.



Do not reconfigure the port that is used for the managing computer connection since a wrong configuration can cause a management disconnection or Ethernet services interruption.

➤ **To configure the Ethernet Mode:**

- In the Ethernet Ports Configuration pane, use the drop-down menus to choose the required modes.

4.4.9. Operations

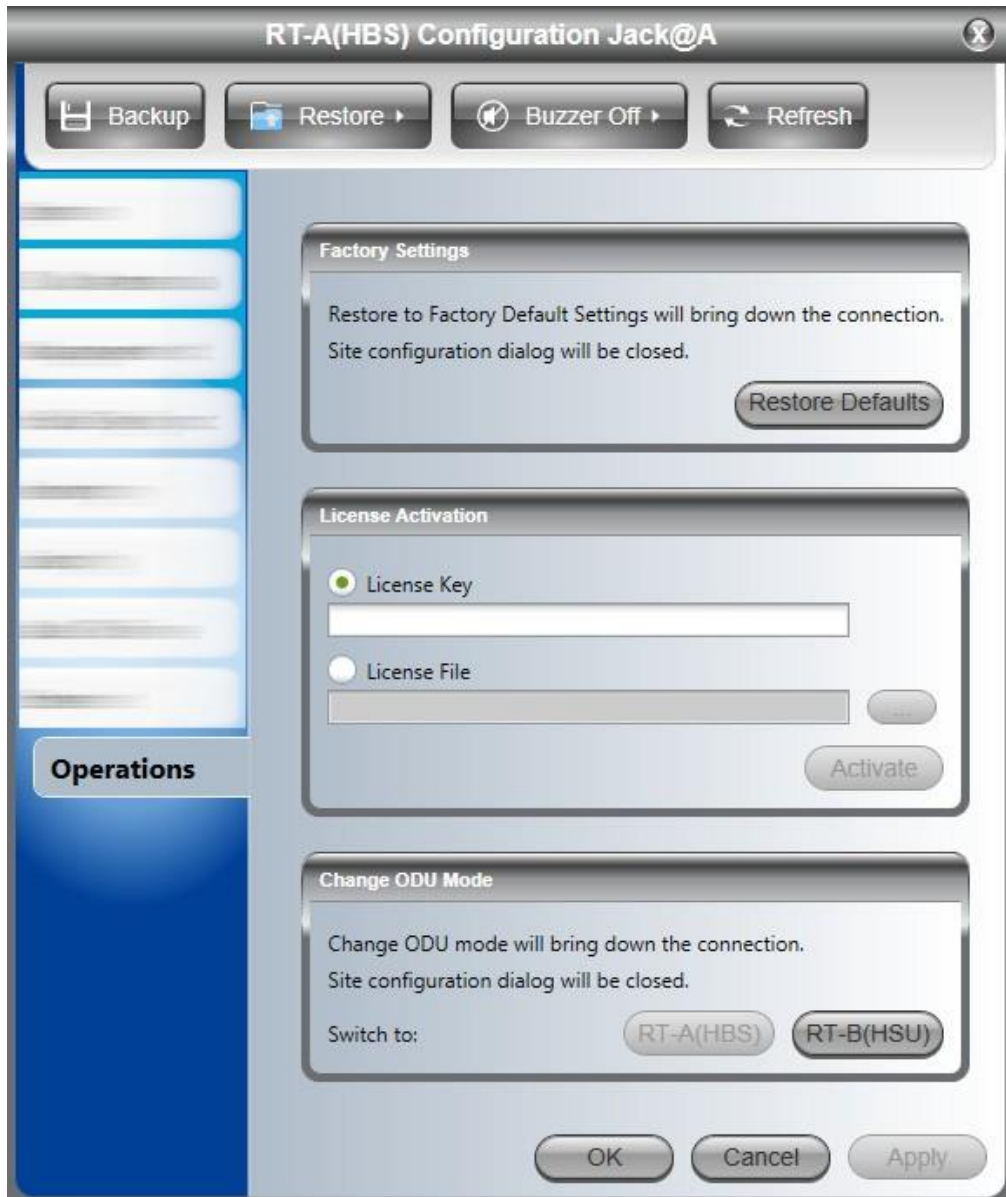


Figure 4-20: Restore Factory Settings, License Activation and Change ODU Mode

Reverting to Factory Settings

Clicking the Restore Defaults button opens the following dialog:



License Activation

Some product enhancements require a license key or a file of license keys. For a single key, just enter the supplied license Key and click Activate. If you have a list of them (a text file) you will need to use the License File option.

Change ODU Mode

When you set up your link, you defined one unit as an RT-A(HBS) (Master ODU) and the other as an RT-B(HSU) (Slave ODU). If you need to change this, use this option.

Changing the ODU Mode will change the fundamental behavior of the specific unit being changed.

4.5. Deactivate RT-A(HBS)



Deactivating the RT-A(HBS) halts traffic over the link and drops it back to the

default transmission mode prior to configuration with one exception: The RT-B(HSU) remains “registered” but inaccessible over the air. You can reactivate the RT-A(HBS) without needing to re-register the RT-B(HSU). All of the RT-B(HSU) configuration settings are preserved.

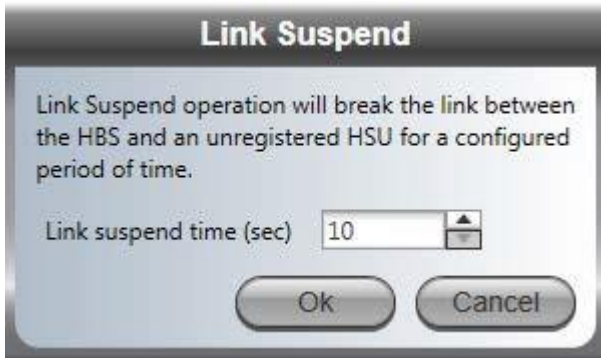
4.6. Deregister RT-B(HSU)



Deregistering the RT-B(HSU) stops link traffics but leaves it accessible over the air from the RT-A(HBS). All of the RT-B(HSU) tool bar functions are available.

4.7. Suspend a Deregistered RT-B(HSU)

You may break the link (cause a full sync loss) to the deregistered RT-B(HSU) for a fixed amount of time.



4.8. Reset the ODU



The reset functions are equivalent to powering the ODU down and then powering it up again.

Chapter 5: Monitoring and Diagnostics

The RADWIN Manager application enables you to monitor the link between the Master ODU and Slave ODU, as well as perform basic diagnostic operations, such as throughput testing.

This chapter covers:

- [Retrieving Link Information \(Get Diagnostics\)](#)
- [Throughput Checking](#)
- [Recent Events](#)
- [Performance Monitoring](#)
- [Manager Traps](#)
- [Active Alarms](#)

5.1. Retrieving Link Information (Get Diagnostics)

The Get Diagnostics feature collects and writes Link and Manager information from selected sites into a text file. The file information can be used for diagnostics and should be sent to RADWIN Customer Service to expedite assistance.

The following table lists link and system information that can be monitored.

Table 5-1: Get Diagnostics Data and Description

Data	Description
System Data	General information about the system
Events Log	<ul style="list-style-type: none">• List of system events, including those from other sites if this site is defined as the trap destination• Last 256 events from all sites
Link Information	Information about the RT-A(HBS) and RT-B(HSU) settings
Site Configuration	Data about the site parameters

Table 5-1: Get Diagnostics Data and Description (Continued)

Data	Description
Monitor	Detailed event data record
Active Alarms	Active Alarms are raised for any event affecting availability or
Service Configuration	Settings: MIMO, Tx Ratio, MIR, VLAN, QoS
Performance Monitor	Network performance data over defined time periods - - every 15
Spectrum Analysis	For RT-A(HBS), selected RT-B(HSU)s and general interference

➤ **To get diagnostics:**

1. Click the Get Diagnostics button:

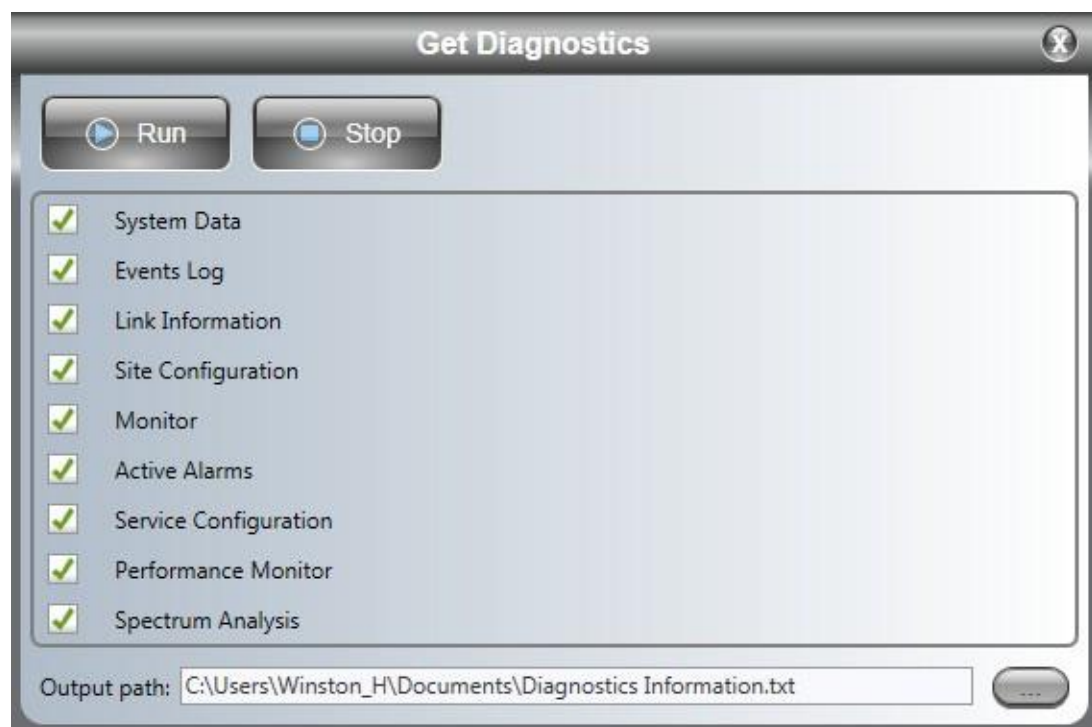
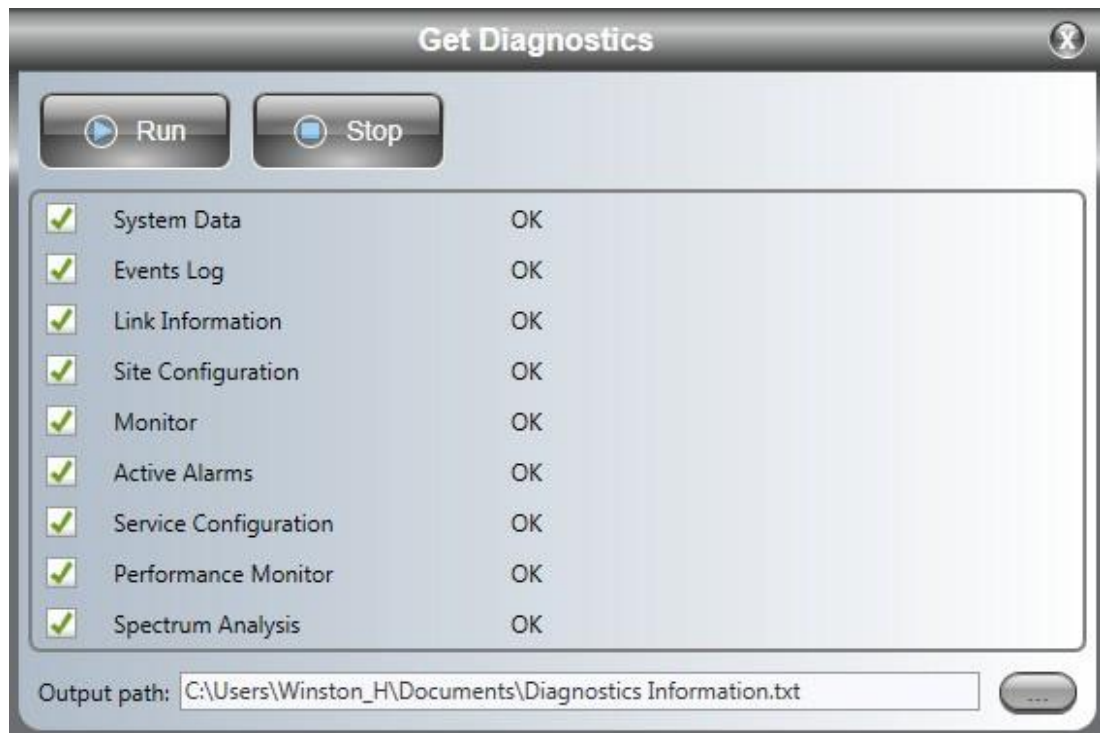


Figure 5-1: Get Diagnostics window

2. Select or deselect the data options. If the file is to be sent to RADWIN Customer Service, leave all options checked.
3. Click File Path to specify the file name and older in which you want to save the file and then click Run to save the information.

On completion, the status of the checked items is confirmed:



The content of the Diagnostics report is an aggregate of all the more specific reports discussed below. It is primarily intended for use by RADWIN Customer Service.



A supplementary diagnostics retrieval feature is available for the RADWIN 2000 Alpha EMB / RADWIN 2000 Alpha Integrated. See *Diagnostics File*.



The Spectrum Analysis output is available directly from the Spectrum View utility as a CSV file (see [Spectrum View](#)). The format in the Diagnostics report is intended for use by RADWIN Customer Service. The Spectrum Analysis section of the Diagnostics report is based on the last available spectrum analysis (if any). If you are submitting a support request involving interference issues, or if you are specifically asked by Customer Service to submit a Diagnostics report containing a recent spectrum analysis, you should carry out the analysis in accordance with the Spectrum View instructions prior to using the Get Diagnostics facility.

5.2. Throughput Checking

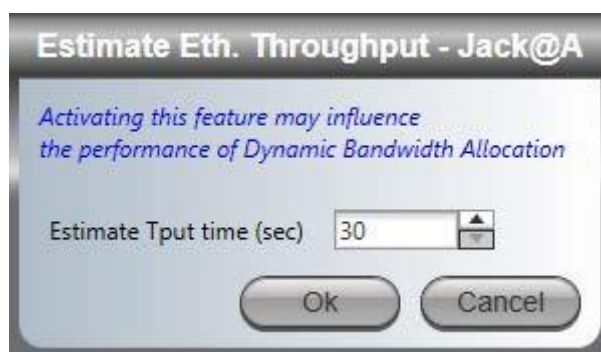
In this mode, RADWIN 2000-Plus Family estimates Ethernet throughput by filling frames over the air to maximum for 30 seconds. This mode should not influence service.

➤ **To use Throughput Checking:**

1. Chose Estimated Throughput from the Tools tab:



2. You are asked to enter the testing period:



3. Enter the required time and click OK to continue. The Ethernet services area changes appearance and the estimated throughput is displayed:



At the end of 30 seconds, the display reverts to normal.

5.3. Recent Events

The Recent Events log records system failures, loss of synchronization, loss of signal, compatibility problems and other fault conditions and events.



The foregoing event types include events from all links for which this managing computer has been defined as the traps address. Only events from RADWIN equipment will be shown.

Alarms (traps) are displayed in the Events Log in the lower panel of the main window. The Events Log may be saved as a text file.

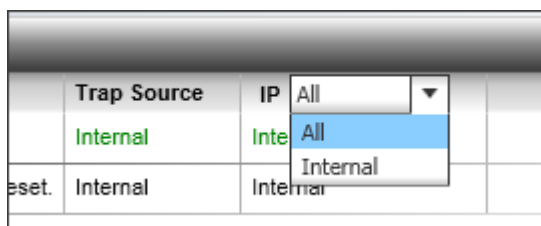
The Events Log includes the following fields:

- » Sequential number (ID)
- » Date and time stamp
- » Message
- » Trap source
- » IP address of the ODU that initiated alarm.

A screenshot of the 'Events Log' window. It features a table with columns for Number, Date & Time, Message, Trap Source, IPv4, and IPv6. The IPv4 column has a dropdown menu set to 'All'. Two event entries are visible: one with ID 000001 and another with ID 000002.

Number	Date & Time	Message	Trap Source	IPv4	IPv6
000001	28/01/2015 11:35:08	Connected to Jack@A.	Internal	Internal	
000002	28/01/2015 13:16:47	Jill@B Site will be reset.	Internal	Internal	

You may filter the events shown by choosing All or Internal.

A close-up of the filter dropdown menu in the Events Log. The menu is open, showing 'All' and 'Internal' options. The 'Internal' option is currently selected.

Trap Source	IP
Internal	Internal
reset.	Internal

A full report may be seen by clicking Recent Events in either ODU tool bar:



In each case, the report has the same format:



Here is a more readable enlargement of the table area:

Number	Device Date & Time	Description	Interface
1	01/09/2005 00:00:00	Management port status changed to disconnected	Management Port on Odu
2	01/09/2005 00:00:00	The time was set to: THU SEP 01 00:00:00 2005	
3	01/09/2005 00:00:00	HBS ready	
4	01/09/2005 00:00:00	HBS Name inactive	Radio Interface
5	01/09/2005 00:00:00	HSS operating state was changed to: Independent Unit	
6	01/09/2005 00:00:00	HSS multiple sync pulse sources were detected	
7	01/09/2005 00:00:00	HSS additional sync pulse was detected	
8	01/09/2005 00:00:00	HSS client status - Not Synchronized. The reason is: Pulse not detected	

The left button may be used to save the report to a file.

5.4. Performance Monitoring

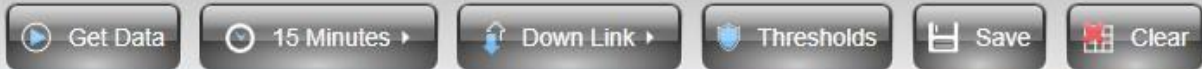
5.4.1. Obtaining Reports

RADWIN 2000-Plus Family Performance Monitoring constantly monitors traffic over the radio link and collects statistics data for the air interface and Ethernet ports. It does so continuously, even when the RADWIN Manager is not connected. The report is obtained from the Tools tab:



The on-screen and generated reports have the same general formats, but there are differences in what is reported.

The Performance Monitoring window offers the following button menu:



You can choose monitoring for Uplink or Downlink:



Choose the data period required with the 15 Minutes button.



- Current gives you the latest entry.
- 15 Minutes provides data in a scroll down list in 15-minute intervals.
- Daily (24 hours) shows results for the last 30 days at midnight.

The Threshold button enables you to set the upper traffic thresholds for reporting. Traffic conditions above the threshold indicate congestion and probably lost frames. The thresholds are set separately for uplink and downlink:

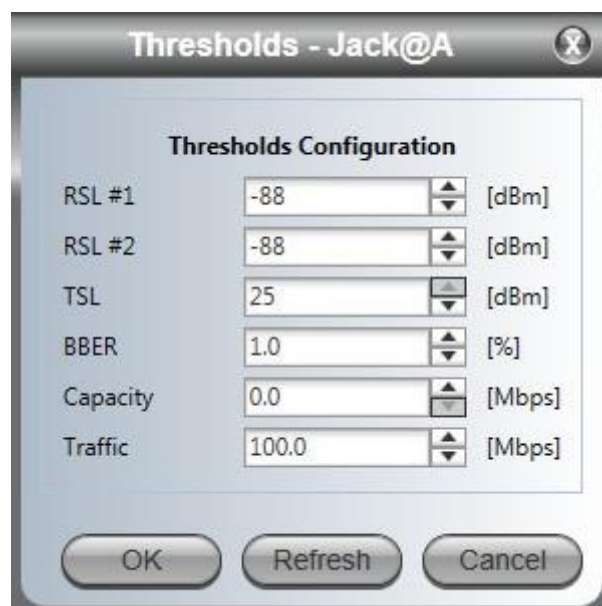


Figure 5-2: Setting the upper traffic threshold - Downlink

To get data for display, click Get Data. The process may take a few seconds.

Here is an extract for the downlink Performance Monitoring report based on 15 minutes recording:

Integrity	Date & Time	UAS	ES	SES	BBE	Min RSL (dBm)	Max RSL (dBm)	RSL Thresh 1 (-88 dBm)	RSL Thresh 2
✓	25/02/2014 11:00:00	0	0	0	0	-54	-54	0	0
✓	25/02/2014 10:45:00	0	0	0	0	-54	-54	0	0
✓	25/02/2014 10:30:00	0	0	0	0	-54	-54	0	0
✓	25/02/2014 10:15:00	0	0	0	0	-54	-54	0	0
✓	25/02/2014 10:00:00	0	0	0	0	-54	-53	0	0
✓	25/02/2014 09:45:00	0	0	0	0	-54	-53	0	0
✓	25/02/2014 09:30:00	0	0	0	0	-55	-53	0	0
✓	25/02/2014 09:15:00	0	0	0	0	-55	-53	0	0

Figure 5-3: Downlink - Performance Monitoring report - Valid data

The on-screen report may be scrolled vertically and horizontally. The meaning of the column headings is shown in the following table:

Table 5-2: Performance Monitoring Fields

Column Heading	Abbreviation Meaning	Description
Integrity	Valid data flag	Green checkmark for current and valid; Red cross for invalidated data (See example below). Note that the Performance Monitoring data is not valid if not all the values were stored (e.g., due to clock changes within the interval or power up reset)
Date & Time	Time stamp	Data are recorded every 15 minutes; the last 30 days of recordings are maintained. Roll-over is at midnight.
UAS	Unavailable Seconds	Seconds in which the interface was out of service.
ES	Errored seconds	The number of seconds in which there was at least one error block.
SES	Severe Errored Seconds	The number of seconds in which the service quality was low as determined by the BBER threshold.
BBE	Background Block Error	The number of errored blocks in an interval.
Min RSL	Minimum Received Signal Level	The value of the smallest signal received during the interval.
Max RSL	Maximum Received Signal Level	The value of the largest signal received during the interval.

Table 5-2: Performance Monitoring Fields (Continued)

Column Heading	Abbreviation Meaning	Description
RSL Thresh 1	Receive Signal Level #1 set in Figure 5-2	Receive Signal Level #1 set in Figure 5-2 .
RSL Thresh 2	Receive Signal Level #2 set in Figure 5-2	Receive Signal Level #2 set in Figure 5-2 .
Min TSL	Minimum Transmitted Signal Level	The value of the smallest signal transmitted during the interval.
Max TSL	Maximum Transmitted Signal Level	The value of the largest signal transmitted during the interval.
TSL Thresh	Transmit Signal Level set in Figure 5-2	Transmit Signal Level set in Figure 5-2 .
BBER Thresh	Background Block Error Ratio Threshold	Background Block Error Ratio Threshold set in Figure 5-2 .
Rx MBytes	Received Mbytes	The number of Megabytes received at the specified port within the interval
Tx MBytes	Transmitted Mbytes	The number of Megabytes transmitted at the specified port within the interval.
Below Capacity Thresh	Threshold set in Figure 5-2	Time in seconds during which the actual traffic was below the threshold signal strength value.
Above Traffic Thresh	Threshold set in Figure 5-2	Time in seconds during which the actual traffic exceeded the threshold signal strength value.

Data becomes invalidated following a reset. In the example below, the Slave ODU was reset shortly after 08:45. All data prior to that time becomes invalidated. The only valid items are the recordings following the re-sync.

Integrity	Date & Time	UAS	ES	SES	BBE	Min RSL (dBm)	Max RSL (dBm)	RSL Thresh 1 (-88 dBm)	RSL Thresh 2 (-88 dBm)	Min TSL (dBm)	Max TSL (dBm)	TSL Thresh (26 dBm)	BBER Thresh (1.0 %)	Rx MBytes
✓	25/02/2014 11:15:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 11:00:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 10:45:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 10:30:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 10:15:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 10:00:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 09:45:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 09:30:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 09:15:00	0	0	0	0	-56	-55	0	0	5	5	0	0	0
✓	25/02/2014 09:00:00	0	0	0	0	-56	-54	3	3	5	5	0	0	0
✗	25/02/2014 08:45:00	0	0	0	0	0	0	0	0	-30	-30	0	0	0
✗	25/02/2014 08:30:00	0	0	0	0	0	0	0	0	-30	-30	0	0	0
✗	25/02/2014 08:15:00	0	0	0	0	0	0	0	0	-30	-30	0	0	0

Figure 5-4: Performance Monitoring report - Showing invalid data

Use the Save button to store the current data to a file and the Clear button to delete currently stored performance data.

5.4.2. More on the Thresholds

RSL Thresholds

Two RSL Thresholds can be defined. They are used as an indicator of problems in the radio channel. You can check the RSS from the Link Budget Calculator results during installation. Values of -5dB and -8dB from the current RSS are typical.

TSL Threshold

A counter is maintained for the number of second intervals during which Tx power exceeds this threshold.

BBER Threshold

The Background Block Error Ratio is measured as a percentage. The threshold can be set from 0.1% up to 50%.

An 8% threshold is recommended. If there are no problems during the interval, then for that threshold, the recommended BBER value should be 0. Since the system provides a lossless Ethernet service, there is throughput degradation in case of interference. The degradation is proportional to the BBER.

Ethernet Thresholds - Capacity

This is used as a basis for checking adherence to a Service Level Agreement. It is the number of seconds count that the link capacity falls below the threshold.

Ethernet Thresholds - Traffic

The number of seconds count that received traffic exceeded this threshold. It can be used to measure traffic peaks.

5.5. Manager Traps

The RADWIN Manager application issues traps to indicate various events displayed in the Events Log.

Table 5-3: RADWIN Manager Trap Messages

Trap Message	Severity	Remarks
Cannot bind to trap service port. Port 162 already in use by ProcessName (pid: ProcessId)	Warning	The RADWIN Manager will not catch any traps from the ODU, some other application has grabbed this port.
Device unreachable!	Error	Check the connectivity to the ODU
Connected to <site_name>	Information	
<site_name> Site will be reset.	Information	
Restore Factory Default Settings in process on Site <site_name>	Information	
Factory Settings: The process was not finished due to connection issues.	Warning	Factory settings failed due to connectivity problems to ODU
Reset: The process was not finished due to connection issues.	Warning	Factory settings failed due to connectivity problems to target - ODU will not be reset
Cannot Write to Monitor file. There is not enough space on the disk.	Warning	Free some space on the disk on the managing computer and retry
Windows Error: <error_ID>. Cannot Write to Monitor file.	Warning	Operating System error on the managing computer
Identical IP addresses at <local_site_name> and <remote_site_name>	Warning	Set up a different IP to each site
The Product is not identified at the <local_site_name> site.	Warning	RADWIN Manager is incompatible with the ODU software version
The Product is not identified at the <remote_site_name> site.	Warning	
The Product is not identified at both sites.	Warning	
Product Not Identified!	Warning	

Table 5-3: RADWIN Manager Trap Messages (Continued)

Trap Message	Severity	Remarks
The Manager identified a newer ODU release at the <remote_site_name> site.	Warning	ODU release is newer than RADWIN Manager release. Wizards are not available. RADWIN Manager will be used just for monitoring. Upgrade the RADWIN Manager. (You will get this message as a pop up)
The Manager identified a newer ODU release at the <local_site_name> site.	Warning	
Newer Version identified at the <local_site_name> site.	Warning	ODU release is newer than RADWIN Manager release. Wizards are not available. RADWIN Manager will be used just for monitoring. Upgrade the RADWIN Manager.
Newer Version identified at the <remote_site_name> site.	Warning	
Newer Version Identified!	Warning	

5.6. Active Alarms

Active Alarms are raised for any event affecting availability or quality of service. They are site specific and are obtained using the site tool bar:



Here is an example:

HSU Active Alarms Haydn@HFU.01.01

Save Refresh

Device Date & Time	Description	Interface
9/1/2005 12:00:00 AM	Management port status changed to disconnected	Management Port on Odu

Here is the table part in more detail:

Device Date & Time	Description	Interface
9/1/2005 12:00:00 AM	Management port status changed to disconnected	Management Port on Odu

Current Active Alarms may be saved to a file. The list displayed will not be updated unless you click Refresh.

5.7. Other Diagnostic Aids

5.7.1. Link Budget Calculator

The Link Budget Calculator is part of the RADWIN Manager software and is found in the Help menu. This useful utility enables you to calculate the expected performance of the wireless link and the possible configurations for a specific link range including antenna size, cable loss and climate conditions. For full details, see the *Site Survey* application note.

➤ **To run the Link Budget Calculator from the Windows Start Menu:**

- Go to Start | Programs | RADWIN Manager | Link Budget Calculator

5.7.2. Online Help

Online help can be accessed from the Help menu on the main window of the RADWIN Manager. Using most common Web browsers, it may also be run going to

Start | Programs | RADWIN Manager | User Manual RADWIN 5000

5.7.3. Customer Service

Customer support for this product can be obtained from the local VAR, Integrator or distributor from whom it was purchased.

Chapter 6: Backup, Restore, and Upgrade

6.1. Scope of this Chapter

This chapter shows you how to back up and restore the software as well as the link configuration in addition to upgrading the software.

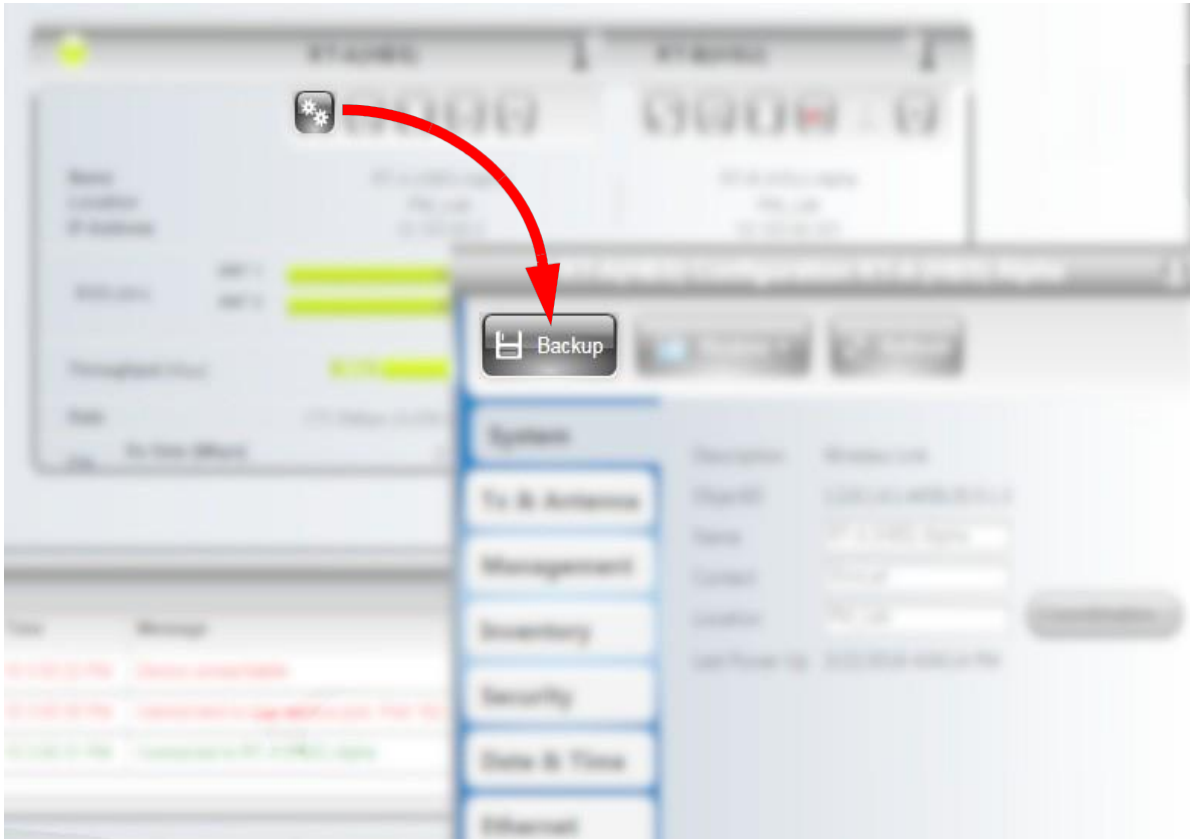
You can back up the radio unit software for a complete link (Bulk Backup) or a single site. The Restore facility is selective: You may restore backed up radio units one at a time. The restore may be the full software or just the configuration settings.



A backup (full or configuration only) may be restored to another radio unit provided that the product IDs and revision levels of the source and target radio units are identical. They are shown in the radio unit Inventory window.

6.2. System & Site Backup

1. In the RADWIN Manager, from the RT-A(HBS), open the Configuration window, then click the Backup button:



2. A Windows dialog will open prompting you to save the backup file. Save the backup file in a convenient location.
 - > This backup file has a name constructed from the IP address of the selected unit and the present date.
 - > The file is used to carry out both a Configuration Restore, and a Full Restore.
 - > If you have chosen the RT-A(HBS), the file includes *all* system and software information for the unit and the link.
 - > If you have chosen the RT-B(HSU), the file includes software information for the selected unit only.

6.3. Bulk Software Backup

➤ **To back up a link:**

1. Go to Tools | Bulk Backup:



The following detached window appears:

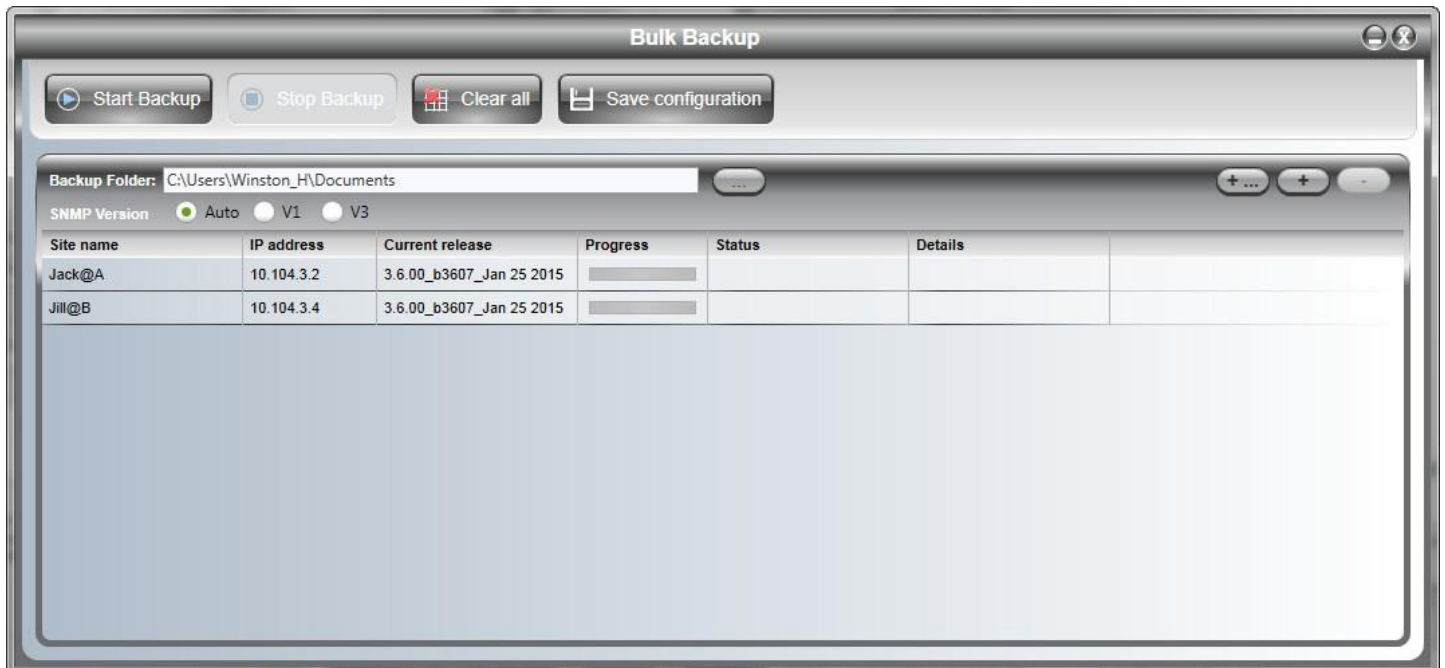


Figure 6-1: Bulk Backup setup window

The default sites shown in the Bulk Backup list panel belong to the currently installed link. The list may be empty if you are running the RADWIN Manager “offline”.

2. The Bulk Backup list title bar has three buttons on the right-hand side.



Figure 6-2: Add / Remove site buttons

The left button opens a Windows file dialog to locate a list of locations to backup. The list has the following format for SNMPv1:

<IP address>,<Read-Only community>,<Read-Write community> For SNMPv3 it is:

<IP address>,<Dummy>,<User_type ><Password> For example:

10.104.3.2,netman,admin,netwireless

10.104.3.4,netman,admin,netwireless

A PtMP list will contain the HBS and registered HSUs. The center button allows you to add a single site:



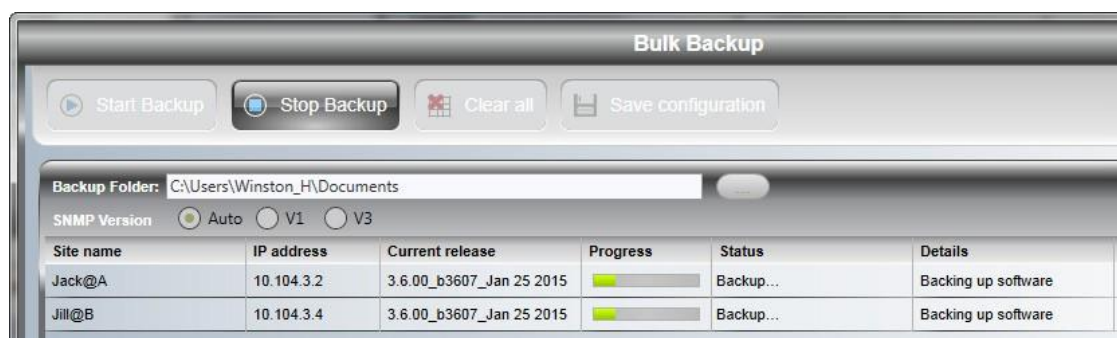
Figure 6-3: Adding a single site for backup

Enter the IP address of the site, the Read-Write Community (Default: *netman*) and then click OK. The site will appear in the Software Upgrade list box.

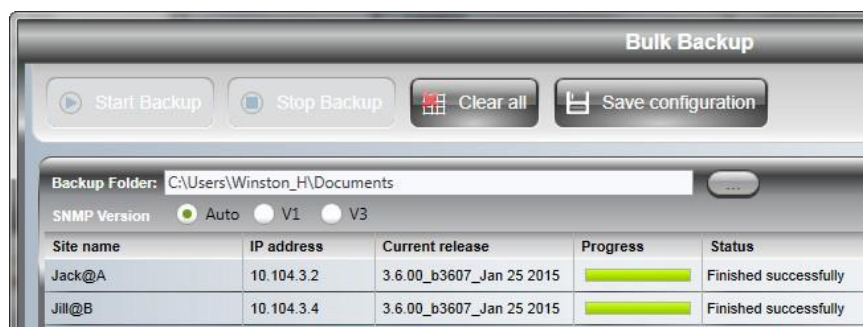
Items from the list can be cleared by selecting them and then using the right button.

The right button may be re-used to remove one or more selected sites.

3. You may choose the SNMP version but probably it should be best left at your log-on setting.
4. Click the Start Backup button. Progress bars indicate backup status.



The success or failure of the backup is displayed on completion:



Save Configuration produces a text file in the format of the above example for backing up an installed link.

The files produced by the above process are:

10.104.3.4_29.01.2015.backup

10.104.3.2_29.01.2015.backup

BulkBackupConfig_2015_01_29.txt

Notice that the files are date stamped. The first two files are binary. The last is the save-configuration text file:

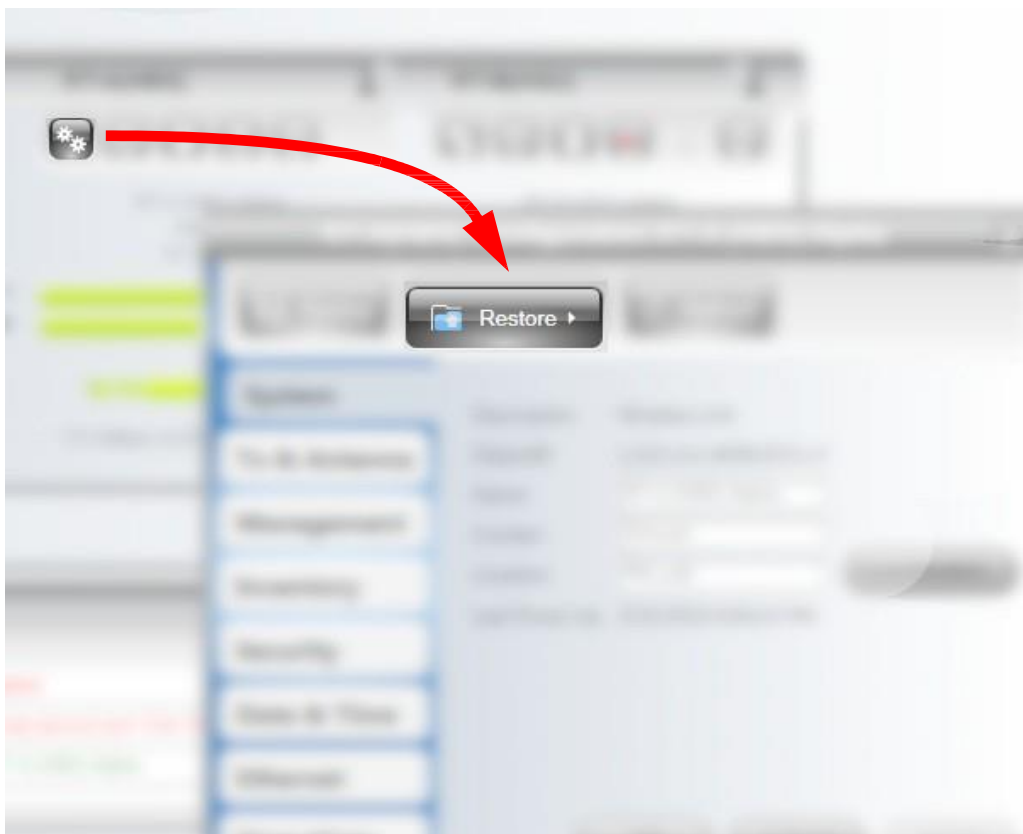
10.104.3.2,netman,admin,netwireless

10.104.3.4,netman,admin,netwireless

The backup files are identical in naming convention and format to those produced on a site-by-site basis.

6.4. System & Site Restore

3. In the RADWIN Manager, from the RT-A(HBS), open the Configuration window, then click the Restore button:



The Restore button offers two extra options, Configuration Restore or Full Restore.



Configuration Restore just restores configuration settings, whereas Full Restore reverts the radio unit software to the backed-up version.

6.5. Upgrading an Installed Link

➤ **To upgrade software for a link:**

1. In the RADWIN Manager, click the Tools | Software Upgrade button. The following detached window appears:

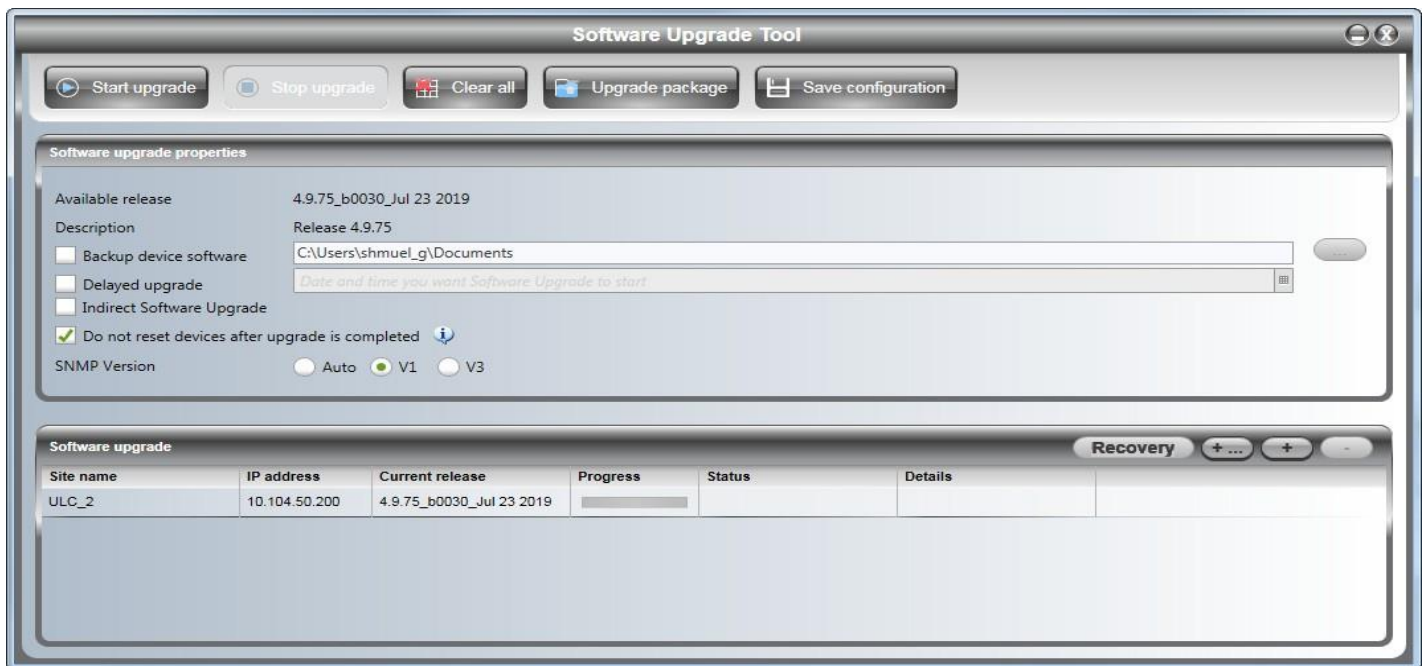




Figure 6-4: Software Upgrade Utility - Main window

The default sites shown in the Software Upgrade list panel belong to the currently installed sector. The list may be empty if you are running the RADWIN Manager “offline”.

2. To back up your existing system, check Backup device software checkbox. Then 

click the  button for a standard file dialog. The default location is the My Documents directory on the managing computer or the last backup directory you used.

3. In addition to the previous step, you may opt to perform a delayed upgrade. Check the **Delayed Upgrade** box and enter the date and time for the delayed upgrade.

4. **Indirect Software Upgrade** - allows you to upgrade the units without having to define their IP addresses. Note that this does not work if the sector uses IPv6, or you have chosen to use HTTP as the file transfer protocol (available for RADWIN 2000 Alpha EMB or RADWIN 2000 Alpha Integrated units only).
5. Choose the SNMP version of the units: V1, V3 or Auto.
6. The Software upgrade list title bar has three buttons on the right-hand side.



Figure 6-5: Add / Remove site buttons

The left button opens a Windows file dialog to locate a list of locations to update. The list has the following format:

<IP address>,<Read-Only community>,<Read-Write community>

For example:

10.104.3.2,netman

10.104.3.4,netman

The list should include RT-A(HBS)s and RT-B(HSU)s able to accept the same upgrade. Non-upgradable items will result in an error message. Contact Customer Service about upgrading them.

The center button allows you to add a single site:



Figure 6-6: Adding a single site for upgrade



Enter the IP address of the site and the Read-Write Community (Default: *netman*). If you are a SNMPv3 user, add your username and password and then click OK. The site will appear in the Software Upgrade list box.

Items from the list can be cleared by selecting them and then using the right button.

The right button in [Figure 6-3](#), may be used to remove one or more selected sites.

7. Having created an update list, click Upgrade Package to choose the relevant files. The default files are located in the SWU subdirectory in the RADWIN Manager installation area.

For RADWIN 2000-Plus Family, always choose the SWU_5k.swu file (Not the 2k package).

8. **Do not reset** this option instructs the RADWIN Manager to not reset the units after the upgrade is done. Note that even if you select this option, if you are upgrading the RADWIN 2000 Alpha EMB or RADWIN 2000 Alpha Integrated, the unit will be reset in any case.
9. **Recovery:** If a unit has failed an upgrade, you can attempt an upgrade to a new software version, but with the factory default settings (except IP address). To upgrade in this manner, click the **Recovery** button () and follow the instructions on screen.
10. To back up your existing system, check Backup device software checkbox. Then click the  button for a standard file dialog. The default location is the My Documents directory on the managing computer or the last backup directory you used.



The backup here is the same as that in [Backup and Restore](#) and serves the same purpose. It provides a fallback if the upgrade proves problematic.

11. In addition to the previous step, you may opt to perform a delayed upgrade. Check the Delayed Upgrade box and enter the date and time for the delayed upgrade.
12. The radio button determines how your radio units should be reset. Bear in mind that on the one hand, a reset involves a service interruption, but on the other hand, the software upgrade will not become effective until after the reset is carried out.
13. Click Start Upgrade to commence the process. For an immediate update, you can observe the upgrade progress from the green progress bars:

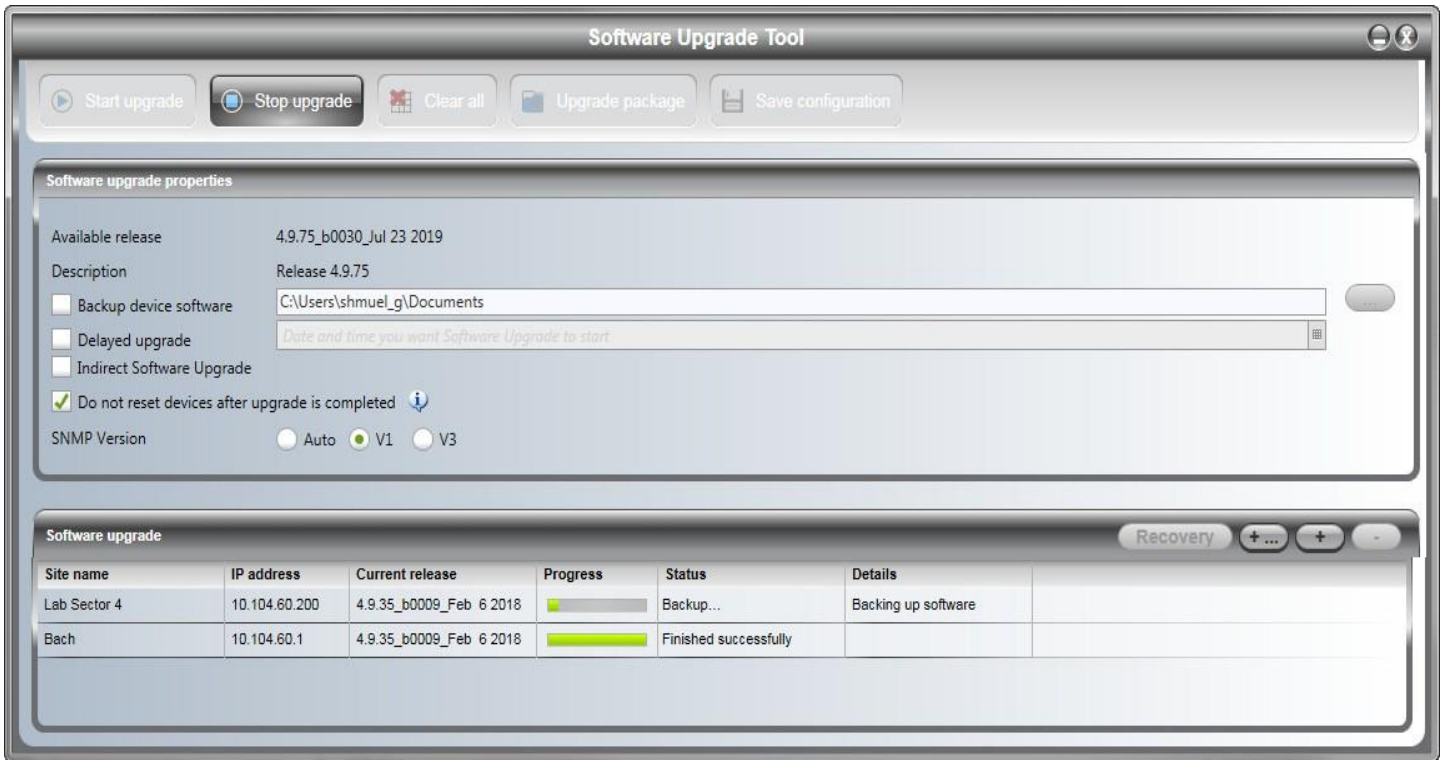


Figure 6-7: Software upgrade in progress - Note the **Stop upgrade** button

Software upgrade				
Site name	IP address	Current release	Progress	Status
Jack@A	10.104.3.2	3.6.00_b3606_Jan 20 2015	<div style="width: 100%; height: 10px; background-color: #90EE90;"></div>	Reset done
Jill@B	10.104.3.4	3.6.00_b3606_Jan 20 2015	<div style="width: 100%; height: 10px; background-color: #90EE90;"></div>	Reset done

Figure 6-8: Software upgrade completed successfully

14. Use the title bar exit button to dismiss the Software upgrade window.



Caution

If any sites fail to update, a warning notice will be displayed. If one or more sites of a sector update fails, you should correct the problem and update the failed sites as soon as possible. If you do not, following the next reset of the updated sites, you could experience a link software mismatch which may affect service.

Chapter 7: VLAN Functionality

7.1. Scope of this Chapter

This chapter describes how the components of a RADWIN 2000-Plus Family link deal with VLAN tagging and untagging.

7.2. VLAN Tagging - Overview

7.2.1. VLAN and Related Terminology

Both the technical literature and the RADWIN Manager use the terms VLAN ID and VID interchangeably to denote a VLAN identification number.

Reminder: RT-A(HBS) always means the Master ODU and RT-B(HSU) always means the Slave ODU.

7.2.2. VLAN Background Information on the Web

The standards defining VLAN Tagging are IEEE_802.1Q and extensions.

For general background about VLAN see http://en.wikipedia.org/wiki/Virtual_LAN.

Background information about Double Tagging also known as QinQ may be found here: <http://en.wikipedia.org/wiki/802.1QinQ>.

7.3. Requirements

It is assumed that you are familiar with VLAN usage and terminology.

7.4. VLAN Tagging

VLAN tagging enables multiple bridged networks to transparently share the same physical network link without leakage of information between networks:

IEEE 802.1Q is used as the encapsulation protocol to implement this mechanism over Ethernet networks.

7.4.1. QinQ (Double Tagging) for Service Providers

QinQ is useful for Service Providers, allowing them to use VLANs internally in their “transport network” while mixing Ethernet traffic from clients that are already VLAN-tagged.

The outer tag (representing the Provider VLAN) comes first, followed by the inner tag. In QinQ, the EtherType = 0x9100. VLAN tags may be stacked three or more deep.

When using this type of “Provider Tagging”, you should keep the following in mind:

- Under Provider Tagging, the system double-tags egress frames towards the Provider’s network. The system adds a tag with a VLAN ID and EtherType = 0x9100 to all frames, as configured by the service provider (Provider VLAN ID).
- The system always adds tags to each frame with VLAN ID and EtherType = 0x9100. Therefore,
 - > For a frame without a tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will have one tag
 - > For a frame with a VLAN tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will be double-tagged

For a frame with a VLAN tag and a provider tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will be triple-tagged and so on.

At the egress side, the RT-B(HSU) removes the QinQ tag with EtherType = 0x9100 no matter what the value of its VLAN ID.

7.4.2. VLAN Untagging

VLAN Untagging means the removal of a VLAN or a Provider tag.

7.4.3. Port Functionality



In a 2000-Plus link, all VLAN activity is configured and supported from the RT-B(HSU).

To this end, VLAN functionality is supported at the LAN port of the RT-B(HSU).

The RT-B(HSU) LAN port can be configured to handle Ethernet frames at the ingress direction (where frames enter the RT-B(HSU)) and at the egress direction (where frames exit the RT-B(HSU)).

Ingress Direction

Table 7-1: Port settings - Ingress direction

Transparent	The port 'does nothing' with regard to VLANs - inbound frames are left untouched.
Tag	<p>Frames entering the RT-B(HSU) port without VLAN or QinQ tagging are tagged with VLAN ID and Priority^a, which are preconfigured by the user. Frames which are already tagged at ingress are not modified and pass through.</p> 
Provider tag	<p>Frames entering the RT-B(HSU) port are tagged with provider's VLAN ID and Priority which are preconfigured by the user. Frames which are already tagged with Provider tagging at the ingress are not modified and passed through.</p> 


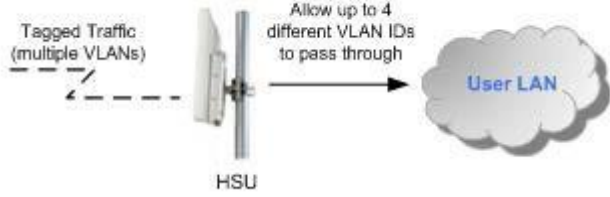
a. Priority Code Point (PCP) refers to the IEEE 802.1p priority. It indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc).

Egress Direction

Table 7-2: Port settings - Egress direction

Transparent	The port 'does nothing' with regard to VLANs - outbound frames are left untouched.
--------------------	--

Table 7-2: Port settings - Egress direction (Continued)

<p>Untag all</p>	<p>Port configured to untag user VLAD tags for all frames.</p> 
<p>Filter</p>	

7.5. VLAN Configuration Using the RADWIN Manager



Caution

Incorrect VLAN configuration may cause havoc on your network. The facilities described below are offered as a service to enable you to get best value from your RADWIN 2000-Plus Family links and are provided “as is”. Under no circumstances does RADWIN accept responsibility for network system or financial damages arising from incorrect use of these VLAN facilities.

7.5.1. Management Traffic and Ethernet Service Separation

You can define a VLAN ID for management traffic separation. You should configure the system to prevent conflicts as detailed below.

When configured for the default operational mode, a “Provider port” will handle ingress traffic as follows:

- Filters frames that are not tagged with the Provider VLAN ID
- Removes the Provider double tag

Therefore, if a port is configured for management traffic separation by VLAN and as ‘Provider port’, then the received management frames must be double tagged as follows:

- The outer tag has to be the Provider’s tag (so the frame is not filtered)

- The internal tag has to be management VLAN ID

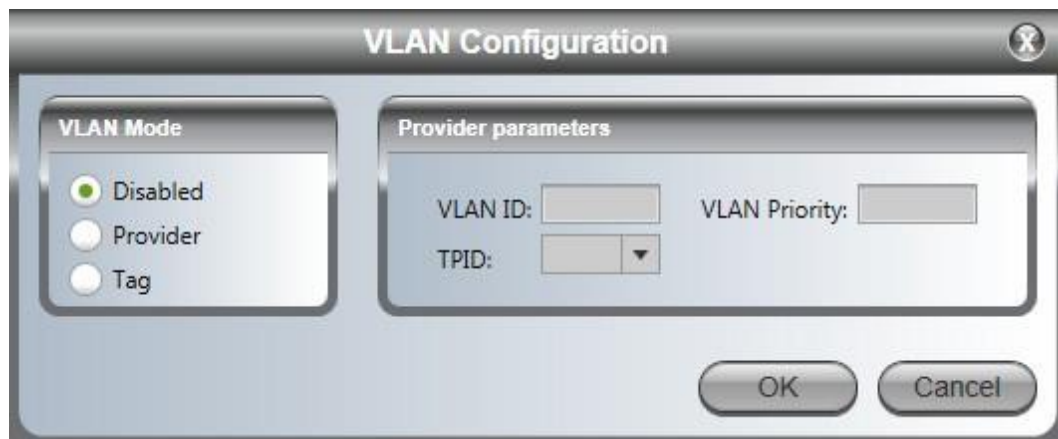
To avoid mix-ups, best practice is to:

- Separate the management and data ports
- Define only a data port with Provider function

7.5.2. Configuration of VLAN Tagging for Ethernet Service

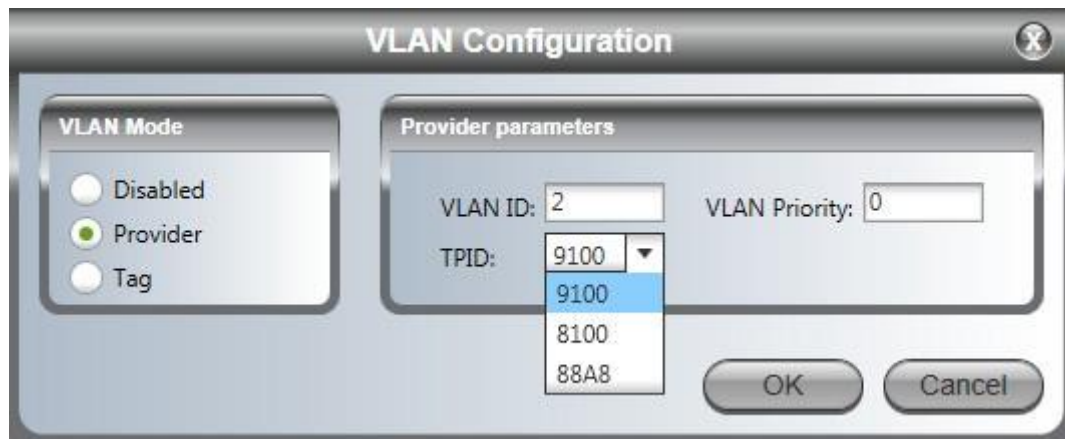
➤ To set up an RT-B(HSU) for VLAN tagging:

1. Open Link Configuration -> Ethernet and then click the VLAN Configuration button.



In Disabled mode, Ethernet frames pass transparently over the radio links.

2. For Provider tagging, click the Provider Radio button:



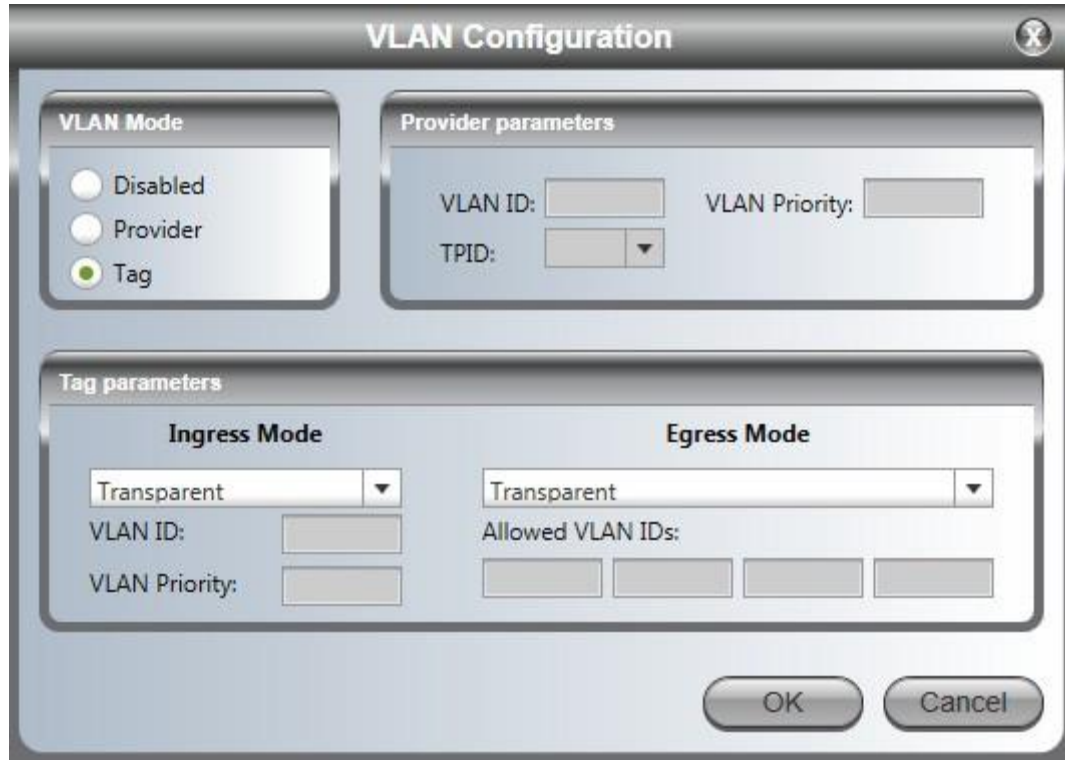
In Provider mode, Ethernet frames are tagged with the provider's VLAN ID before they enter into the provider's network/backbone.

3. Enter a Provider VLAN ID and Priority. The VLAN ID must be in the range 2 to 4094. The VLAN Priority must be in the range 0 to 7. You may also change the TPID from the default as shown.
4. Click OK to accept.



This facility is provided to enable connection through legacy switches requiring it. Otherwise, there is no need to change the TPID.

- For user VLAN tagging, click the Tag Radio button:



In Tag mode, Ethernet frames are tagged or untagged to distinguish between different networks.

- For completely transparent passage of tagged frames, there is nothing further to do. [Table 7-3](#) shows the possible settings for each combination of Ingress and Egress modes.
- Click OK.

Table 7-3: Further VLAN Configuration options and results by Tag mode

Ingress	Egress			
	Transparent	Untag All	Untag Filtered	Filter
Transparent	Frames are not modified and are forwarded transparently	All frames with VLAN tag are untagged ^a	Allow VLAN IDs: Allow up to 4 VIDs to be passed through. ^b Untag VLAN IDs: Untag the VLAN tag of the selected VLAN IDs.	Allow up to 4 VIDs to be passed through. ^c

Tag: Enter a VID (1-4094) and Priority (0-7) ^d	Frames are not modified and are forwarded transparently	All frames with VLAN tag are untagged	Allow up to 4 VLANs to be passed through	Allow up to 4 VLANs to be passed through
--	---	---------------------------------------	--	--

- a. Frames with Provider Tag 9100 or 88A8 will be passed through transparently
- b. For frames with Provider Tag 8100, the filter will be applied to the outer tag
- c. For frames with Provider Tag 8100, the filter will be applied to the outer tag
- d. Frames with Provider Tag 8100 at egress will be stripped of the outer tag



Chapter 8: Quality of Service

8.1. Scope of this Chapter

This chapter describes how to set various levels of Quality of Service (QoS) for a RADWIN 2000-Plus Family link.

8.2. Prerequisites

To use the facility, you must be familiar with the use of VLAN (802.1p) or Diffserv.

8.3. QoS - Overview

QoS is a technique for prioritization of network traffic packets during congestion.

RADWIN 2000-Plus Family links support two classification criteria, VLAN based or Diffserv based. You may choose which of them to use.

Table 8-1: Default priorities and allocation by VLAN ID and Diffserv

Quality queue	Priority	
	Diffserv	VLAN
Real time	48-63	6-7
Near real time (responsive applications)	32-47	4-5
Controlled load	16-31	2-3
Best effort	0-15	0-1

Based upon the classification criterion chosen, received packets will be mapped into one of four quality groups: Real time, Near real time, Controlled load and Best effort.

You may partition the total link capacity across the four Quality queues. The default weights as percentages are shown in [Table 8-1](#).

8.4. Setting up the Link for QoS

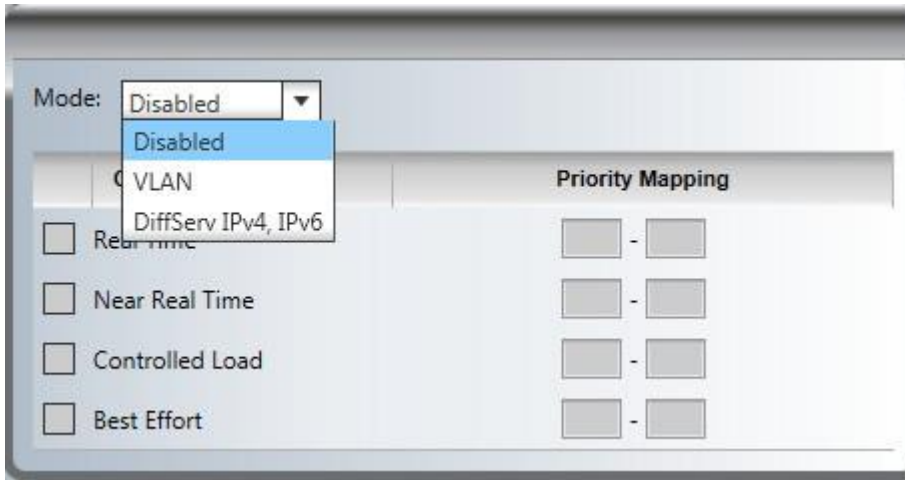
8.4.1. Preparing for QoS

Open Link Configuration -> Ethernet, then click the QoS Configuration button.

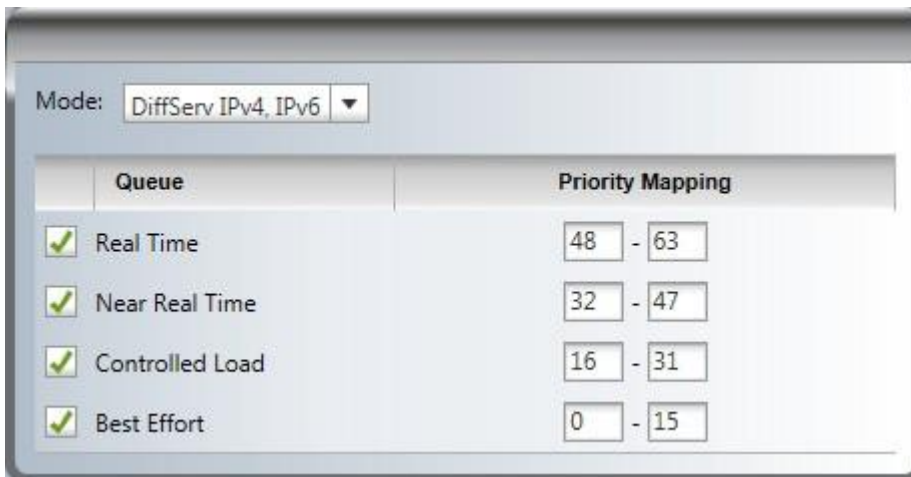


Figure 8-1: QoS Configuration window

QoS is disabled by default. You may choose between the VLAN (802.1p) and Diffserv methods.



The default settings for Diffserv and VLAN are as shown in the next two figures:



If you un-check a queue, it will be disabled for the link. It will not prevent the Slave ODU from configuring it as “live”. The purpose behind this is to avoid the necessity of reconfiguring QoS for the Slave ODU, should the queue be reinstated.

8.4.2. Assigning Queue Priorities

Four mechanisms are available to control queue performance:

- **Strict** - An over-the-air packet is loaded first with data from Real Time queue (see [Figure 8-2](#)), and then from the remaining queues in order. If there is too much data for the first queue, it will “starve” the lower queues and so on.
- **Weight** - One solution to such “starvation” is to weight input flow to the four queues. This could still lead to wasted resources. If in the example below, the actual traffic is all Near Real Time, only 20% will be allocated to Near real time and the rest will be held up.
- **Maximum Information Rate (MIR)** - This is a simple throttle mechanism, which suffers from a drawback similar to the previous case.
- **Time to Live (TTL)** in ms - This device is used to reduce re-transmits of real time data (such as voice or viewed video).



To configure queue priorities for uplink and downlink in turn:

1. For each queue, both downlink and uplink enter the required weight, MIR and TTL. The MIR and TTL may respectively be left Unlimited and Disabled in which case the system will use a “best effort” method.

If you exceed 100% total weight, you will receive an error message.

	Queue	Strict / Weight [%]	Maximum Information Rate [Mbps]	Configurable TTL [ms]
<input checked="" type="checkbox"/>	Real Time	<input type="checkbox"/> 15	0.5 100 <input checked="" type="checkbox"/> Unlimited	5 500 <input checked="" type="checkbox"/> Disabled
<input checked="" type="checkbox"/>	Near Real Time	<input type="checkbox"/> 20	0.5 100 <input checked="" type="checkbox"/> Unlimited	5 500 <input checked="" type="checkbox"/> Disabled
<input checked="" type="checkbox"/>	Controlled Load	<input type="checkbox"/> 25	0.5 100 <input checked="" type="checkbox"/> Unlimited	5 500 <input checked="" type="checkbox"/> Disabled
<input checked="" type="checkbox"/>	Best Effort	<input type="checkbox"/> 42	0.5 100 <input checked="" type="checkbox"/> Unlimited	5 500 <input checked="" type="checkbox"/> Disabled

Total queue weights can't exceed 100.

Figure 8-2: The four QoS data queues

You will be required to correct this before leaving the window other than by cancellation.

If you are under-booked, for example by setting a queue to zero, the unused weight will be distributed to the remaining queues. The effect of doing this will only become apparent under congestion. In particular, a queue set to zero weight will become nearly blocked under congestion with packets passing through on a best effort basis.

2. When you complete your entries, in the QoS Configuration window ([Figure 8-1](#)), click OK to save them and continue.

Chapter 9: FCC/ISED DFS Considerations

9.1. Scope of this Chapter

This chapter describes the criteria for registering devices of a RADWIN 2000-Plus Family link in the WISPA database, and if any should be registered, how to do so.

9.2. FCC 5.4GHz Device Registration

The FCC requires that devices installed within 35 km of any TDWR location should be registered in the voluntary WISPA sponsored database.

The FCC has published a TDWR Location Information table that lists the exact location of all TDWR towers (see [Table 9-1](#) at the end of the chapter).

1. When installing a 5.4 GHz device, define your exact location (latitude and longitude).
2. Use the TDWR Location Information table to determine if the distance between the device and any TDWR tower is less than 35 km.
3. If the distance is less than 35 km, then register the device in the voluntary WISPA sponsored database (following section).
4. (For ISED only): Disable the frequencies between 5570 – 5680 MHz from the available channels list.
5. (For ISED only): The frequency range between 5.600 to 5.650 GHz is not included in the available channels list.

9.3. Registering the Device

➤ **To register a device:**

1. Enter the website <http://www.spectrumbridge.com/udia/home.aspx> and follow the instructions.

At your first entry into the site, you will be required to register as a user:

The screenshot shows the WISPA (Wireless Internet Service Providers Association) website. The header features the WISPA logo and a search bar. Below the header, there are navigation links for 'Overview' and 'Search', and a 'User Signup | Login' link. The main content area is titled 'UNII Device Interference Advisor (UDIA)' and is powered by SPECTRUM BRIDGE. The page includes a large image of a radar tower and a 'Search for Terminal Doppler Weather Radars' button. Below the image, there is a link to an 'FCC Memorandum on UNII Device Operation Do Your Part To Share The Air UDIA Press Release'. The text describes the UDIA as an online database and registry for Terminal Doppler Weather Radar (TDWR) systems and registered UNII devices. It lists two main functions: searching for devices within 35 km of TDWR sites and voluntarily registering technical information. A prominent 'User Registration' button is visible. The background section explains that TDWRs are strategically placed near 47 major airports and that their frequencies (5.60-5.65 GHz) are shared with UNII frequencies (5.47-5.725 GHz). The UDIA database was developed to promote cooperation between the FCC, the FAA, and the wireless industry.

2. Click the User Registration button to enter the registration page.

WISPA[®]
Wireless Internet Service Providers Association

Overview Search User Signup | Login

User Registration

Already have an account? [Sign in](#)

Email (This will be your username)

First Name

Last Name

Business Name

Phone

Country

Address

City

State/Province

Zip/Postal Code

Type of Registrant

Security Question

Security Answer

Password

Confirm Password

Powered by: SPECTRUM BRIDGE

3. Fill in the registration page and click Register.
4. To complete device registration enter the Register Device tab as shown:



You are offered this:

WISPA®
Wireless Internet Service Providers Association

Overview Search Device Management My Account Logout

UMB Device Registration

Fields marked with a * are required

Location Data

Degrees / Minutes / Seconds/Decimal

Latitude North/South

Longitude East/West

Don't know the coordinates? [Click here](#)

Ground Elevation Meters

Antenna Height Meters

Add Address Add

Equipment Data

FCCID

External Antenna Model*

Radio Model

Radio Manufacturer

Radio Serial Number

Building/Tower Contact Person*

Active Indicates the device is currently active
 Indicates the device can be viewed by all registered users.

General Access

Register Device

Powered by **SPECTRUM BRIDGE**

Copyright © 2010 Spectrum Bridge, Inc.
All rights reserved. All trademarks are the property of their respective owners.

- Fill in the required information in the preceding web page and click the Register Device button.

9.4. TDWR Table

The following table contains the latitude and longitude locations of the Terminal Doppler Weather Radars (TDWR). Use this table to determine if the Master or Client device installed is within 35 km radius of a TDWR location. If one of the installed devices is within 35 km radius of any TDWR location, then disable all frequencies between 5570 – 5680 MHz from the available channels list.

Table 9-1: Latitude and longitude locations of TDWRs

STATE	CITY	LONGITUDE	LATITUDE	FREQUENCY	TERRAIN ELEVATION (MSL) [ft]	ANTENNA HEIGHT ABOVE TERRAIN [ft]
AZ	PHOENIX	W 112 09 46	N 33 25 14	5610 MHz	1024	64
CO	DENVER	W 104 31 35	N 39 43 39	5615 MHz	5643	64
FL	FT LAUDERDALE	W 080 20 39	N 26 08 36	5645 MHz	7	113
FL	MIAMI	W 080 29 28	N 25 45 27	5605 MHz	10	113
FL	ORLANDO	W 081 19 33	N 28 20 37	5640 MHz	72	97
FL	TAMPA	W 082 31 04	N 27 51 35	5620 MHz	14	80
FL	WEST PALM BEACH	W 080 16 23	N 26 41 17	5615 MHz	20	113
GA	ATLANTA	W 084 15 44	N 33 38 48	5615 MHz	962	113
IL	MCCOOK	W 087 51 31	N 41 47 50	5615 MHz	646	97
IL	CRESTWOOD	W 087 43 47	N 41 39 05	5645 MHz	663	113
IN	INDIANAPOLIS	W 086 26 08	N 39 38 14	5605 MHz	751	97

Table 9-1: Latitude and longitude locations of TDWRs (Continued)

STATE	CITY	LONGI- TUDE	LATITUDE	FRE- QUENC Y	TER- RAIN ELEVA- TION (MSL) [ft]	ANTEN NA HEIGH T ABOVE TER- RAIN [ft]
KS	WICHITA	W 097 26 13	N 37 30 26	5603 MHz	1270	80
KY	COVINGTON CIN- CINNATI	W 084 34 48	N 38 53 53	5610 MHz	942	97
KY	LOUISVILLE	W 085 36 38	N 38 02 45	5646 MHz	617	113
LA	NEW ORLEANS	W 090 24 11	N 30 01 18	5645 MHz	2	97
MA	BOSTON	W 070 56 01	N 42 09 30	5610 MHz	151	113
MD	BRANDYWINE	W 076 50 42	N 38 41 43	5635 MHz	233	113
MD	BENFIELD	W 076 37 48	N 39 05 23	5645 MHz	184	113
MD	CLINTON	W 076 57 43	N 38 45 32	5615 MHz	249	97
MI	DETROIT	W 083 30 54	N 42 06 40	5615 MHz	656	113
MN	MINNEAPOLIS	W 092 55 58	N 44 52 17	5610 MHz	1040	80
MO	KANSAS CITY	W 094 44 31	N 39 29 55	5605 MHz	1040	64
MO	SAINT LOUIS	W 090 29 21	N 38 48 20	5610 MHz	551	97
MS	DESOTO COUNTY	W 089 59 33	N 34 53 45	5610 MHz	371	113
NC	CHARLOTTE	W 080 53 06	N 35 20 14	5608 MHz	757	113
NC	RALEIGH DURHAM	W 078 41 50	N 36 00 07	5647 MHz	400	113

Table 9-1: Latitude and longitude locations of TDWRs (Continued)

STATE	CITY	LONGI- TUDE	LATITUDE	FRE- QUENC Y	TER- RAIN ELEVA- TION (MSL) [ft]	ANTEN NA HEIGH T ABOVE TER- RAIN [ft]
NJ	WOODBIDGE	W 074 16 13	N 40 35 37	5620 MHz	19	113
NJ	PENNSAUKEN	W 075 04 12	N 39 56 57	5610 MHz	39	113
NV	LAS VEGAS	W 115 00 26	N 36 08 37	5645 MHz	1995	64
NY	FLOYD BENNETT FIELD	W 073 52 49	N 40 35 20	5647 MHz	8	97
OH	DAYTON	W 084 07 23	N 40 01 19	5640 MHz	922	97
OH	CLEVELAND	W 082 00 28	N 41 17 23	5645 MHz	817	113
OH	COLUMBUS	W 082 42 55	N 40 00 20	5605 MHz	1037	113
OK	AERO. CTR TDWR #1	W 097 37 31	N 35 24 19	5610 MHz	1285	80
OK	AERO. CTR TDWR #2	W 097 37 43	N 35 23 34	5620 MHz	1293	97
OK	TULSA	W 095 49 34	N 36 04 14	5605 MHz	712	113
OK	OKLAHOMA CITY	W 097 30 36	N 35 16 34	5603 MHz	1195	64
PA	HANOVER	W 080 29 10	N 40 30 05	5615 MHz	1266	113
PR	SAN JUAN	W 066 10 46	N 18 28 26	5610 MHz	59	113
TN	NASHVILLE	W 086 39 42	N 35 58 47	5605 MHz	722	97
TX	HOUSTON INTER- CONTL	W 095 34 01	N 30 03 54	5605 MHz	154	97

Table 9-1: Latitude and longitude locations of TDWRs (Continued)

STATE	CITY	LONGI- TUDE	LATITUDE	FRE- QUENC Y	TER- RAIN ELEVA- TION (MSL) [ft]	ANTEN NA HEIGH T ABOVE TER- RAIN [ft]
TX	PEARLAND	W 095 14 30	N 29 30 59	5645 MHz	36	80
TX	DALLAS LOVE FIELD	W 096 58 06	N 32 55 33	5608 MHz	541	80
TX	LEWISVILLE DFW	W 096 55 05	N 33 03 53	5640 MHz	554	31
UT	SALT LAKE CITY	W 111 55 47	N 40 58 02	5610 MHz	4219	80
VA	LEESBURG	W 077 31 46	N 39 05 02	5605 MHz	361	113
WI	MILWAUKEE	W 088 02 47	N 42 49 10	5603 MHz	820	113

Chapter 10: Spectrum View

10.1. Scope of this Chapter

This chapter shows how to use the Spectrum View tool. We assume that the reader knows about RF Spectrum Analysis

10.2. What is Spectrum View

The RADWIN Manager Spectrum View utility is an RF survey tool designed to support the link installation prior to full link service activation. The tool provides comprehensive and clear spectral measurement information enabling easier, faster and better quality installations.

You can view real-time spectrum information, save the spectral information and view retrieved spectral information from historic spectrum scans.

Separate information is generated for the Slave and Master - all by selection.

RADWIN's spectrum measurement and estimation algorithms are designed to show accurate information accommodating variations in frequency, temperature and interference power and at the same time overcoming anomalies that tend to occur in high interference environments.

10.3. Who needs it

As indicated in the previous paragraph, Spectrum View is primarily a professional tool for the technician. The Spectrum View reports may be generated as images, CSV files or text files as part of the Get Diagnostics feature. All of these are intended for use by to RADWIN Customer Service to assist with diagnosing interference related problems.

10.4. Two Ways to Run Spectrum View

Spectrum View may be run from RT-A(HBS) in which case you have a choice of analyzing both sites in the link in one run or choosing just one.

Spectrum View may also be run on a managing computer directly connected to the RT-B(HSU). Remember that, in such a case, the results will be quite different if the RT-B(HSU) is already part of a link (registered or not) or if it is completely a stand-alone, for example using a different spectral range and operating Band from the RT-A(HBS). In the former case, expect a “noise hump” around the channels used by the link due to the duty signals from the RT-A(HBS).

10.5. Where is the Spectrum View Data stored

Spectrum View data is always stored in the ODU originating the analysis. The RT-A(HBS) maintains the last Spectrum View analysis data for both members of the link. If you run Spectrum View from a directly connected ODU, it stores its own data, which may be quite different from the analysis obtained for the same RT-B(HSU) from the RT-A(HBS).

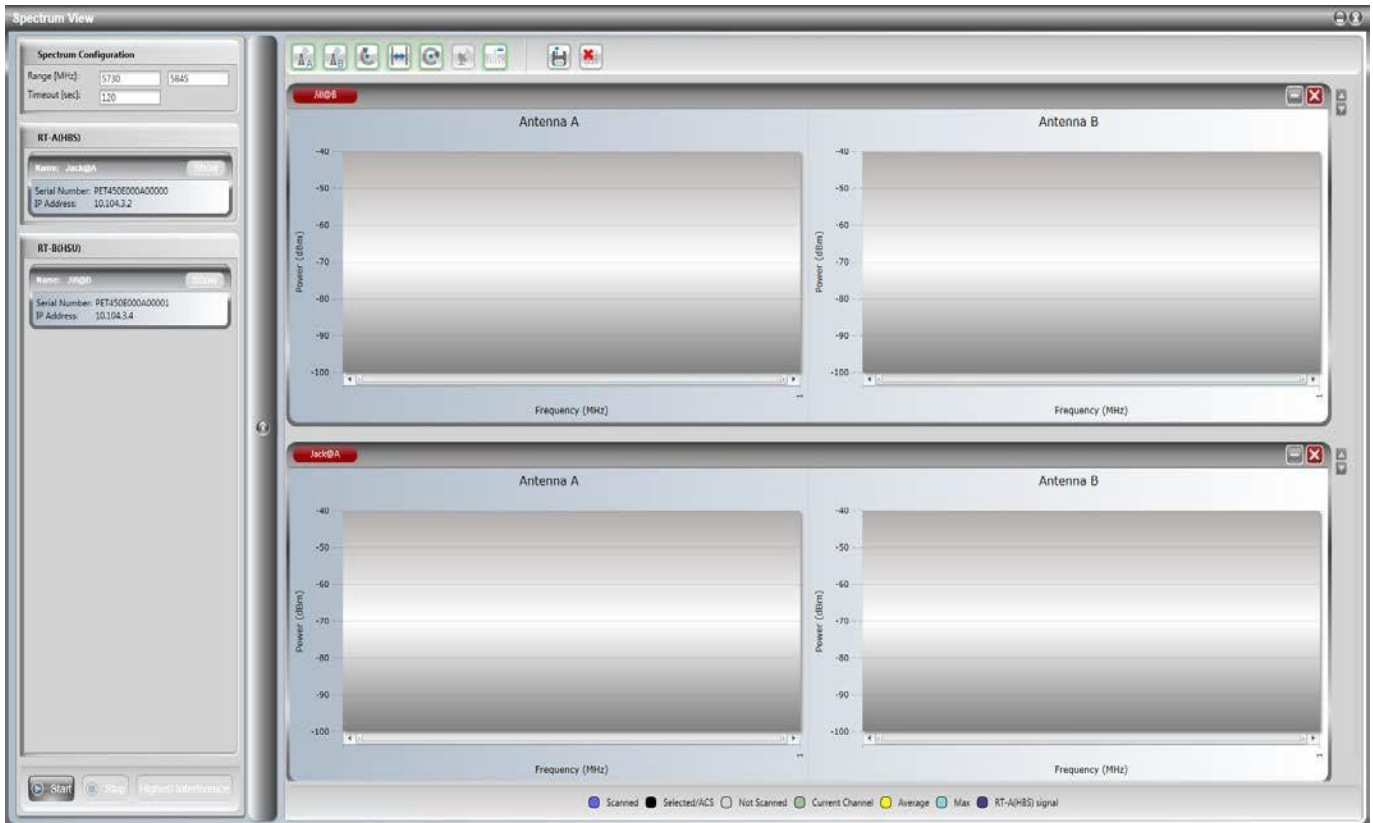
10.6. Spectrum View Main Window

In this section, we review the main window management controls.

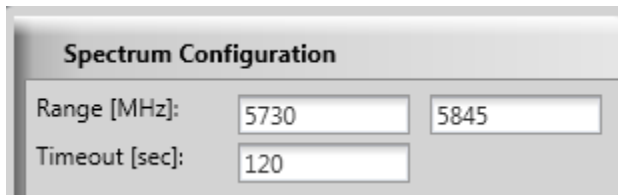
From the Tools tab, choose Spectrum View.



The Spectrum View main window opens in full screen mode:



Use the top left panel to set the Spectrum View configuration parameters and choose an analysis type - Entire link or Specific ODU.



The settings are “sticky” for the link and will be reused. The analysis range is limited from 4900 to 6050 MHz with a maximum difference of 500MHz. Erroneous entries will be shown

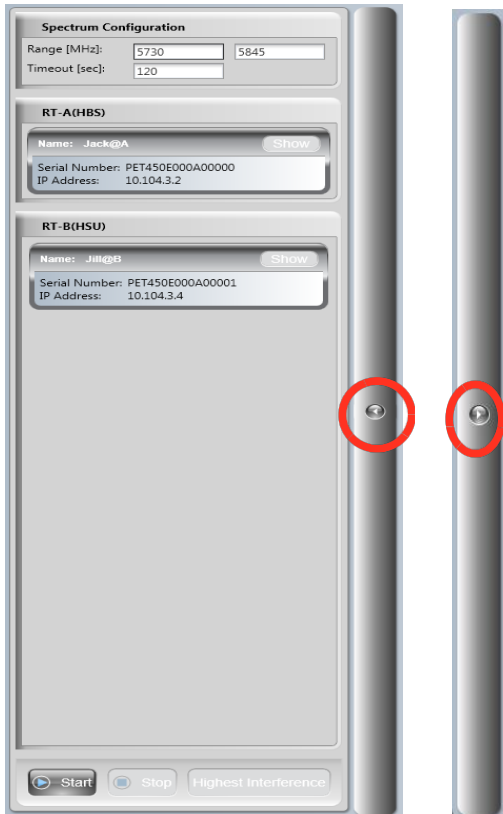


with a red border like this:

The timeout is the maximum analysis time per site. Use the bottom button bar to start or stop an analysis:



Since a large link will clutter up the right-hand display area, you may selectively Show, minimize or remove a link member. Another way of freeing up more space for analysis displays is to hide the left-hand panel using the circled arrow:



The standard X button closes the window completely (but does not loose data). The - button collapses the view to look like this:



The two side arrows (circled) are used to reorder a stack of such view on the display area:












The remaining controls on the Spectrum View main window relate to Spectrum View data manipulation. We will cover them in the next section using a live analysis.

10.7. Spectrum View Display Function Buttons

Spectrum View data manipulation functions are provided on the top button bar:



Table 10-1: Spectrum View Analysis Display Buttons functionality

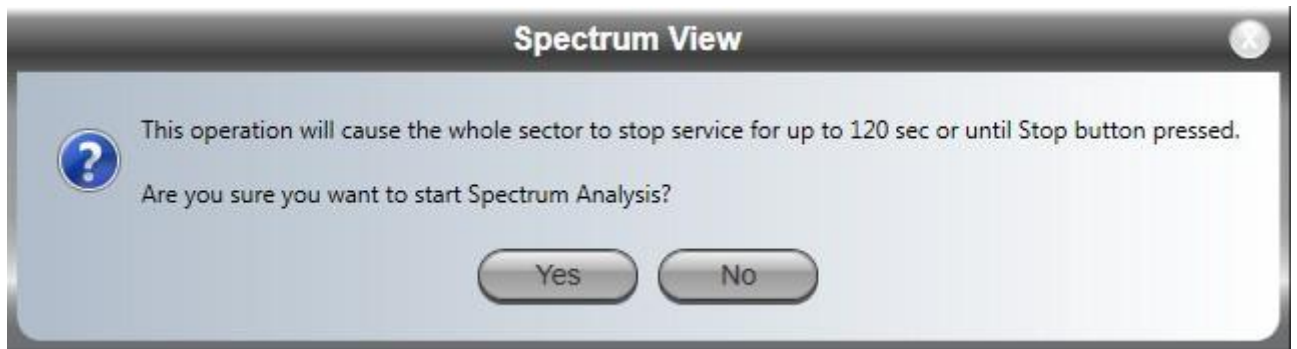
Button	Purpose
	Show/Hide Antenna A
	Show/Hide Antenna B
	Show/Hide average
	Show/Hide current channel (HSUs only)
	Show/Hide maximum
	Not in use
	Show/Hide point values
	Save the analysis to a CSV file
	Clear all link member analyses from the display (They can be shown again)



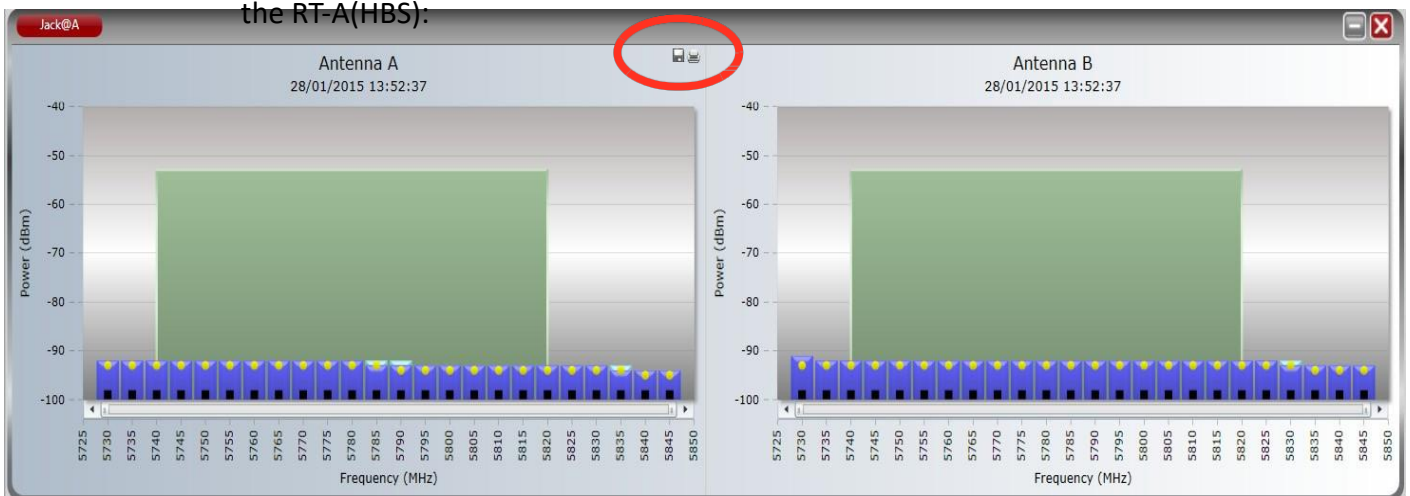
Each button function applies to all the link members at once.

10.8. Running Spectrum View

Click Start. You are offered the following cautionary message:



If it is acceptable to drop the service, click Yes. The processing may appear to have stopped - but it is not complete until all of the Show buttons for link are enabled. Here is the result for the RT-A(HBS):



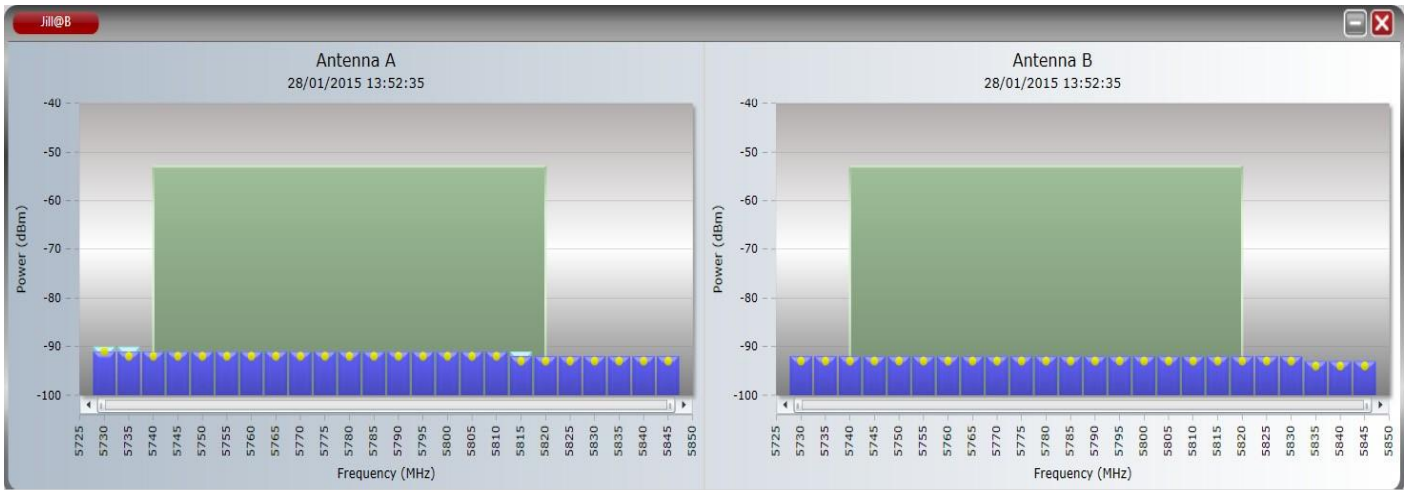
The keys to the color coding are permanently displayed at the bottom of the main window:



Figure 10-1: Spectrum View Analysis color codes

The green band reflects the current Master operating frequency. Notice also the small fly-over diskette icon (circled) to the upper left of either graph. Clicking it opens a Windows File- Save dialog allowing you to save the graph to disk as a jpg file.

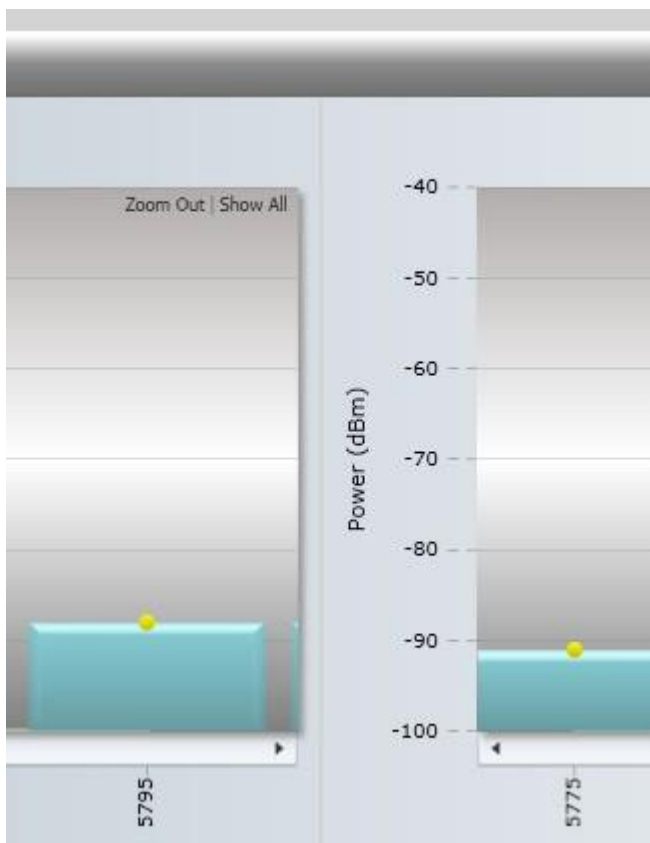
Here is the analysis for RT-B(HSU). It is very similar:



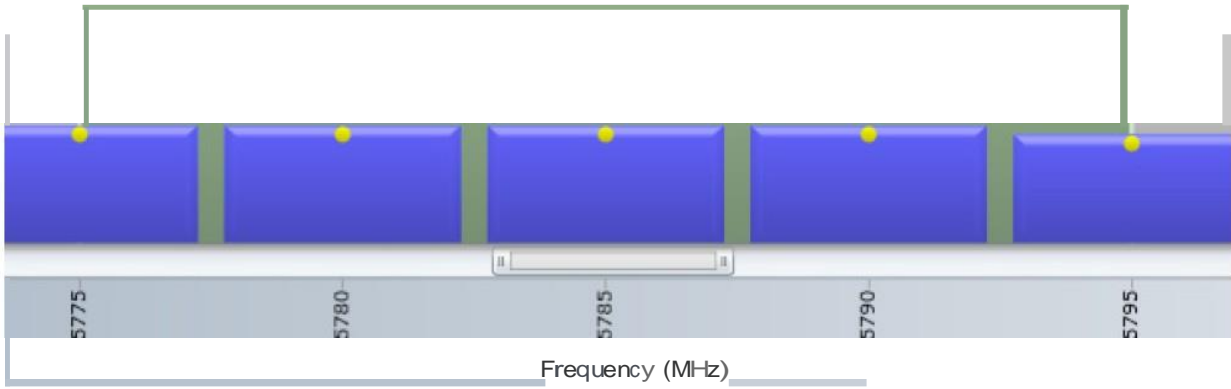
The light green rectangle in the background of both antenna displays reflects actual channel (20 MHz wide here) being used by the Slave. The title bar also contains the Slave's IP address.

10.9. Zooming in and out

You may zoom in on a range of interest and enlarge it. Use the mouse to swipe the range from left to right or reverse and then click. The swiped range is zoomed in. You may repeat this several times. The zoom applies to all charts for all element in the analysis. An indicator is provided at the top right of each chart:



Zoom out returns you to the previous zoom state. Show all reverts you to the original display. In a zoomed state, a horizontal scroll bar enables you to view other areas of the displayed frequency range.



Chapter 11: Web Interface for Alpha EMB/Int units

11.1. Scope of this Chapter

This chapter describes how to configure Alpha EMB/Int units via its web interface.

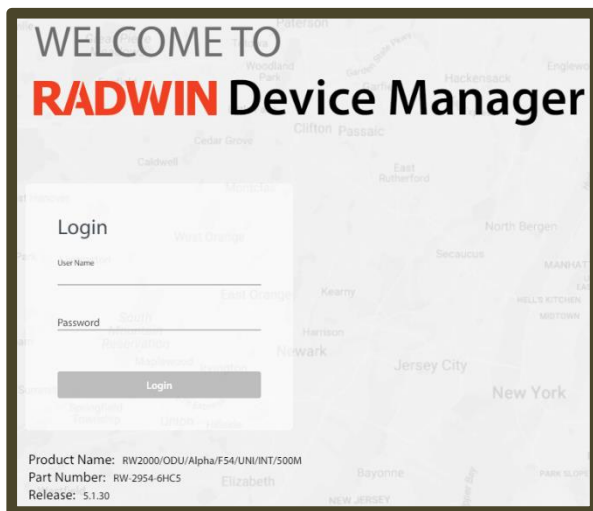
LFF and SFF units do not have a web interface.

11.2. Login

Access the web interface by connecting to the unit, either directly via RJ45 cable, or via the internet. We recommend using a PC or a laptop. Enter the unit's IP address in a web browser (default value: 10.0.0.120). A welcome message will appear.

Note - Alpha product has a built-in WiFi AP for management only. For configuration and monitoring, you can connect to the radio via its WiFi AP. The ESSID of the radio is "R [serial number of the unit]" and the default password is "wireless". Upon successful authentication, your WiFi client will get a DHCP IP address.

To login to the radio, enter the IP address of the WiFi AP in a web browser (default value: 192.168.1.1).



Enter the username and password, then click **Login**

Username: admin

Password: netwireless

The main window will appear.

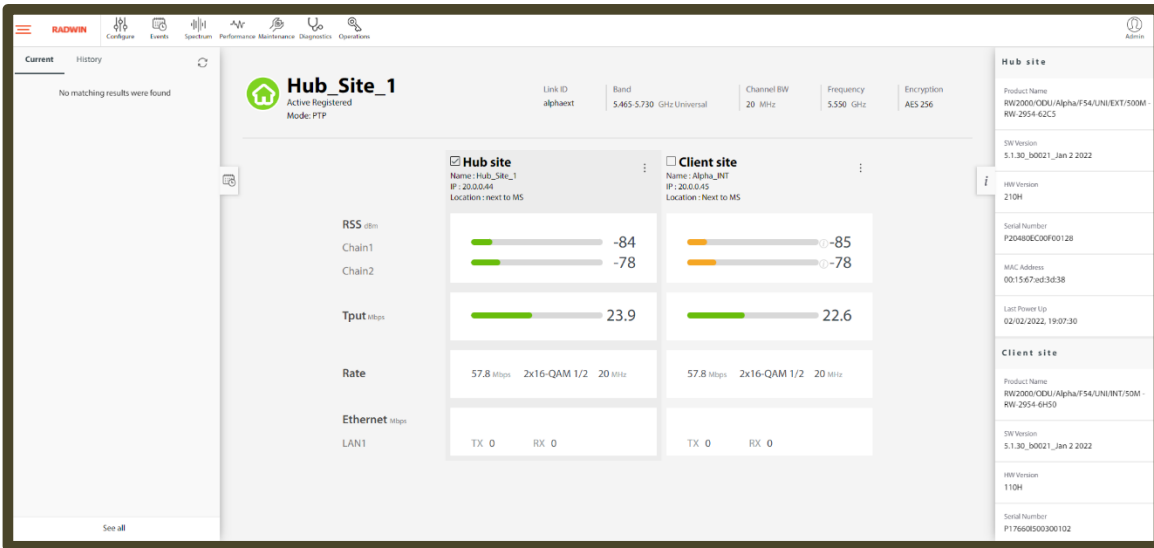


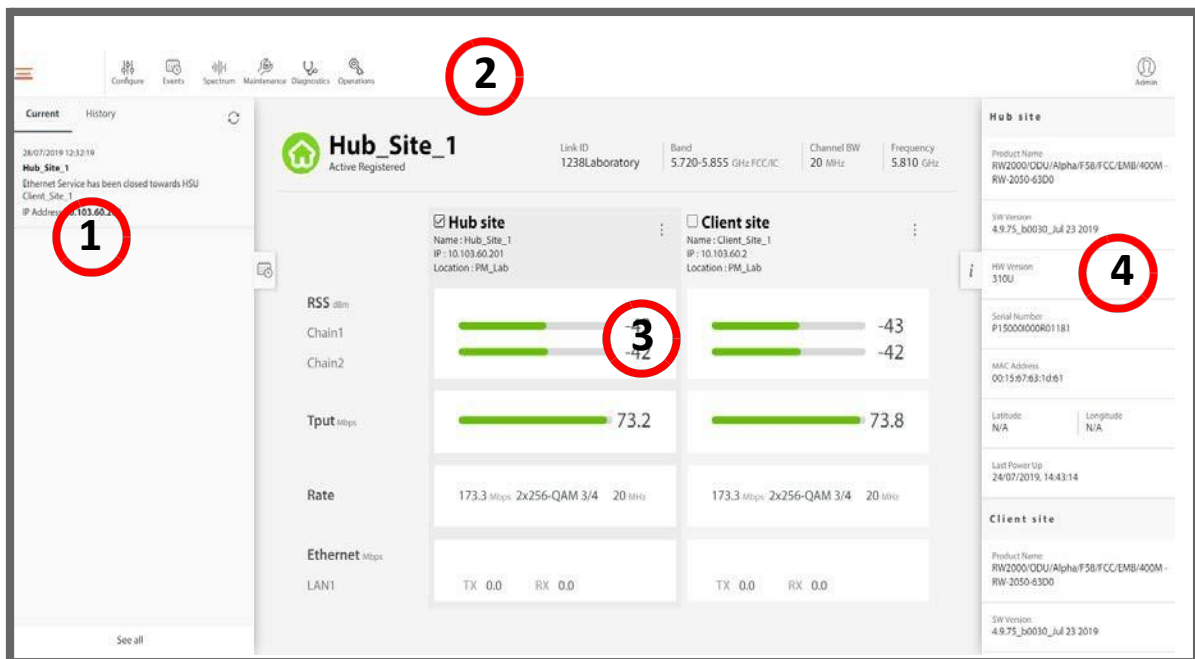
Figure 11-1: Alpha EMB/Int / Ext Main/Overview Window

For an explanation of the Web User Interface, see [Web UI Overview](#).

For instructions on first-time use of an Alpha EMB/Int unit, see [First-Time Use](#).

11.3. Web UI Overview

The Web UI shows the Alpha EMB/Int unit and its opposing unit in the link.



Note – PtP or PtMP mode appears in the main menu under the unit's status. Alpha clients automatically change the mode according to the type of base station (PtP or PtMP) it is synchronized with.

Click on the section of the Web UI for which you want more information:

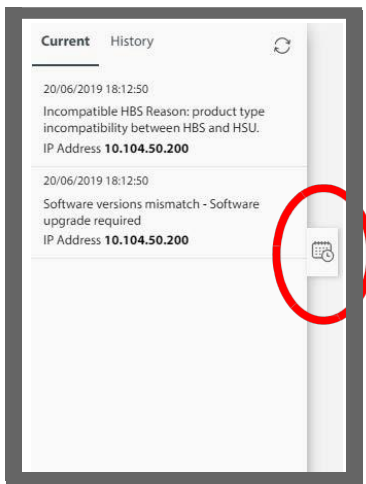
1	<i>History</i>	2	<i>Main icons</i>
3	<i>Radio List</i>	4	<i>Right Pane</i>

11.3.1. History

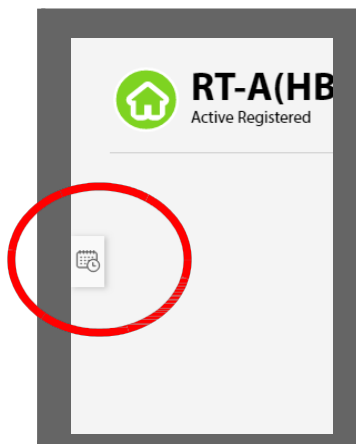
Here you can see the history of events.

Click on the **Current** tab to limit the list to recent events (from the last several hours), or on the **History** tab to see a comprehensive list of events.

- To minimize the History list, click on the minimize symbol:



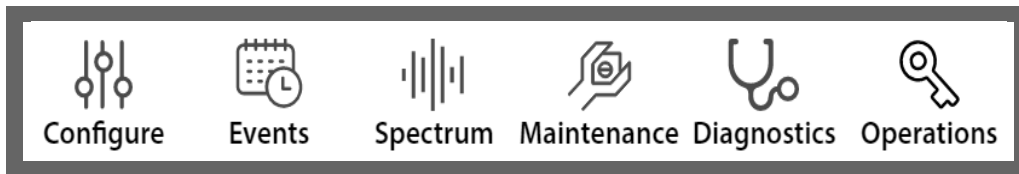
- To restore the History list, click on the minimize symbol again:










11.3.2. Main icons

Along the top edge of the Web UI, there are icons that allow you to carry out certain tasks for the radio units.

The applicable icons become enabled when you select the radio unit relevant for the task.



 <p>Configure</p>	<p>Configure</p>	<p>Set various parameters for the selected unit, including, but not limited to:</p> <ul style="list-style-type: none"> • IP address, • frequency and bandwidth, • transmission power, • passwords, • NTP settings, • WiFi, and more
 <p>Events</p>	<p>Events</p>	<p>Shows system failures, loss of synchronization, loss of signal, compatibility problems and other fault conditions and events for the selected unit or units. You can also search and filter the events by severity, source, and time.</p>
 <p>Spectrum</p>	<p>Spectrum</p>	<p>The Spectrum view utility provides spectral measurements and is be useful in assisting with diagnosing interference related problems prior to full sector activation. It is operated per carrier.</p>
 <p>Maintenance</p>	<p>Maintenance</p>	<p>Back up, upgrade or restore the software in the selected unit or units.</p>
 <p>Diagnostics</p>	<p>Diagnostics</p>	<p>Shows radio signal strength (refer to this when carrying out antenna alignment), allows a ping and trace, a speed test, creates diagnostics files, and allows sniffing of TCP/IP packets.</p>
 <p>Operations</p>	<p>Operations</p>	<p>Resets, restores to factory default configuration, allows license-dependent upgrades, and can change the ODU mode (in PtP link).</p>
 <p>Admin</p>	<p>User Profile Icon</p>	<p>Click this icon to log out of the unit.</p>

Configure



These are the configuration categories:

<i>System</i>	<i>Service (Client site only)</i>	<i>Tx & Antenna</i>
<i>Air Interface</i>	<i>Management</i>	<i>Hub Site Sync (Hub site only)</i>
<i>Inventory</i>	<i>Security</i>	<i>Date & Time</i>
<i>Ethernet</i>	<i>General (Hub site only)</i>	

11.3.3. System

General

These items are convenience fields: **Description**, **Object ID**, **Name**, **Contact**, **Location**, and **Last Power Up**. Name and Location are typically entered during registration. If you make any changes, click **Save** to have them take effect.

The screenshot shows a web interface for configuring a system. On the left, there is a sidebar with 'System' selected and 'General' highlighted. Below 'General' is 'Coordinates'. The main area displays the following fields:

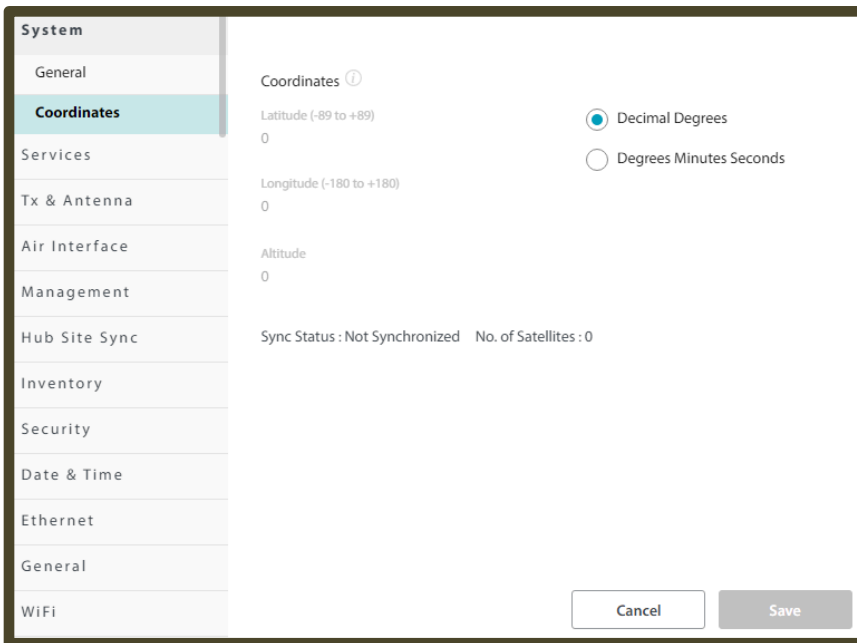
- Description: Wireless Link
- Object ID: 1.3.6.1.4.1.4458.20.5.1.1
- Name: DUO_PM
- Contact: Person
- Location: PM_Lab
- Last Power Up: 12/11/2018, 14:21:05

At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Coordinates

The coordinates (latitude and longitude) use either decimal degrees or degrees, minutes, and seconds. If you make any changes, click **Save** to have them take effect.

For an Alpha unit with h/w that support GPS, the coordinates are automatically displayed after the GPS is synchronized with the satellites.



11.3.4. Service (Client site only)

This category has four sub-categories:

MIR (Maximum Information Rate)

MIMO Modes

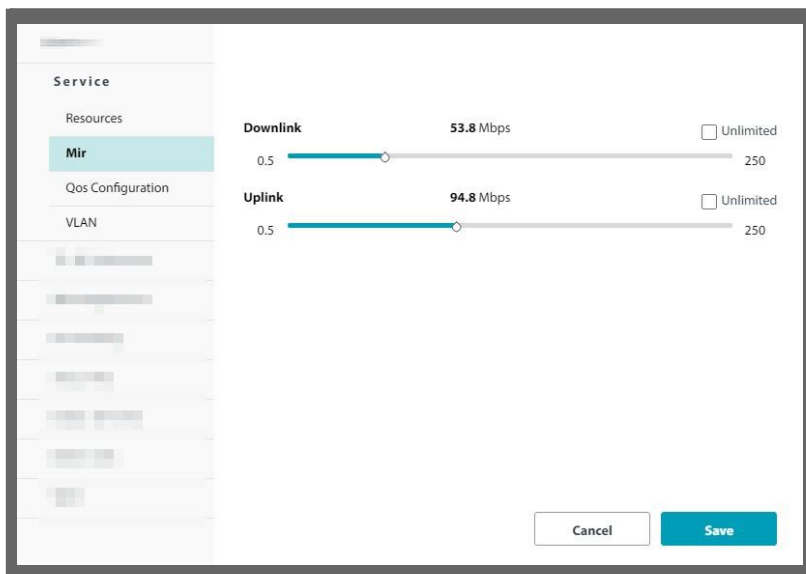
QoS Configuration (Client site)

VLAN

MIR (Maximum Information Rate)

Although this is set during registration, you can change it here.

Use the sliders to set the maximum throughput rate you want for the specific HSU in each direction: down link and up link. You can choose a value or click the Unlimited checkbox.



Click **Save** to have your changes take effect.

MIMO Modes

- Select a MIMO Mode for the selected Client site:
 - Spatial Multiplexing (default) splits the data into two streams on transmission and recombines it on reception providing maximum throughput. This provides a higher throughput.
 - **Diversity** transmits the same data on both streams. This mode helps to ensure more reliable data transmission in a noisy environment, although throughput will be lower.
 - Auto Selection instructs the system to choose whichever mode is most efficient.
- Click **Save** to have your changes take effect.

QoS Configuration (Client site)

To configure QoS, you must do so from the Client site and from the Hub site. This section describes how to configure QoS from the Client site side. To see how to configure QoS from the Hub site, see [QoS Configuration \(Hub site\)](#).

Queue	Strict / Weight %	Maximum Information Rate Mbps
Real Time	↑ 15	0.5 <input type="checkbox"/> Unlimited
Active Voice over IP	↓ 15	0.5 <input type="checkbox"/> Unlimited
Near Real Time	↑ 20	0.5 <input type="checkbox"/> Unlimited
Active	↓ 20	0.5 <input type="checkbox"/> Unlimited
Controlled Load	↑ 22	0.5 <input type="checkbox"/> Unlimited
Active	↓ 14	0.5 <input type="checkbox"/> Unlimited
Best Effort	↑ 40	0.5 <input type="checkbox"/> Unlimited
Active	↓ 40	0.5 <input type="checkbox"/> Unlimited
Total uplink	97 %	
Total downlink	89 %	

1. Enable the **Mode** field. (See [Enabling a VoIP Queue \(Client site\)](#) for VoIP).
2. Set the **weight percentage** for each queue by moving the spinners up or down.

Light blue for uplink, pink for downlink.

The weight percentage determines what percentage of the throughput will be dedicated for the indicated queue.

The total weight is shown in the lower part of the window. If you exceed 100% total weight, you will receive an error message.

If you are under-booked, for example by setting a queue to zero, the unused weight will be distributed to the remaining queues. The effect of doing this will only

become apparent under congestion. In particular, a queue set to zero weight will become nearly blocked under congestion with packets passing through on a best effort basis.

3. **Strict:** If you place a checkmark in the Strict box, *all traffic* of the specific queue will be passed through. The Weight percentage will become disabled. Placing a checkmark here can only be done in order: First Real Time, then finally Best Effort. That is, you cannot place a checkmark in Near Real Time without one in Real Time as well. Like the weight percentage, uplink and downlink are configured separately.
4. **Maximum Information Rate:** Although the weight percentage affects how much relative traffic will be allowed through, you can set here the absolute maximum to allow through. Place a checkmark to make this valued unlimited.

Enabling a VoIP Queue (Client site)

Note the following:

- To enable VoIP, you must enable it from both the Hub site and the Client site.
 - To configure VoIP from the Hub site side, see [Enabling a VoIP Queue \(Hub site\)](#).
 - The VoIP feature, as implemented here, assumes that your end-user has a gateway or other network device that defines the traffic to be VoIP with the correct QoS defined (VLAN or DiffServ, in accordance with your configuration done here). The definition must be done at both ends of the data stream.
 - Enabling a VoIP queue may decrease the unit's peak throughput in some scenarios. Therefore, make sure that you absolutely need to enable a VoIP queue before doing so.
1. Click **Voice over IP**. The Voice over IP indicator will turn green.

Resources	Queue	Strict / Weight %	Maximum Information Rate Mbps
Mir	Real Time	↑ <input checked="" type="checkbox"/> 0	0.5 <input type="checkbox"/> Unlimited
	Active Voice over IP	↓ <input checked="" type="checkbox"/> 0	0.5 <input type="checkbox"/> Unlimited
	Near Real Time	↑ <input type="checkbox"/> 20	0.5 <input type="checkbox"/> Unlimited
	Active	↓ <input type="checkbox"/> 20	0.5 <input type="checkbox"/> Unlimited
VLAN			
Tx & Antenna			

The weight percentages of the Real Time queue will become zero in both the uplink and downlink directions. This means that the VoIP traffic is treated in a similar fashion to the Real Time traffic.

VoIP works whether you are using VLAN or DiffServ, but you must be consistent with this QoS mode throughout the data stream.

2. Click **Save** to have your changes take effect.

VLAN

Configure a VLAN for traffic here. To configure the management VLAN, see [VLAN](#).

VLAN configuration is carried out per Client site.

If VLAN is not enabled, ethernet frames pass transparently over the radio links.

VLAN Background Information

The standards defining VLAN Tagging are IEEE_802.1Q and extensions.

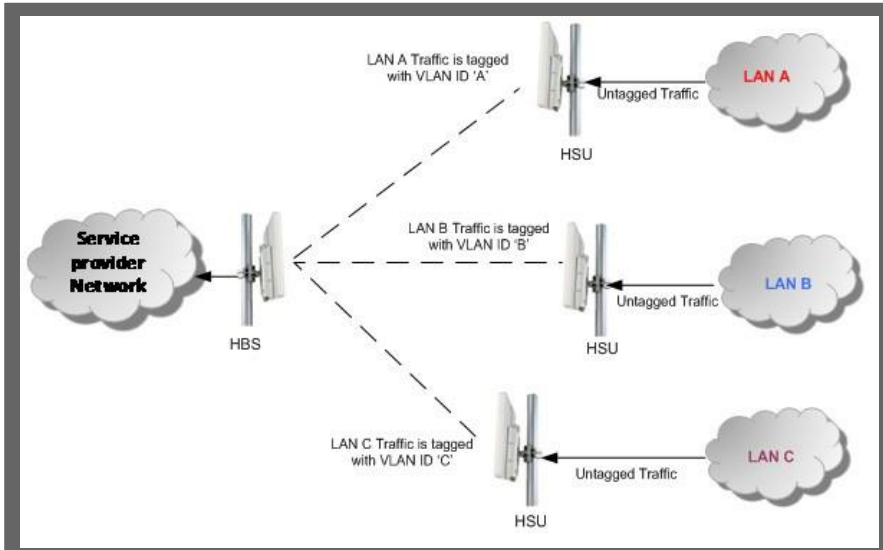
For general background about VLAN, see http://en.wikipedia.org/wiki/Virtual_LAN.

Background information about Double Tagging, also known as QinQ, may be found here:

<http://en.wikipedia.org/wiki/802.1QinQ>.

VLAN Tagging

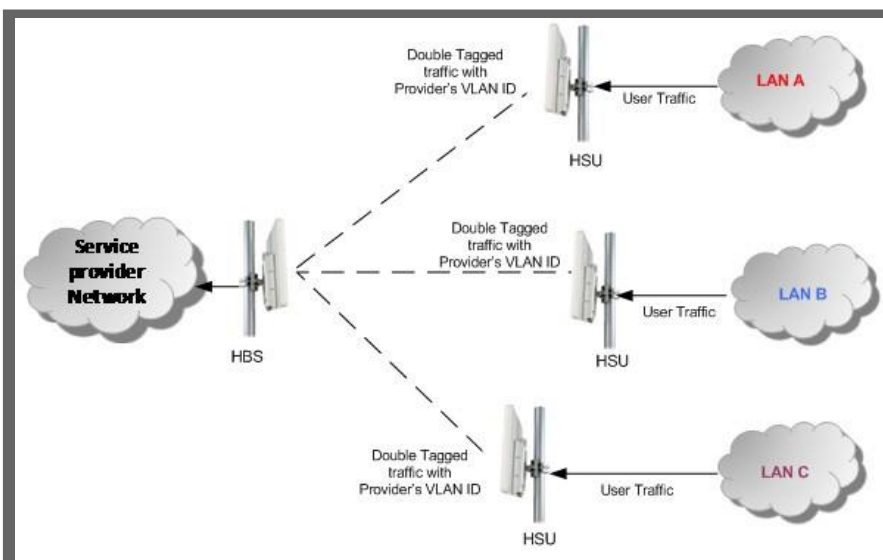
VLAN tagging enables multiple bridged networks to transparently share the same physical network link without leakage of information between networks.



IEEE 802.1Q is used as the encapsulation protocol to implement this mechanism over Ethernet networks.

QinQ (Double Tagging) for Service Providers

QinQ is useful for Service Providers, allowing them to use VLANs internally in their “transport network” while mixing Ethernet traffic from clients that are already VLAN-tagged.



The outer tag (representing the Provider VLAN) comes first, followed by the inner tag. In QinQ the EtherType = 0x9100. VLAN tags may be stacked three or more deep.

When using this type of “Provider Tagging”, you should keep the following in mind:

- Under Provider Tagging, the system double-tags egress frames towards the Provider’s network. The system adds a tag with a VLAN ID and EtherType = 0x9100 to all frames, as configured by the service provider (Provider VLAN ID).
- The system always adds tags to each frame with a VLAN ID and EtherType = 0x9100. Therefore,
 - > For a frame without a tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will have one tag.
 - > For a frame with a VLAN tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will be double tagged.

For a frame with a VLAN tag and a provider tag – the system will add a tag with VLAN ID and EtherType = 0x9100 so the frame will be triple-tagged and so on.

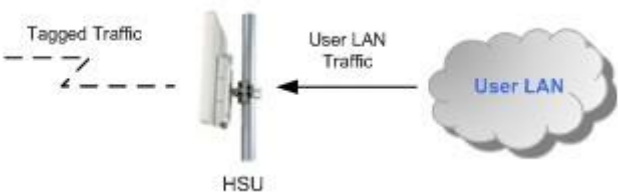
At the egress side, the HSU removes the QinQ tag with EtherType = 0x9100 no matter what the value of its VLAN ID.


Port Setting

In a 2000-Plus link, all VLAN activity is configured and supported from the Client site.

The Client site management port can be configured to handle Ethernet frames at the ingress direction (where frames enter the Client site) and at the egress direction (where frames exit the Client site).


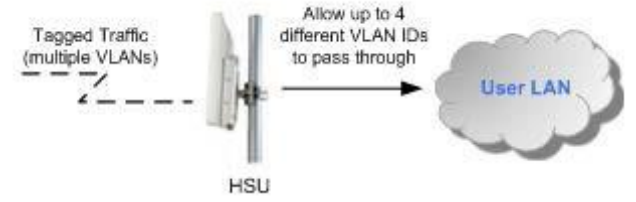
Ingress Direction

Transparent	The port ‘does nothing’ with regard to VLANs - inbound frames are left untouched.
Tag	<p>Frames entering the Client site port without VLAN or QinQ tagging are tagged with VLAN ID and Priority^a, which are preconfigured by the user. Frames which are already tagged at ingress are not modified and pass through.</p>  <p>The diagram illustrates the ingress direction of traffic. On the right, a cloud labeled 'User LAN' has an arrow pointing left towards a vertical line representing the 'HSU' (Host Service Unit). This arrow is labeled 'User LAN Traffic'. From the HSU, a dashed arrow points further left, labeled 'Tagged Traffic', indicating that the traffic is being processed and tagged by the HSU.</p>

<p>Provider tag</p>	<p>Frames entering the Client site port are tagged with provider's VLAN ID and Priority which are preconfigured by the user. Frames which are already tagged with Provider tagging at the ingress are not modified and passed through</p> 
----------------------------	--

a. Priority Code Point (PCP) refers to the IEEE 802.1p priority. It indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc).

Egress Direction

<p>Transparent</p>	<p>The port 'does nothing' with regard to VLANs - outbound frames are left untouched.</p>
<p>Untag all</p>	<p>Port configured to untag user VLAN tags for all frames.</p> 
<p>Filter</p>	<p>Port configured to allow up to 4 different VLAN IDs to pass through.</p> 

Before proceeding, note the following:



If you are not a VLAN expert, please be aware that incorrect VLAN configuration may cause havoc on your network. The facilities described below are offered as a service to enable you to get best value from your 2000-Plus link and are provided "as is". Under no circumstances does RADWIN accept responsibility for network system or financial damages arising from incorrect use of these VLAN facilities.

Management Traffic and Ethernet Service Separation

You can define a VLAN ID for management traffic separation. You should configure the system to prevent conflicts:

When configured for the default operational mode, a "Provider port" will handle ingress traffic as follows:

- Filters frames that are not tagged with the Provider VLAN ID
- Removes the Provider double tag

Therefore, if a port is configured for management traffic separation by VLAN and as 'Provider port', then the received management frames must be double tagged as follows:

- The outer tag has to be the Provider's tag (so the frame is not filtered)
- The internal tag has to be management VLAN ID

To avoid mix-ups, best practice is to:

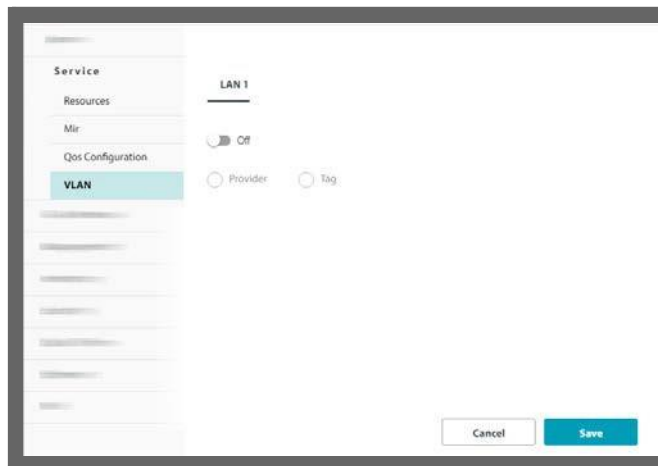
- Separate the management and data ports
- Define only a data port with Provider function



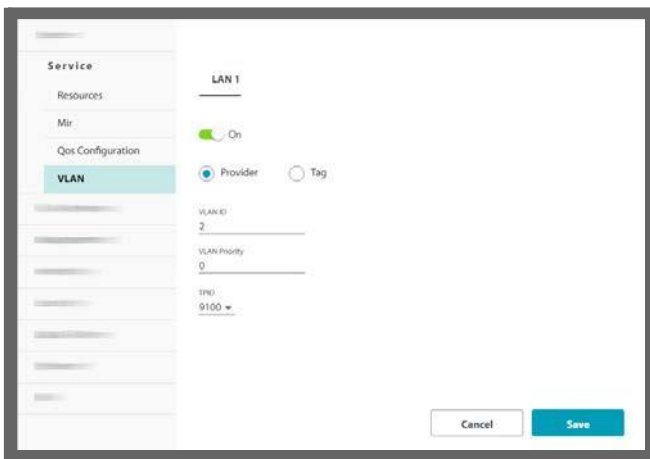
If traffic VLAN tagging is in force for the Client site ingress direction and management VLAN is in use at the Hub site (see [VLAN](#)), then the VLAN ID at the Client site ingress direction must be the same as the VLAN ID for management at the Hub site.

VLAN Configuration

1. Select the Client site to be configured, click the **Configuration** icon, click **Service -> VLAN**.



2. Click **Off** to enable the VLAN window. It will turn to **On**.



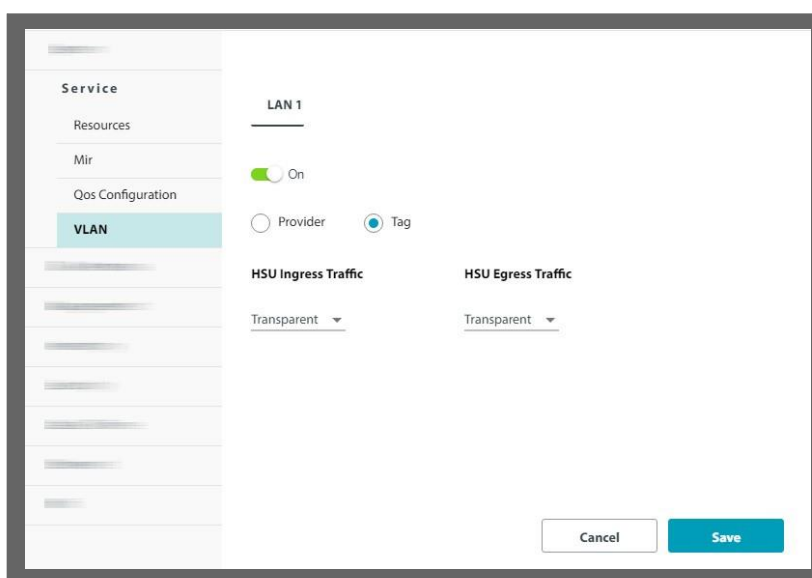
3. If you are using Provider tagging, click the Provider Radio button.

4. In Provider mode, Ethernet frames are tagged with the provider's VLAN ID before they enter the provider's network/backbone.
5. Enter a Provider VLAN ID and Priority. The VLAN ID must be in the range 2 to 4094. The VLAN Priority must be in the range 0 to 7. You may also change the TPID from the default as shown.



This facility is provided to enable connection through legacy switches requiring it. Otherwise, there is no need to change the TPID.

6. Click **Save** to have your changes take effect.
7. If you are using VLAN tagging, click the **Tag** radio button.
8. In Tag mode, Ethernet frames are tagged or untagged to distinguish between different networks.



9. For completely transparent passage of tagged frames, there is nothing further to do. Click **Save** to have your changes take effect.
10. However, if you wish to not have transparent passage of frames, the following table shows the possible settings for each combination of Ingress and Egress modes:

Ingress	Transparent	Frames are not modified and are forwarded transparently
	Tag	Enter a VLAN ID (1-4094) and Priority (0-7)

Egress	Transparent	Frames are not modified and are forwarded transparently
	Untag All	All frames with VLAN tag are untagged
	Filter	Allow up to 4 VLAN IDs to be passed through
	Untag Filtered	Allow VLAN IDs: <ul style="list-style-type: none"> • Allow up to 4 VLAN IDs to be passed through Untag: <ul style="list-style-type: none"> • Untag the VLAN tag of the selected VLAN IDs

11. Click **Save** to have your changes take effect.

Quality Detection

This option allows you to configure the device to send an indication when link quality degrades. There are three parameters, evaluated per link (HBS-SU pair):

BLQ Baseline Link Quality: Value that the throughput of the link should have. Configured at the SU for the uplink and downlink separately.

Th Detection Threshold¹: A percentage of the Baseline Link Quality below which the link quality is considered to be degraded. Configured at the HBS.

tF Detection Seconds²: Time that the degradation must persist (Th) before an indication is issued. Setting this parameter to an appropriate value can prevent the system from reacting to brief peaks (or valleys) of link quality value (throughput) changes that do not disturb link functionality. Configured at the HBS.

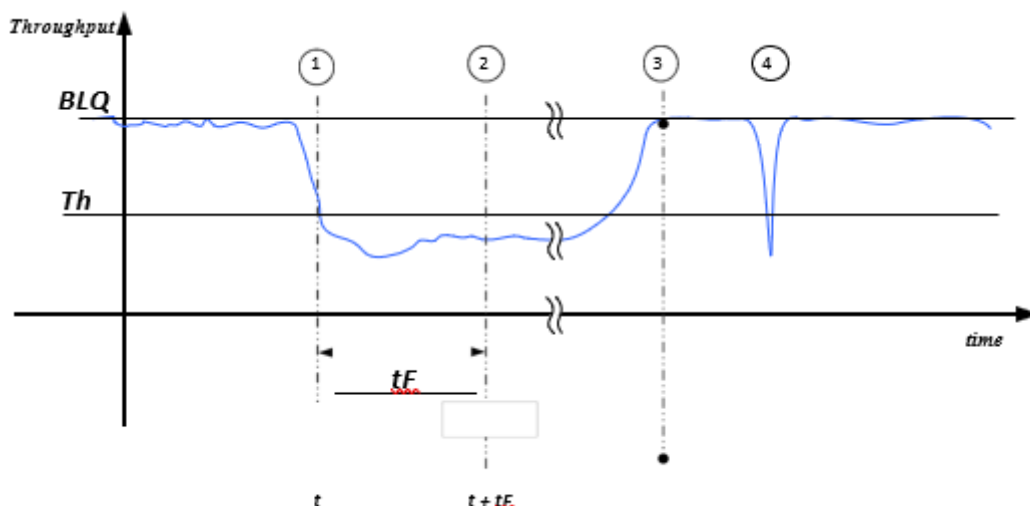


Figure 2-5: Quality Detection parameters

In [Figure 2-5, Quality Detection parameters](#), the blue line represents the real-time throughput value of the link.

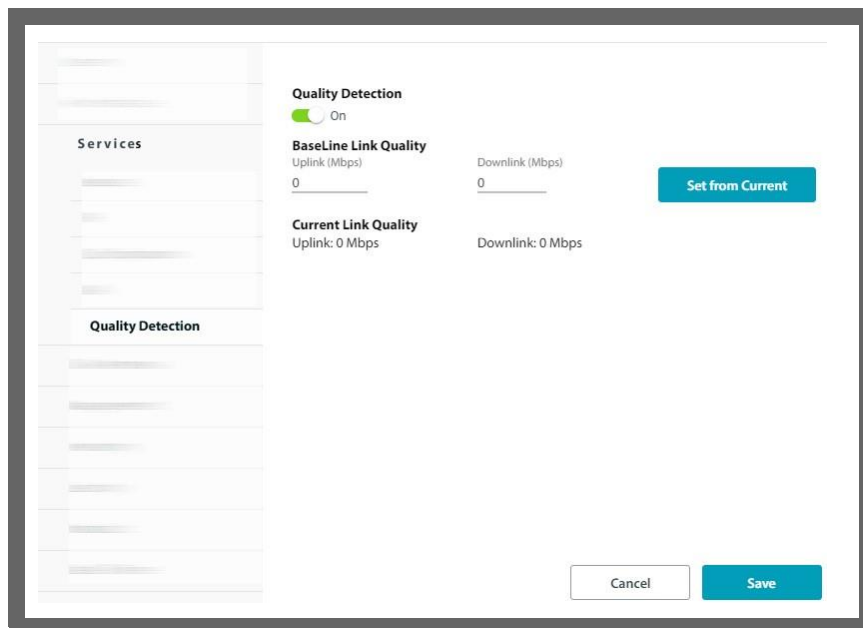
- ① The user has set the baseline link quality (**BLQ**) and the indication threshold value (T_h). At time t , the signal throughput of the link decreases below this threshold. This causes the system to start a clock to measure the persistence of the low throughput condition.
- ② From the time t to the time $t + tF$ (Detection Seconds), the low throughput condition persisted. An indication of link degradation is then issued.
- ③ The user has taken whatever measures necessary to rectify the link degradation, and the signal recovers. At that point, an indication is issued that the link quality degradation condition no longer exists.
- ④ For a link quality degradation that lasts for a shorter period of time than tF (Detection Seconds), no indication is issued.

Configure Quality Detection as follows:

1. This is called "Indication Threshold" (T_h) in the RADWIN Manager
2. This is called "Indication Time" (tF) in the RADWIN Manager


SU side

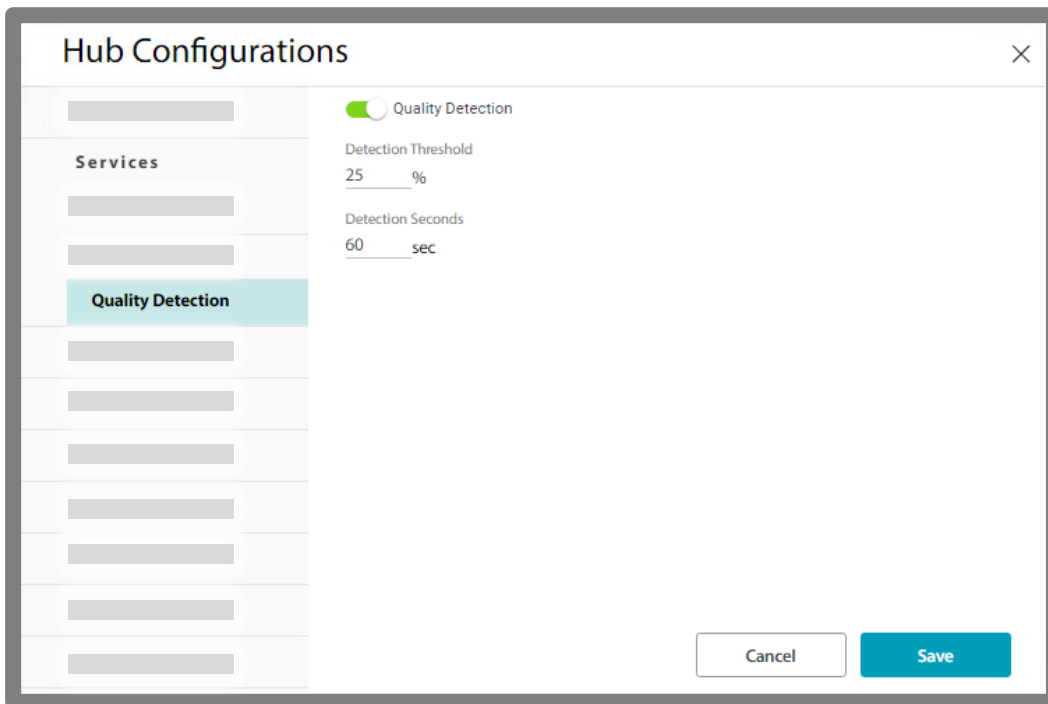
1. Select the SU.
2. Click the Configuration icon ().
3. Click Services -> Quality Detection.
4. Enable Quality Detection by clicking its switch to On.



5. Select the **Baseline Link Quality** for the uplink and for the downlink in mega-bits per second (Mbps). They do not have to be the same.
6. You can set this value from the current throughput value (shown as Current Link Quality) by clicking **Set from Current**.
7. Click **Save**.

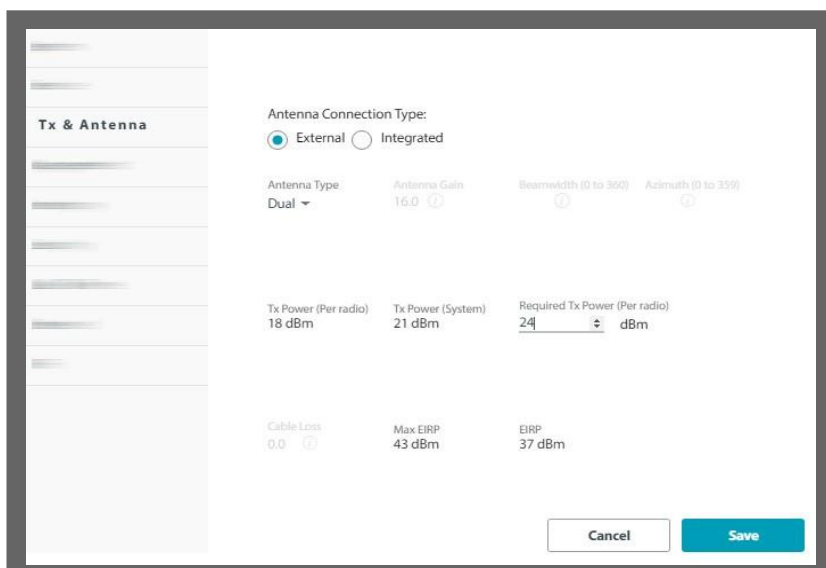
HBS side

1. Select the HBS.
2. Click the Configuration icon ().
3. Click **Services** -> **Quality Detection**.
4. Enable Quality Detection by clicking its switch to **On**.
5. Select the Detection Threshold (Th) in percent value, relative to the baseline link quality value.
6. Select the Detection Seconds time (tF).
7. Click **Save**.



11.3.5. Tx & Antenna

Changes made here may affect link quality, and in the case of antenna type, cause a re-sync.



If you make any changes, click **Save** to have them take effect.

Air Interface

Radio

Sector ID: Set the Sector ID here (same as Link ID). This must be the same as the Hub site to which the Client site is to connect.

Channel Bandwidth: Shows the channel bandwidth. This is set at the Hub site.

Operating Channel (Hub site only): Shows the frequency channel on which the link is operating.

Automatic Channel Selection (Hub site only): Select this option to have the Hub site automatically select the best channel on which to work. You can select all of the channels or clear your selection.

Alternatively, you can manually select any of the displayed channels.

Change Band

- You can change the frequency band here. Only frequency bands allowed by your regulatory environment will appear.
- If you make any changes, click **Save** to have them take effect.

11.3.6. Management

This category enables you to change the IP address, Subnet Mask and Default Gateway of the selected device, configure the management VLAN, set trap destinations, change the management protocol and its authentication mode, set the IP address of a Syslog server, and add or remove user definitions.

Network

Configure management IP address

You may configure a link for IPv4, IPv6, or both. Using both IP versions is useful in conjunction with applications that do not fully support IPv6.

1. Choose what type of IP address to enter (IPv4, IPv6, or both).

IP Version
IPv4

IPv4	IPv6
IP Address 10.103.151.23	IP Address ::11.0.0.0
Subnet Mask 255.255.255.0	Subnet Prefix Length 64
Default Gateway 10.103.151.201	Default Gateway ::10.0.0.0

Vlan
 On

VLAN ID [2 - 4094]
2

VLAN Priority [0 - 7]
0

Cancel Save

Here, you can choose both, and enter the IPv6 addresses:

IP Version
IPv4 + IPv6

IPv4	IPv6
IP Address 10.104.60.230	IP Address 205:104:60:230
Subnet Mask 255.255.255.0	Subnet Prefix Length 64
Default Gateway 10.104.60.201	Default Gateway 205:104:60:201

Cancel Save

2. Enter the appropriate IP address or addresses, including the Subnet Mask and Default Gateway (for IPv4), and/or the Subnet Prefix Length and Default Gateway (for IPv6).
3. Click **Save**.
4. If you changed any value, you will see a warning message that a device reset will be done. To confirm, click **OK**.

Configure management VLAN

Configure the management VLAN here. To configure a VLAN for traffic, See [VLAN](#).

The management VLAN enables the separation of user traffic from management traffic whenever such separation is required.

To enable VLAN for management:

1. Check ON in the VLAN checkbox.
2. Enter a VLAN ID. Its value should be between 2 and 4094.

After entering the VLAN ID, only packets with the specified VLAN ID are processed for management purposes by the HBS/SU. This includes all the protocols supported by the radio (ICMP, SNMP, Telnet and NTP). Using VLAN for management traffic affects all types of management connections (local, network and over the air).

3. Enter a Priority number between 0 and 7.

The VLAN priority is used for the traffic sent from the radio to the managing computer.

4. Change the VLAN ID and Priority of the managing computer NIC to be the same as those of steps 2 and 3 respectively.
5. Click **Save**.

Lost or forgotten VLAN ID or IP Address (For Alpha)

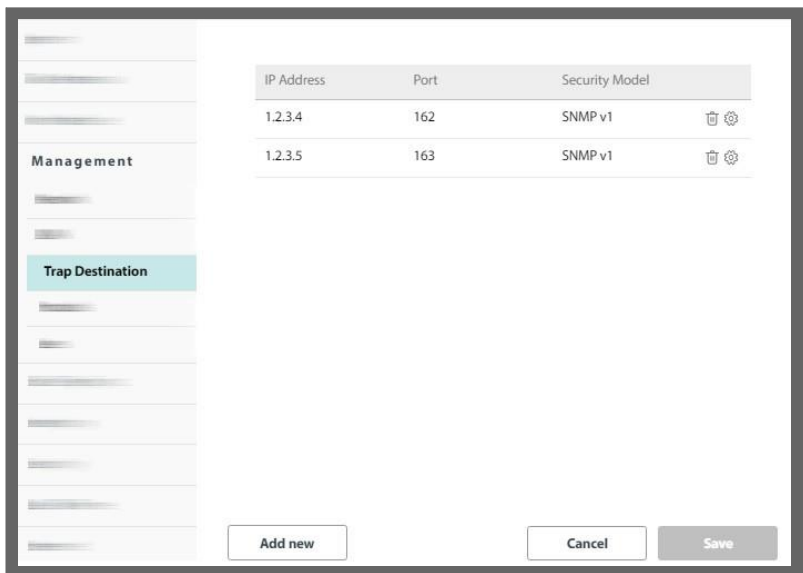
If the VLAN ID or IP address of the SU unit is forgotten, you can reset the unit find the IP address using a sniffer (like Wireshark).

When the SU is reset, it sends a Gratuitous ARP packet toward the Ethernet interface which contains the management VLAN ID and IP address.

You can also reset the unit and locally access to it via the WiFi.

Trap Destinations

All traps are saved at each location you define.



➤ **To set a new trap destination:**

1. Click **Add new**.
2. In the window that appears, enter the Trap Destination IP Address, Port, and Security Model (SNMP v1 or v3). If choosing SNMP v3, enter the username and password. The IP address can be the same as the managing computer. The events log will be stored at the address(es) chosen.

New Trap Destination

IP Address: 1.2.3.6 Port: 162



Security Model: SNMP v1

User Name: Password:

Cancel Save

3. Once you are finished, click **Save** to have your changes take effect.

➤ **To change (edit or delete) a trap destination:**

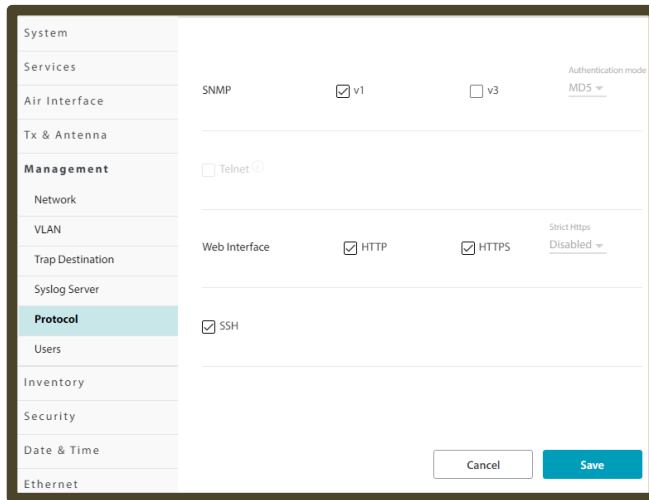
1. To delete a trap destination, click the trash icon () on the same line as the IP address.
2. To edit a destination, click the configuration icon () on the same line as the IP address.
3. In the window that appears, change the parameters you wish to change (Trap Destination IP Address, Port, and/or Security Model). If choosing SNMP v3, enter the username and password. The IP address can be the same as the managing

computer. The events log will be stored at the address(es) chosen.

4. Once you are finished, click **Save** to have your changes take effect.

Protocol

You can set the management protocol as well as the Web Interface access method.



SNMP

SNMP support is permanently enabled. You may choose between SNMPv1, SNMPv3 or both.

You can leave the default authentication mode for SNMPv3 as MD5 (message digest algorithm) or change it to SHA1 (secure hash algorithm).

Web Interface

The unit can be configured for HTTP access, HTTPS access, or both.

- Place a checkmark in the box next to the protocol you want from the **Web Interface** line.
- The next time you log on to the unit's Web Interface, use the access method you chose here.
- If you chose HTTPS, you can log on using HTTPS, but if you log on using HTTP, you will automatically be logged on as HTTPS..... *unless:*
You select Enabled from the Strict HTTPS pull-down menu (on the far right of the window). If you enable this, you must log in using HTTPS.
- If you select both HTTP and HTTPS, then you can log in using either method.
- Once you are finished, click **Save** to have any changes take effect. You will be logged out. You must then log in again using the access method you chose.

An admin user must be logged in with HTTPS to make changes in users.

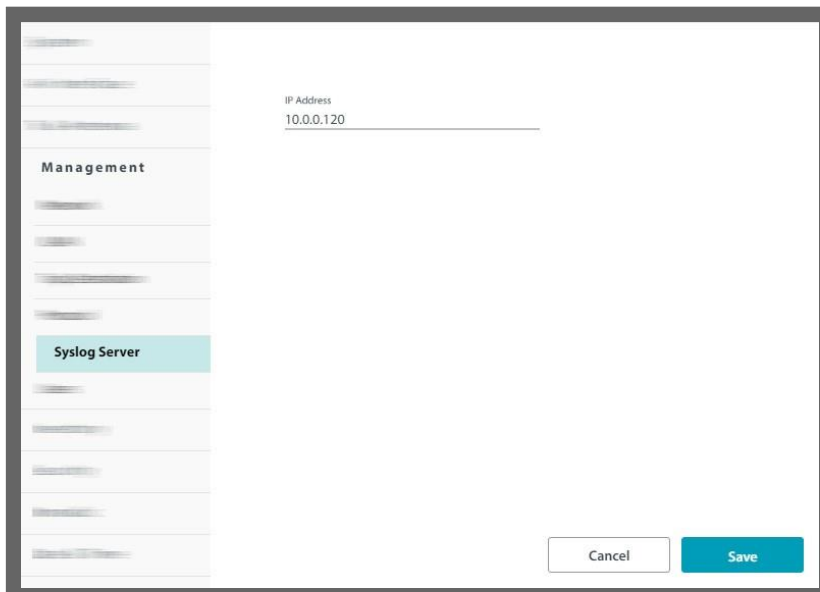
SSH

Turn SSH CLI on or off

For a list of supported CLI commands, See appendix

Syslog Server (Hub site only)

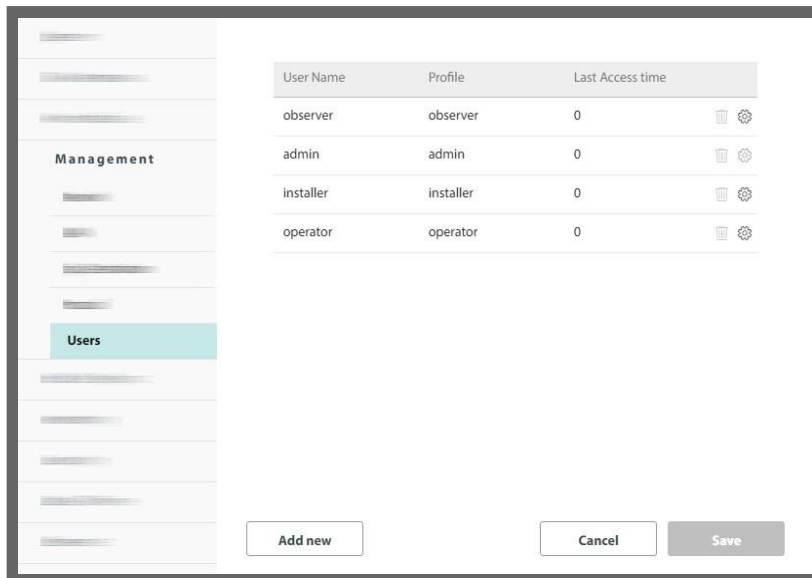
This field shows the IP address of a Syslog server to which the selected radio unit sends Syslog messages. This is configured per individual unit.



The screenshot shows a configuration page for a Syslog Server. On the left, there is a sidebar with several menu items. The 'Syslog Server' item is highlighted in a light blue color. The main content area is titled 'IP Address' and contains a text input field with the value '10.0.0.120'. Below the input field, there are two buttons: a white 'Cancel' button and a blue 'Save' button.

- Enter the IP Address of the Syslog server and click **Save**. It could be the IP address of the managing computer. The Syslog events will be stored at the address chosen.

Users



Here, an admin user can define users and assign to them a pre-defined category. The admin user must be logged in using HTTPS (see [Web Interface](#)). Once you define a user, that person can use the username and password to log in.

Possible user profiles are as follows:

Profile	Default Password	Function
observer	netobserver	Read Only
operator	netpublic	Can install and configure the sector but cannot change the operating frequency or regulation.
installer	netinstaller	Functions as an Operator, in addition to being able to change the operating frequency or regulation, antenna gain and cable loss. Only an Installer can change the antenna gain and cable loss.
admin	netwireless	Functions as an Operator, in addition to being able to change new users. Pre-defined users cannot be changed. Can change the operating frequency or regulation, and the security mode (enhanced).

New user:

Click **Add new**, and the New User window will open.




Caution

To add or edit a user, you must be logged in via secure HTTP (that is, HTTPS). Do this by making sure that HTTPS is selected (from a selected unit, click the Configure icon, then from Management -> Protocol, select the HTTPS box. Then log in using the same IP address as before but add https:// before its address.

1. Enter a convenient name for the new user
2. Choose the profile for this user. The profile determines what the user can and cannot do.
3. Set the password for this user and confirm it.
4. Click **Save** to have your changes take effect.
5. You will see the new user in the Users list.

Edit user:

Click the configuration icon (), and the Edit User window will open.

1. Change the name, if needed.
2. Change the profile, if needed. This determines what the user can and cannot do.
3. Set the password for this user and confirm it. This must be done no matter what action you take here.
4. Click **Save** to have your changes take effect.
5. You will see the edited user in the Users list.

Remove user:

You cannot remove pre-defined users.

1. Click on the trash icon () to remove the user.
2. The user will be removed from the Users list.

RADIUS User Authentication

(HBS only)



You must be logged in using SNMPv3 and via HTTPS for this option to be available (See [SNMP](#)).

This option enables you to set lists of individuals and IP addresses that are permitted to manage radio units. The lists consist of a user/permissions list (which uses a RADIUS server), an access control list for IP addresses, or your own “white list”, which does not use a RADIUS server.



This RADIUS option is used to authenticate management access to the radios in the sector. It is **not** used to authorize the various SU radios in the sector. That RADIUS option is described elsewhere (See [RADIUS Authorization](#)).

Operation

This option uses parameters stored on both the HBS and the RADIUS server as follows:

HBS- based parameters:

- » A list of IP addresses - from which management access is permitted - is stored on the HBS. There are two lists:
 - A RADIUS-based Authentication Control List (ACL)
 - A non-RADIUS-based “White List”
- » SNMP community definition is defined and stored in the HBS¹.
- » The HBS then applies this information to each SU in turn.

RADIUS Server-based parameters:

- » Username, password and a permissions list are stored in a RADIUS server. This list is in addition to and independent of the IP address lists stored in the HBS.
- » When logging on, the HBS queries the RADIUS server for this information.

1. The SNMP community may be different for the SUs, depending on your system configuration.

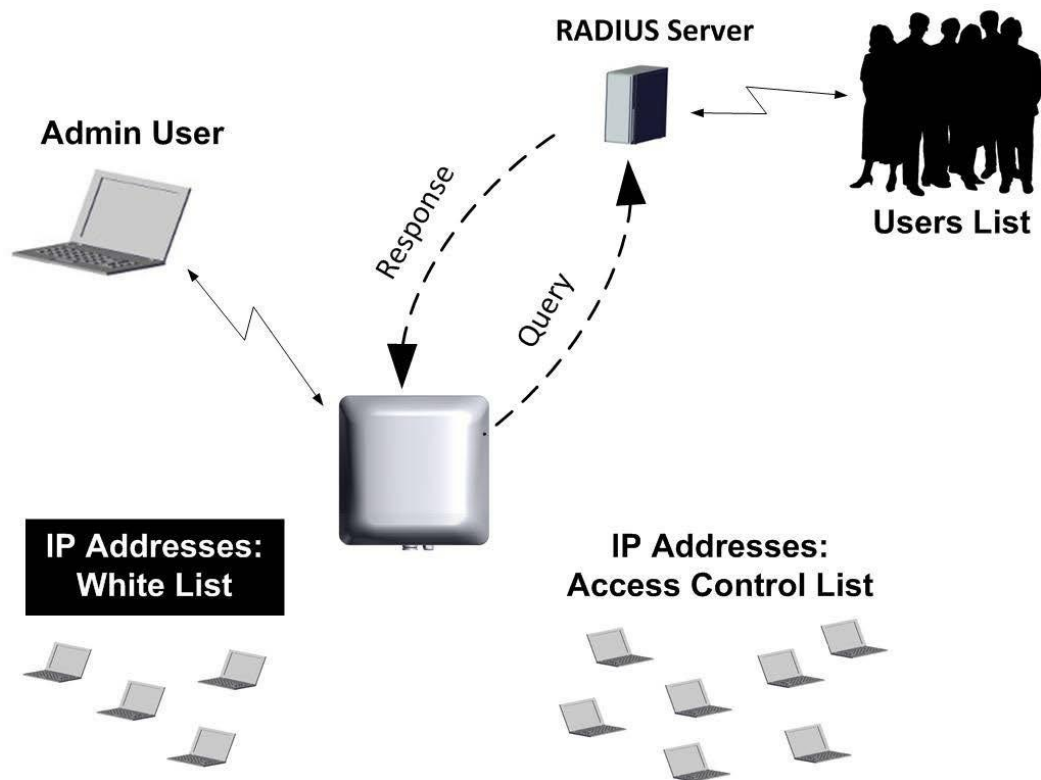


Figure 2-12: RADIUS authentication set up

Customer Preparations

1. You must supply a server that operates the RADIUS protocol. Make sure you have:
 - The IP address of the RADIUS server
 - The port of the RADIUS server to which the HBS must connect
 - The Secret of the RADIUS server
2. Prepare the following parameters for the RADIUS server:
 - a. User profile definitions. These are usually, but not always, confined to the following definitions:
 - HBS Read-Only, SU Read-Only
 - HBS Read-Write, SU Read-Write
 - HBS Read-Only, SU Read-Write
 - b. Permitted users. Each one must have:
 - Username
 - Password
 - Timeout value (in seconds)
 - User profile choice
3. Prepare a list of IP addresses for the Access Control List (ACL). This will be a list of IP addresses from which management access to the HBS is permitted. This list is stored on the HBS, but works only when a RADIUS server is connected, and when RADIUS authentication mode is enabled.
4. Prepare a “white list” of IP addresses. This will be a list of IP addresses from which

management access to the HBS is permitted. This list is stored on the HBS, and is independent of a RADIUS server, although it works only when RADIUS authentication mode is enabled.

Prepare Files for the RADIUS Server

Prepare two files for the RADIUS server: Data Dictionary supplement and Users definitions.

Data Dictionary supplement:

This is a supplement to the standard RADIUS Data Dictionary. This file defines the user profiles. Add this text to the end of the standard RADIUS Data Dictionary. An example supplement looks as follows:

```
#vendor id
VENDOR    RADWIN          4458

BEGIN-VENDOR RADWIN

# User Permissions Profile, the attribute starts with "number"=10 in
# order not to collide with previous RADWIN RADIUS definitions for HSU
# Authorization
ATTRIBUTE RADWIN_UserProfile 10 integer

VALUE RADWIN_UserProfile ObserverHbsObserverHsu 1
VALUE RADWIN_UserProfile AdminHbsAdminHsu 4
VALUE RADWIN_UserProfile InstallerHbsInstallerHsu 5
VALUE RADWIN_UserProfile OperatorHbsOperatorHsu 6
VALUE RADWIN_UserProfile OperatorHbsInstallerHsu 7
VALUE RADWIN_UserProfile ObserverHbsOperatorHsu 8

#ObserverHbsObserverHsu is identical to ReadOnlyHbsReadOnlyHsu

ATTRIBUTE RADWIN_SessionTimeout 11 integer

END-VENDOR RADWIN
```

The above example shows that the UserProfile is defined as attribute "10", to differentiate it from other attributes defined in this file.

- The first profile definition is called "1", the second profile definition is called "4", the third is "5", and so on.

User definitions

The Users file (users.conf) defines the list of users who are allowed to access this sector (HBS), what user profile each one has, and a timeout value (in seconds) after which access is denied. An example appears as follows:

```
# User Name = SectionHead, Password = SunBoss_365, Read-Write
# permissions HBS and HSU, Timeout 24h
SectionHeadCleartext-Password := "SunBoss_365"
    RADWIN_UserProfile = 4
    RADWIN_SessionTimeout = 86400

# User Name = LocalTech, Password = Moon_Crater, Read-Only permissions
```

```
# HBS, Read-Write permissions HSU, Timeout 1h
LocalTechCleartext-Password := "Moon_Crater"
    RADWIN_UserProfile = 1
        RADWIN_SessionTimeout = 3600
```

This above example shows that there are two users with the following usernames: SectionHead and LocalTech.

SectionHead has a password = SunBoss_365

His user profile is "4", meaning he has read and write access to all radios (according to the definition of user profile 4 in the dictionary example shown above)

His timeout value is 86,400 seconds, meaning that he has 24-hour access from the time of his log on. Note that the user will be automatically re-authenticated before this timeout expires.

LocalTech has a password = Moon_Crater

His user profile is "1", meaning he has read-only access to all radios (according to the definition of user profile 1 in the dictionary example shown above).

His timeout value is 3600 seconds, meaning that he has 1-hour access from the time of his log on.

RADIUS User Authentication

Select the HBS, then from the **Management** option, select **RADIUS User Authentication**.

Enable RADIUS Users Authentication ⓘ

Authentication server settings:

IP Address	Port	
0.0.0.0	1812	⚙️
0.0.0.0	1812	⚙️

NAS identifier:
Name ▾ Enable Access Control List

Access Control List ⓘ White Access List ⓘ

IP Address	Subnet Mask	
0.0.0.0	0.0.0.0	⚙️
0.0.0.0	0.0.0.0	⚙️
0.0.0.0	0.0.0.0	⚙️
0.0.0.0	0.0.0.0	⚙️
0.0.0.0	0.0.0.0	⚙️

Cancel Save

To enable the RADIUS authentication mode, check **Enable RADIUS Users Authentication**.

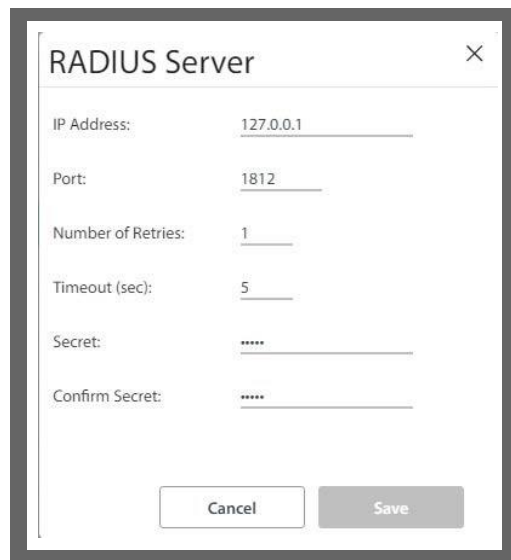


Any time you enter this configuration page, or when you enable one of the options, you will be reminded that you must run the connectivity check to enable the RADIUS User Authentication option. The connectivity check button appears

only after you have entered the connectivity information for the RADIUS server.

Authorization server settings: This shows a list of the available RADIUS servers, their IP addresses, their connection Ports (this is usually 1812), and their Statuses (Check Connectivity, Testing, or Connected), in addition to a configuration button and trash button.

Click the configuration button (⚙️) to open the RADIUS server parameters dialog box.



IP Address: Enter the IP Address of the RADIUS server here.

Port: Enter the communication port to which the HBS connects (usually 1812).

Although you can use the same IP for the different functions of the RADIUS server, you must still use a different port for each function.

Number of Retries: If the first attempt at establishing a connection with the RADIUS server was unsuccessful, carry out this number of retries before moving on to the next available RADIUS server.

Timeout: If there is no response from the RADIUS server after this many seconds, disconnect. A message will appear indicating this situation.

Secret: Secret of the RADIUS server.

Click **Save** to have your changes take effect.

NAS Identifier: If the Access Control List was enabled, then each time the HBS authenticates a user, it reports this fact to the authorization RADIUS server. The report is based on either the Device Name of the HBS or the Device Location, according to your selection in here.



The NAS Identifier Convention chosen here will also change the NAS Identifier Convention for the [802.1x](#) Authentication option, even though the RADIUS server here and that used in the [802.1x](#) Authentication option are not necessarily the same server.

Enable Access Control List: If this is enabled, then only users accessing the system from the IP addresses in the list can access the HBS.

Access Control List

This is a list of IP addresses from which access to the HBS is permitted.

This list is applicable only if both the Enable RADIUS Users Authentication, and the Enable Access Control List box have checkmarks in them.

White Access List

This is a list of IP addresses from which access to the HBS is permitted.

Although the HBS does not query the RADIUS server for authentication for this list, this list is nevertheless applicable only if the Enable RADIUS Users Authentication box has a checkmark in it.

- Each item in each of these lists shows an IP address and subnet mask.
- To change or add an item to each of these lists, click the configuration button (⚙️) to open the RADIUS server parameters dialog box. In this box, you can only change the IP address and the Subnet Mask of the Access Control List item or the White Access List item:

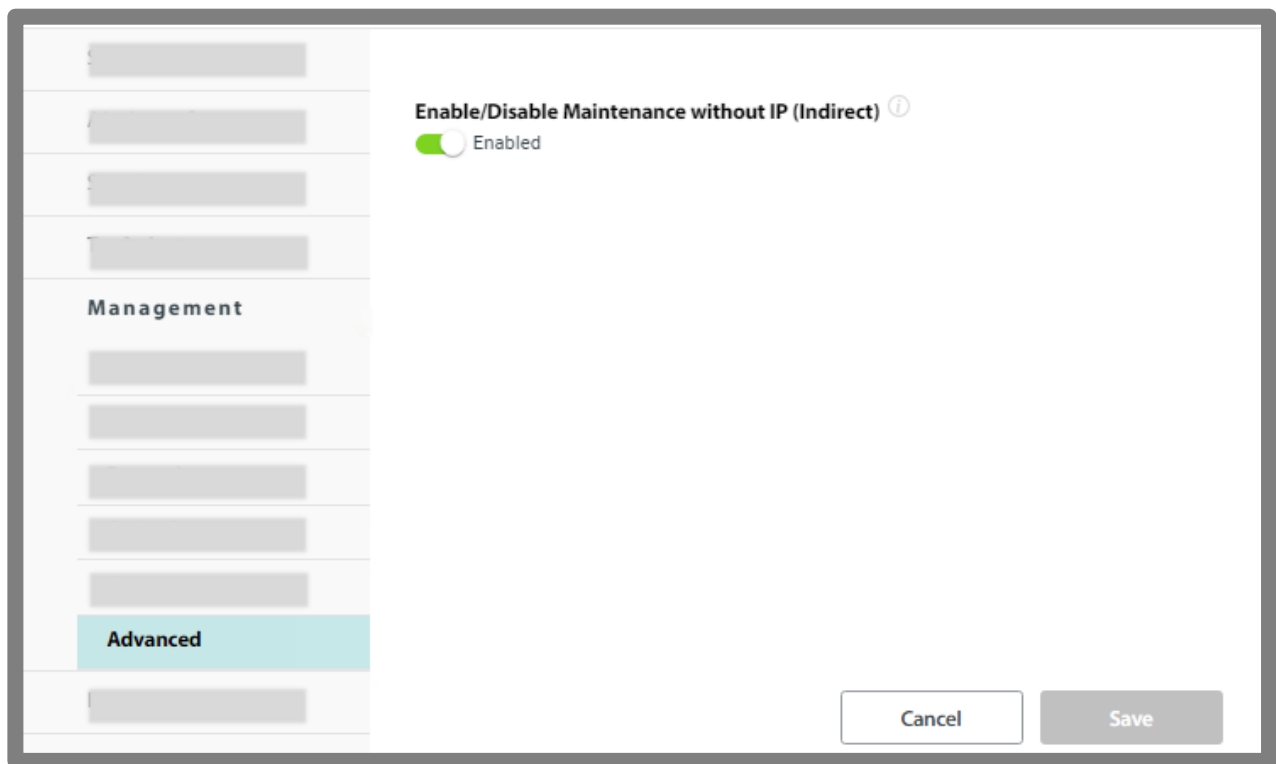


- The authorization RADIUS server and the authentication RADIUS server can be either the same or two different servers.
- Click **Save** to have your changes take effect.

Advanced

Enable / Disable maintenance without IP (indirect)

This option enables to perform SW upgrade or backup to SU devices via the BS without using the IP address of the SUs, meaning without having IP connection to the local IP address of the SU. If you don't use SW upgrade or backup without IP, or wish to disable IP forwarding, disable this option.



11.3.7. Hub Site Sync (Hub site only)

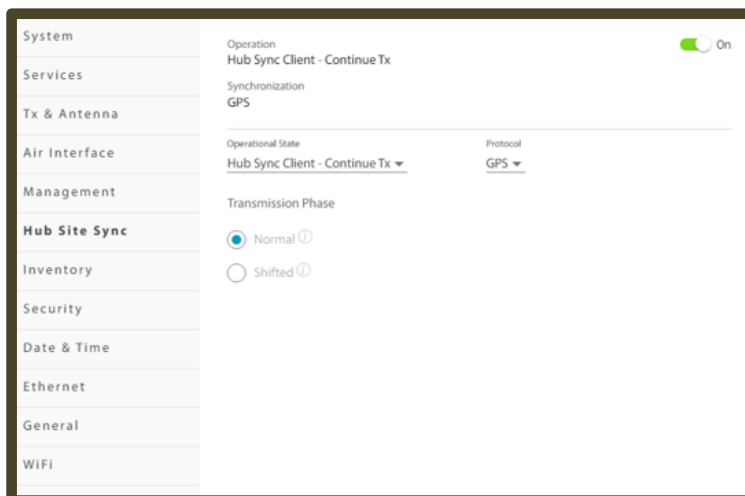
If there are co-located radio units with your Hub site, they can interfere with each other. The Hub Site Synchronization (HSS) feature was created to prevent this.

To enable Hub Site Synchronization, click the switch next to “Independent Unit” to **On**.

See the *Hub Site Synchronization Application Note* for more details.

Protocol is:

When “Ethernet” protocol is selected, the unit is synchronized via the Ethernet (HSSoE – HSS over Ethernet). Alpha h/w that supports GPS has the option to select the “GPS” protocol and to synchronize to the internal GPS.

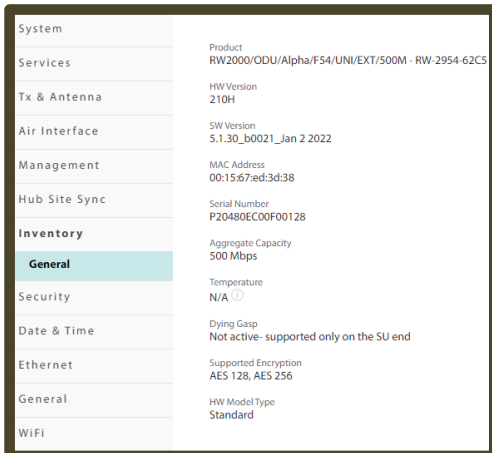


11.3.8. Inventory

This shows the identification information for the selected unit: Product version, hardware version and software version, MAC address, serial number, aggregate capacity, the present temperature inside the unit, the unit's power consumption, supported encryption, h/w mode type and if the Dying Gasp feature is active.

Note that there is an indication of Special edition CBWs for Alpha units with special h/w that does not support CBW of 10Mhz.

You cannot see the IP address here. Go to **Configure -> Management -> Network** to see the IP address of the selected unit.

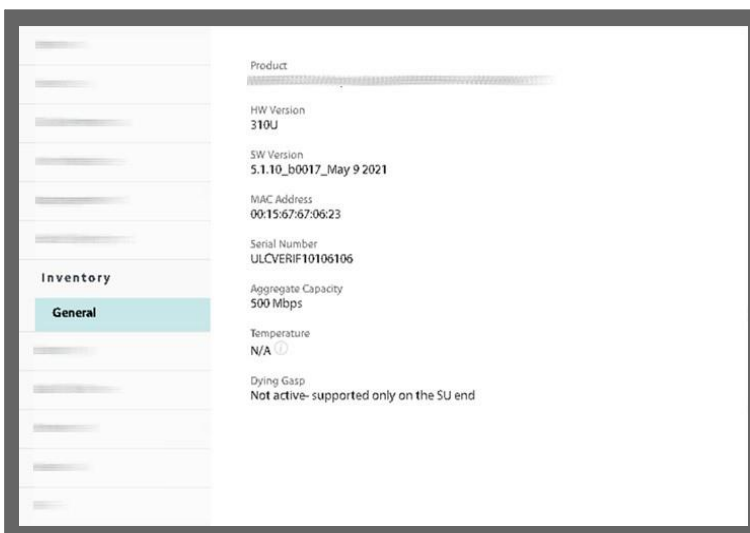


System	
Services	Product RW2000/ODU/Alpha/F54/UNI/EXT/500M - RW-2954-62C5
Tx & Antenna	HW Version 210H
Air Interface	SW Version 5.1.30_b0021_Jan 2 2022
Management	MAC Address 00:15:67:ed:3d:38
Hub Site Sync	Serial Number P20480EC00F00128
Inventory	
General	Aggregate Capacity 500 Mbps
Security	Temperature N/A
Date & Time	Dying Gasp Not active- supported only on the SU end
Ethernet	Supported Encryption AES 128, AES 256
General	HW Model Type Standard
WiFi	

Dying Gasp

Dying Gasp feature: If the unit was shut down due to a power outage, a signal is sent indicating that the reason for the sync loss is a power outage at the RT-B(HSU) that lost the power. Note the following:

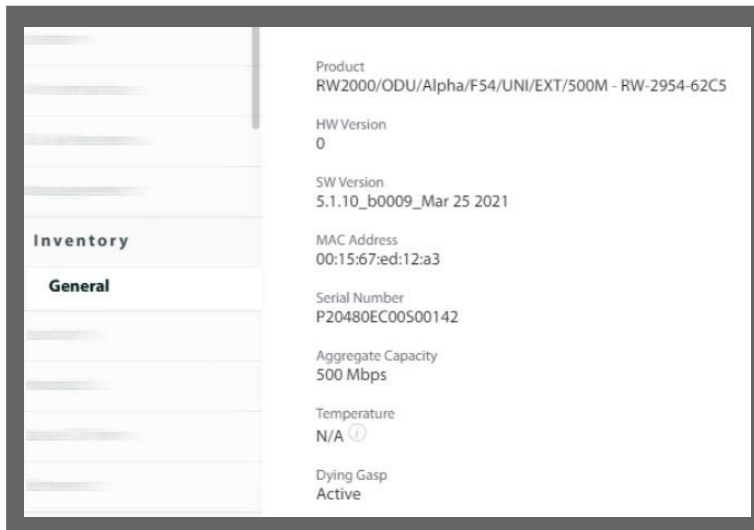
- > The Dying Gasp signal is sent from RT-B(HSU) (Slave ODU or Client site) units only. The signal is not sent from RT-A(HBS) (Master ODU or HUB site) units, and is indicated as being not active.
- > You must use an appropriate PoE for the RT-B(HSU) unit for the Dying Gasp feature to work. The PoE voltage must be ≥ 55 V. If the PoE voltage you are using is lower than 50V (such as 24V POE unit or voltage degraded over the cable), Dying Gasp will be inactive.



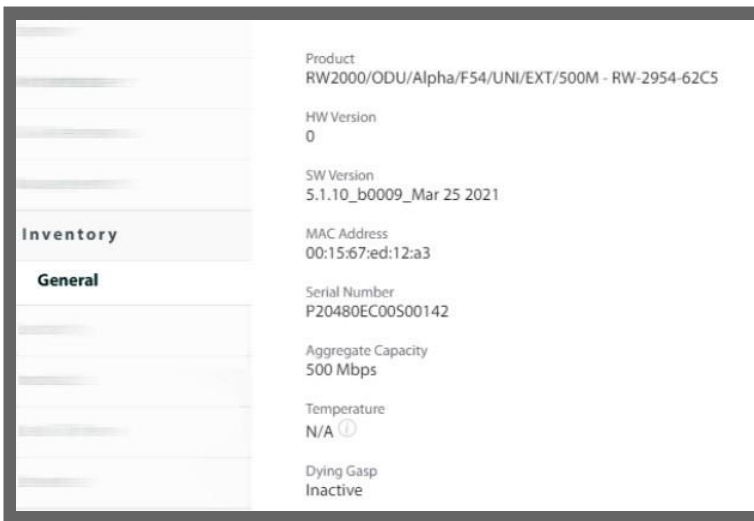
System	
Services	Product [REDACTED]
Tx & Antenna	HW Version 310U
Air Interface	SW Version 5.1.10_b0017_May 9 2021
Management	MAC Address 00:15:67:67:06:23
Hub Site Sync	Serial Number ULCVERIF10106106
Inventory	
General	Aggregate Capacity 500 Mbps
Security	Temperature N/A
Date & Time	Dying Gasp Not active- supported only on the SU end
Ethernet	
General	
WiFi	

**Dying Gasp on RT-A(HBS):
not relevant**





**Dying Gasp on RT-B(HSU):
active**



**Dying Gasp on RT-B(HSU):
Inactive: Low PoE voltage**

- > Feature supported only when AC (of AC PoE) or DC (on DC PoE) input disconnected since it based also on internal capacitance of PoEs
- > Feature supported on PtP and PtMtP (up to 16 CPEs)

11.3.9. Security

The Security dialog enables you to change the SNMP Community strings.

You can also create an encrypted SNMP Community string value file or set and change the link Password and the user password.

SNMP Communities

Each radio unit communicates with the managing computer using the SNMPv1 or SNMPv3 protocol. The SNMPv1 protocol defines three types of communities:

- Read-Only, for retrieving information from the radio unit
- Read-Write, to configure and control the radio unit
- Trap used by the radio unit to issue traps

The read-write Community strings and read-only Community strings have a minimum of five alphanumeric characters. Changing the trap Community is optional.

Editing SNMPv1 Community Strings

When editing these strings, both read-write and read-only Communities must be defined.

➤ To change a Community string:

1. Type the current read-write Community in the **Current Read-Write Community** field (default is *netman*).
2. Click the check box next to the community whose string you wish to change.
3. Type the new Community string and re-type to confirm. A community string must contain at least five and no more than 32 characters excluding SPACE, TAB, and any of ">#@|*?;.,"
4. Click **Save** to have your changes take effect.

Security Mode

The Alpha EMB/Int offers an enhanced version of its usual secured method of working, which offers extra protection against unauthorized access of the system.

It is performed on a unit-by-unit basis and is independent of link structure or hierarchy.

Implement this mode as follows:

1. Make sure you are logged in to the unit via HTTPS (see [Web Interface](#)).
2. Enter the username and password. These are the same values that you used when you logged in to the unit.
3. Click Authenticate.
4. Choose one of the following options:

Secured:	2000-Plus secured operation
	Immediately implement the enhanced security option. When and if the unit is reset, there is a 2-minute grace

Enhanced Security*:
period where the enhanced security option is temporarily removed. After this time, the enhanced security option is re-established automatically.

Enhanced Security:	Immediately implement the enhanced security option.
---------------------------	---

5. Click **Save** to have your changes take effect.

Link Password

This item is available as follows:

- At an isolated Client site
- Never for an active Client site

The default password is *wireless-p2mp*.

➤ To change the link password:

6. Enter the current password.
7. Enter the new password.
8. Confirm the new password.

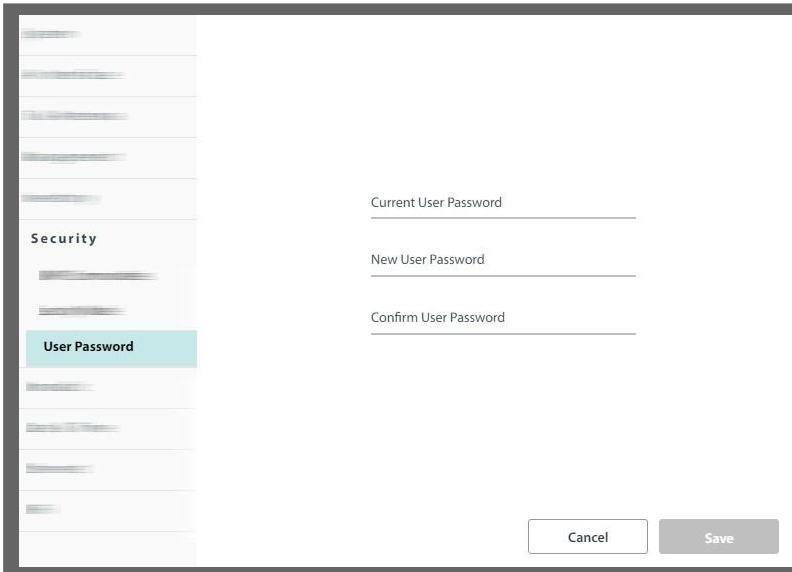


If you have forgotten your Link password, contact customer support.

User Password

➤ To change the user password of the present user:

1. Select **Security -> User Password**. The User Password dialog box opens.



2. Enter the current password.
3. Enter the new password.
4. Confirm the new password.
5. Click **Save**.

11.3.10. Date & Time

Here you can set the date and time of the selected unit, whether manually, based on local time, or on an NTP Server.

The radio unit maintains a date and time. The date and time should be synchronized with any Network Time Protocol (NTP) version 3 compatible server.

During power-up, the radio attempts to configure the initial date and time using an NTP Server. If the server IP address is not configured or is not reachable, a default time is set.

When configuring the NTP Server IP address, you should also configure the offset from the Universal Coordinated Time (UTC). If there is no server available, you can either set the date and time, or you can set it to use the date and time from the managing computer. Note that manual setting is not recommended since it will be overridden by a reset, power up, or synchronization with an NTP Server.



Note

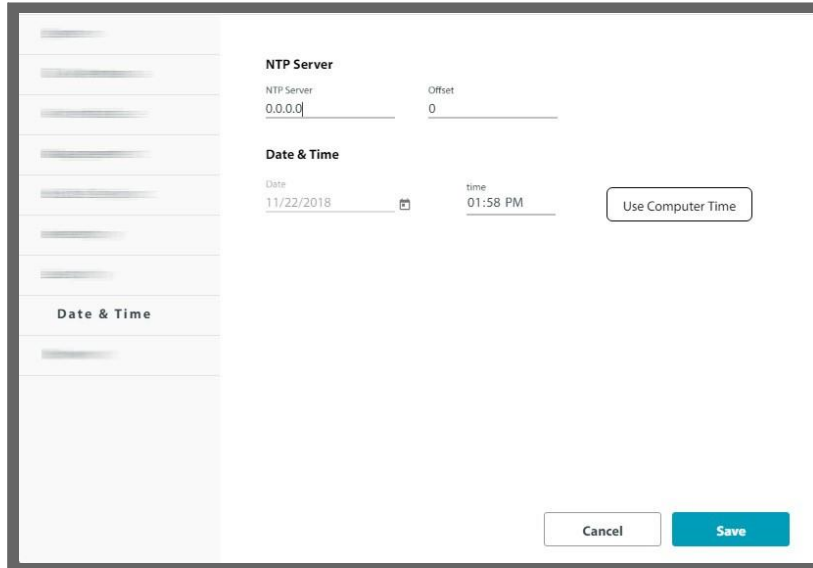
The NTP uses UDP port 123. If a firewall is configured between the radio and the NTP Server, this port must be opened.

It can take up to 8 minutes for the NTP to synchronize the radio date and

time.

➤ **To set the date and time:**

1. Determine the IP address of the NTP server to be used.
2. Test it for connectivity using the command (Windows XP and 7), for example:
w32tm /stripchart /computer:216.218.192.202



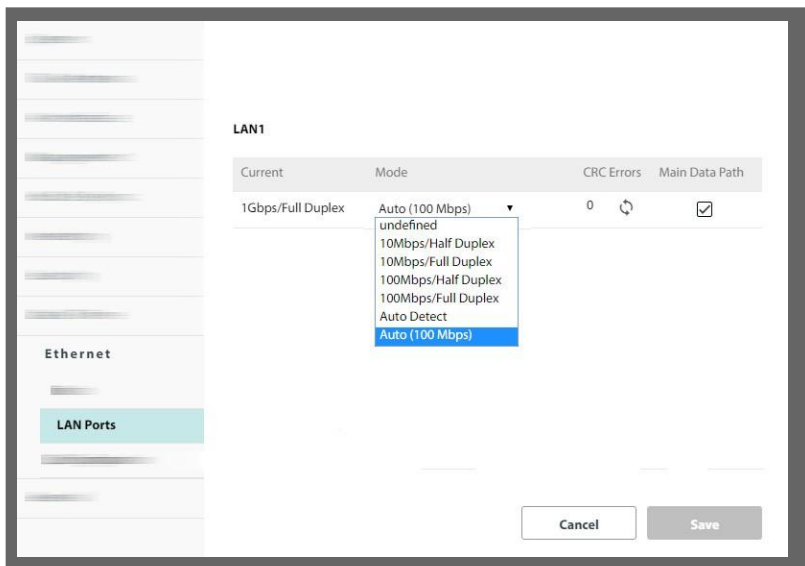
3. If entering an IP address for the NTP Server, enter the new address.
4. Set your site Offset value in minutes ahead or behind GMT (Greenwich Mean Time)
5. To manually set the date and time, click the calendar icon and choose the new date, then click the spinner next to Time to choose the time.
6. To set the time based on the time of the managing computer, click Use Computer Time.
7. Click **Save** to have your changes take effect.

11.3.11. Ethernet

In this category, you can configure the ratio between the uplink and downlink (Tx Ratio), the input ports on the unit, and the QoS (quality of service).

LAN Ports

- The input port (called here “LAN1”) is configurable for line speed (10/100BaseT) and duplex mode (half or full duplex).
- An Auto Detect feature is provided, whereby the line speed and duplex mode are detected automatically using auto-negotiation¹. Use manual configurations when attached external equipment does not support auto-negotiation. The default setting is Auto Detect.

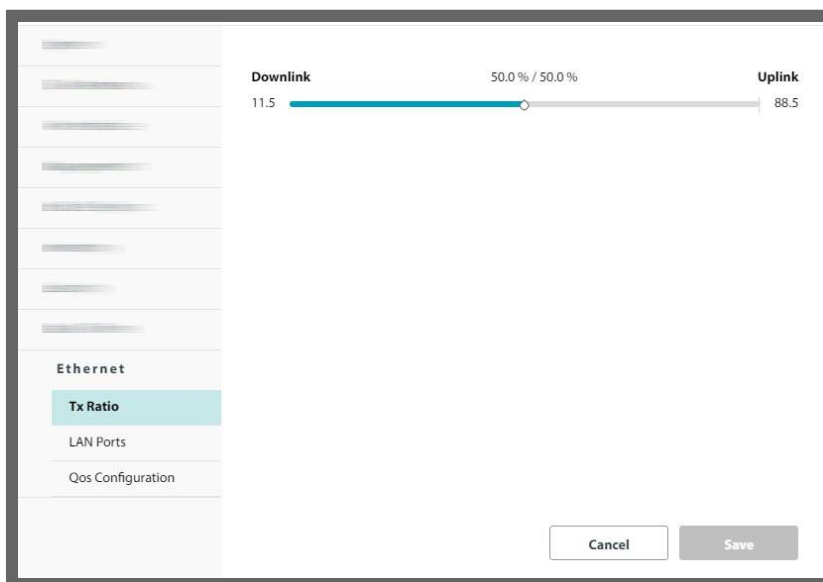


CRC Errors shows how many Cyclic Redundancy Check errors occurred since the last reset.

Tx Ratio (Hub site only)

The **Tx Ratio** (Transmission Ratio, Asymmetric Allocation) shows the allocation of throughput between downlink and uplink traffic at the Hub site. The Transmission Ratio is not only sector-wide: If you use Hub Site Synchronization to collocate several Hub sites (to cover adjacent sectors), they must all use the same Transmission Ratio.

1. Move the slider to the right or left to determine the Tx Ratio.
2. Click **Save** to have your changes take effect.



The allowable range is from 50/50 % to 88/11 %. Setting values beyond this range will cause unpredictable results.

You must ensure that the range remains within allowable values. There is no fail-safe.

shown as well as link distance. In this context, “link” is any collocated RADWIN HBS, not necessarily an Alpha EMB/Int.

QoS Configuration (Hub site)

QoS (Quality of Service) is a technique for prioritization of network traffic packets during congestion.

2000-Plus sectors support two classification criteria: 802.1p priority (referred to as "VLAN" for simplicity) or Diffserv based. You may choose which of them to use. To work with them properly, you must be familiar with the use of VLAN (802.1p) or Diffserv.

This section describes how to configure QoS for the Hub site for the link. However, to fully configure QoS properly, you must also configure it for each Client site as well. To configure QoS from the Client site side, see [QoS Configuration \(Client site\)](#).

Based upon the classification criterion chosen, received packets will be mapped into one of four quality groups: Real time, Near real time, Controlled load or Best effort. You may partition the total link capacity across the four Quality queues. The default weights, as percentages, are shown in the table below:

Quality queue	Priority	
	Diffserv	VLAN
Real time	48-63	6-7
Near real time (responsive applications)	32-47	4-5
Controlled load	16-31	2-3
Best effort	0-15	0-1

You can also define part of the link capacity as carrying Voice-over-IP traffic. This is similar to defining part of it as Real time (see [Enabling a VoiP Queue \(Hub site\)](#)).

1. From the Mode pull-down menu, Choose either the VLAN or Diffserv method.
2. For the method you selected, type the Priority Mapping for each queue. This determines the mapping (or translation) of the priority mapping of the traffic to what is used by the Alpha EMB/Int. Default settings for Diffserv and VLAN are as shown in the next two figures:

The screenshot shows the QoS Configuration interface. The Mode is set to VLAN. The Priority Mapping table is as follows:

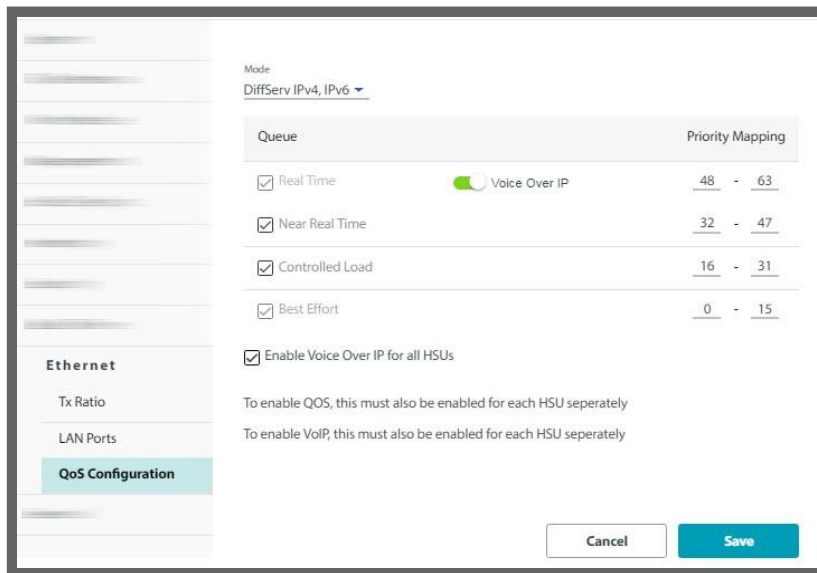
Queue	Priority Mapping
<input checked="" type="checkbox"/> Real Time	6 - 7
<input checked="" type="checkbox"/> Near Real Time	4 - 5
<input checked="" type="checkbox"/> Controlled Load	2 - 3
<input checked="" type="checkbox"/> Best Effort	0 - 1

Additional options include:

- Enable Voice Over IP for all HSUs

Notes: To enable QoS, this must also be enabled for each HSU separately. To enable VoIP, this must also be enabled for each HSU separately.

Buttons: Cancel, Save



3. If you un-check a queue, this queue will be ignored for the sector. It will not prevent the Client site from configuring traffic labeled with this priority level as “live”; it will merely ignore its priority level, as if the traffic was not assigned with any priority level whatsoever. You cannot un-check the Best Effort queue.

Enabling a VoIP Queue (Hub site)

Note the following:

- If a VoIP queue is enabled from the Hub site, it is applied to the Client site presently used in the link. If you replace this unit with different Client sites after the VoIP queue was defined, do one of the following:
 - Enable VoIP on new Client sites (this is the intention of the note “To enable VoIP, this must also be enabled for each HSU separately”), or
 - Re-enable it for the link from the Hub site.
- To configure VoIP from the Client site side, see [Enabling a VoIP Queue \(Client site\)](#).
- The VoIP feature, as implemented here, assumes that your end-user has a gateway or other network device that defines the traffic to be VoIP with the correct QoS defined (VLAN or DiffServ, in accordance with your configuration done here). The definition must be done at both ends of the data stream.
- Enabling a VoIP queue may decrease the link’s peak throughput in some scenarios. Therefore, make sure that you absolutely need to enable a VoIP queue before doing so.
 1. Click Voice Over IP. The Real Time queue will become disabled. This means that VoIP traffic is treated in a similar fashion to Real Time traffic. VoIP works whether you are using VLAN or DiffServ.
 2. Optionally, apply VoIP to the Client sites of the link by clicking on Enable Voice Over IP for all HSUs.
 - If you do not choose this, you must go to the Client site and enable it there.

Click **Save** to have your changes take effect.



Make sure the “Mode” selected is the proper one, is consistent throughout your configuration, and that your end-user has equipment that also defines its VoIP traffic with the Mode you defined here.

11.3.12. General (Hub site only)

In this category, you can configure the Aging Time.

Tx & Antenna	
Air Interface	Aging Time 300 seconds
Management	
Hub Site Sync	
Inventory	
Security	
Date & Time	
Ethernet	
General	
WiFi	

Aging Time

The Hub site works in Bridge Mode. In this mode, it performs both learning and aging, forwarding only relevant packets over the sector. The aging time of the Hub site is by default 300 seconds, although you can change this value here.

11.3.13. WiFi

System	SSID R-P20480EC00F00128	Status Connected	
Services			
Tx & Antenna	Access Point Mode Auto	Password *****	Security WPA2
Air Interface			
Management	IP Address 192.168.1.1	Channel 6	TX Power 15
Hub Site Sync	It is recommended to turn off the device Wi-Fi access before exiting your manager		
Inventory			
Security			
Date & Time			
Ethernet			
General			
WiFi			

Connected Clients		
#	MAC Address	RSSI[dBm]
1	20:16:B9:B7:23:B1	-63
2	5A:5A:84:B8:50:0F	-75
3	00:00:00:00:00:00	0
4	00:00:00:00:00:00	0
5	00:00:00:00:00:00	0

Cancel Save

The SSID status, Security method, and On status of the WiFi unit are displayed.

Access Point Mode:

- Auto: default. Turns on the wifi for 4 hours upon unit power on, and turns it off if no wifi client is connected within 4 hours.
- On: wifi always on
- Off: WiFi disabled

You can set the following WiFi parameters:

- password
 - Default password: “wireless”
- IP address
 - Default IP address is 192.168.1.1
 - Class C (/24) is always assumed
 - The WiFi access point will lease DHCP IP addresses in the same subnet
 - It is required to change the default IP to some other subnet in order to set the SU management IP in 192.168.1.x range
- channel
 - Default: channel 6
- Tx power
 - Default: 15 dBm. Possible range: 1 - 16dBm

Connected Clients:

This area shows up to 5 clients that are connected to this unit, including their MAC addresses and signal strength (RSSI).




Note

The SSID of the WiFi is R- [serial number of units]

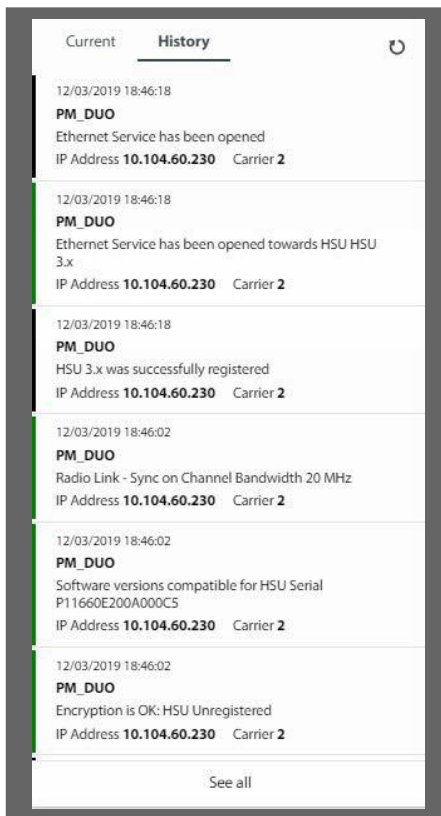
Click **Save** to have your changes take effect.

11.4. Events



1. To display the Events Log, first select the unit or units for which you want to display events. You can select any combination of units.
2. Click on the Events icon in the upper panel of the Web page ; The events

are displayed in the partial Events Log. This is a small version of the complete Events Log and shows a list of events according to the date and time they occurred, its source, a description of the event, IP address of the source, and on which Carrier the event was recorded.



3. Click **Current** to see alarms since the last log in (these are cleared once the alarm condition is removed), click **History** to see all events recorded.
4. Click **See all** to see the full Events Log.

Date & Time	Message	Source	IPv4	IPv6	Severity	Carrier	Interface
09/01/2005_00:23	Ethernet Service has been opened towards HSU Name192	Name190	10.0.0.190		normal		Radio Interface
09/01/2005_00:23	HSU Name192 synchronized	Name190	10.0.0.190		normal		Radio Interface
09/01/2005_00:23	Encryption is OK: HSU Name192	Name190	10.0.0.190		normal		Radio Interface
09/01/2005_00:23	Software versions compatible for HSU Name Name192	Name190	10.0.0.190		normal		Radio Interface
09/01/2005_00:21	HSU Name192 out of sync The reason is: Spectrum analysis.	Name190	10.0.0.190		critical		Radio Interface
09/01/2005_00:21	Ethernet Service has been closed towards HSU Name192	Name190	10.0.0.190		major		Radio Interface
09/01/2005_00:21	Software versions compatible for HSU Name Name191	Name190	10.0.0.190		normal		Radio Interface
09/01/2005_00:21	Encryption is OK: HSU Name191	Name190	10.0.0.190		normal		Radio Interface



The Events Log records system failures, loss of synchronization, loss of signal, compatibility problems and other fault conditions and events.

5. The Events Log may be saved as a Comma Delimited (CSV) or PDF file. Click **Download report** to do so.

The Events Log includes the following fields:

- » Date and time stamp
- » Message
- » Trap source (if the source is a radio unit, this is its name)
- » IP address of the unit that initiated alarm - IPv4 or IPv6. Use the pull-down menu here to filter the list according to the indicated criteria

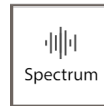
- » Severity of the trap (color-coded)

Critical	
Major	
Minor	
Warning	
Normal	
Info	

- » Carrier on which the trap was found (Carrier 1 or Carrier 2)
- » Interface of the trap

6. Click **Current** to see alarms since the last log in (these are cleared once the alarm condition is removed) or click **History** to see all events recorded.
7. You can filter the list of messages by IP or trap source by entering the desired item in the field at the top center of the window and clicking the spyglass icon.

11.5. Spectrum

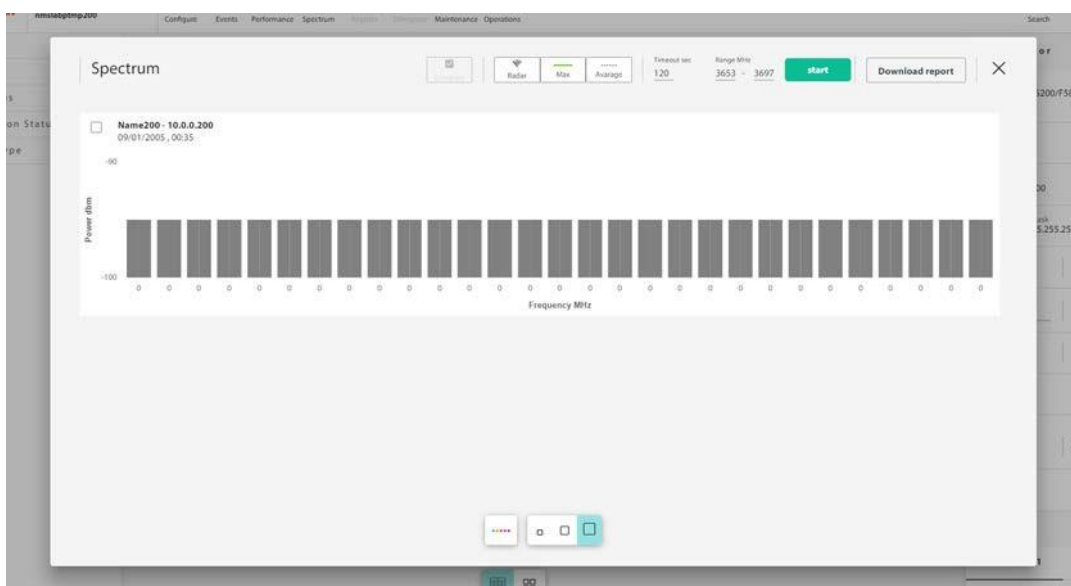


The Spectrum View utility is an RF survey tool that provides spectral measurement information, like power vs. frequency. You can view real-time spectrum information, save results, and view historic spectrum scans. The data is stored in the radio unit itself.

The results of the Spectrum View utility are intended for use by RADWIN Customer Service to assist with diagnosing interference related problems.

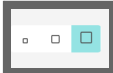
We assume the reader knows about RF Spectrum Analysis so detailed theoretical explanations are not needed.

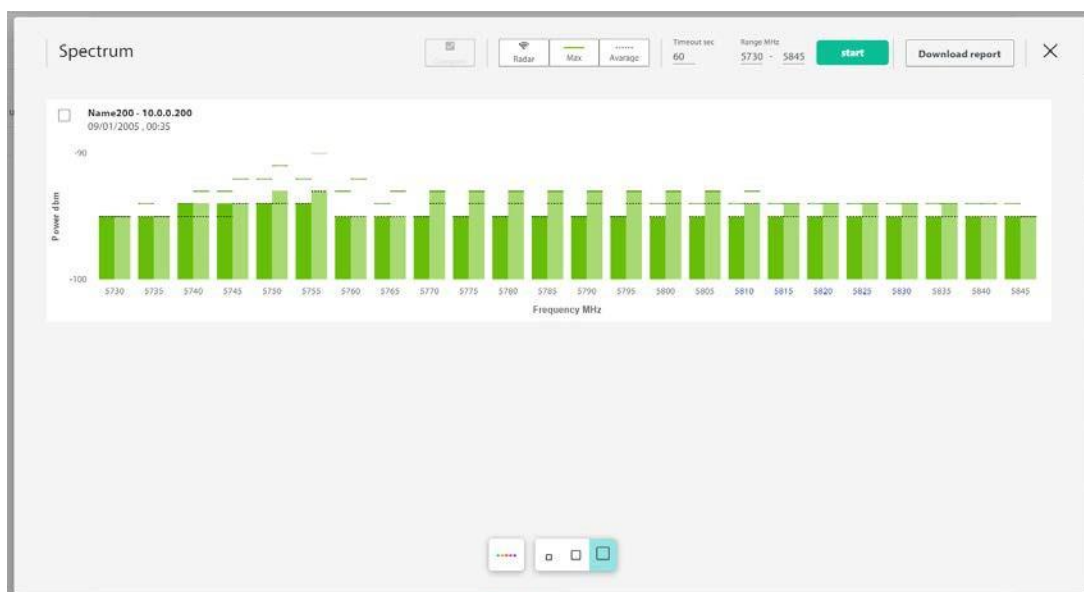
1. Click on the Spectrum View icon  . The Spectrum View window will appear.



A blank Spectrum View result display will appear, where all the bars are grey.

The name(s) of the selected unit(s) appear, together with their IP address(es), date and time.

2. The three box icons in the bottom of the window () allow you to adjust the size of the display so you can show results from more than one unit.
3. To start a scan, first choose its **Timeout sec** time (top of window), which is the maximum analysis time per scan.
4. Select the frequency range (**Range MHz**, top of window). You can only select allowed frequencies.
5. Once you are ready, click **Start** to start the scan and see the results on screen. You will be warned that this is traffic-affecting. If this is acceptable, then click **Yes**.



Green bars relate to those frequencies you chose when you activated the Hub site (see [Activate the Alpha EMB/INT](#)). Dark green is Antenna A and light green is Antenna B.

If there are frequencies that you did not choose when you activated the Hub site, their bars appear blue.

The frequencies the unit is working at has text that appear blue.

Green lines show the maximum power found for the indicated frequency range.

Dotted lines show the average power found for the indicated frequency range.

Radar shows/hides DFS information.

Compare allows you to compare the results from selected units, side-by-side.

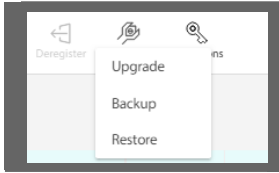
6. If you want to save the report, click **Download Report**, and select a location where to save the report file.

11.6. Maintenance



This allows you to upgrade, backup or restore the target software.

Choose the action you want from the pull-down menu.



11.6.1. Upgrade

1. Click **Choose Upgrade File** and locate the SWUL_5k.swul file.
2. The name, size, and status of the file will be shown.
3. Once you are sure that this is the correct file to use, select it, and click **Open**. The file will be uploaded to the unit and validated. A description of the file will be displayed.
4. Once you are sure that this is the correct file, click **Install**. The upgrade procedure will commence, and when completed, an indication will be shown.

11.6.2. Backup

We recommend carrying out a backup before carrying out a software upgrade.

1. Click **Download**.
2. The system will commence the backup procedure. Once it is finished, the name of the file and the date the backup was done will be shown in this window. Click **Done**.

11.6.3. Restore

3. The backup file will be located in the downloads location of the managing computer, with the extension *.backupl
4. You can retrieve this backup file by clicking on **Restore** and browsing to the file location.

If you wish to restore a previous configuration of the unit that you had already backed up, use this option.

1. Click **Choose Restore File**, and locate the desired *.backupl file.
2. The name, size, and status of the file will be shown.
3. Once you are sure that this is the correct file to use, select it, and click **Open**. A description of the file will be displayed.
4. Once you are sure that this is the correct file, click **Upload**. The restore

procedure will commence, and when completed, an indication will be shown.

5. Upon completion of the restore procedure, the unit will reset and then will operate according to the restored version.

11.7. Diagnostics

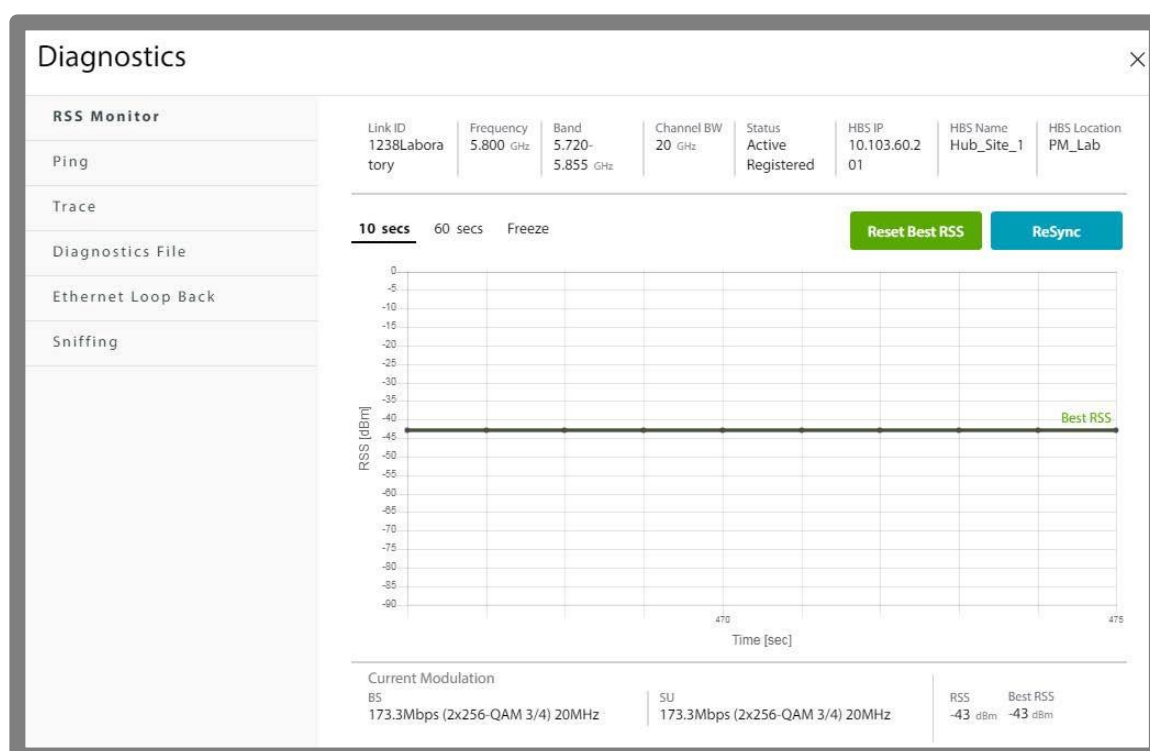


This category provides various tools: Radio Signal Strength display, a ping and trace capability, diagnostic files (to be used by RADWIN professional services), ethernet loop back, and radio unit sniffing.

Click this icon to open the **Diagnostics** window.

11.7.1. RSS Monitor

- This shows the Radio Signal Strength of the selected item or items in real time.
- You can set the re-fresh rate at 10 secs or 60 secs, or you can freeze the display at any point in time.
- The display shows both the present RSS and the best RSS achieved to the present point in time.
- Click Reset Best RSS to reset the best RSS counter and click ReSync to re-synchronize the radio units.
- Use this display when carrying out antenna alignment.



11.7.2. Ping

This is a standard ping function that also allows you to set the number of packets and the packet size sent in the ping action.

1. Enter the target IP address in the Target IP window.
2. Enter the number of packets to be sent in the ping action in the Packets window, and the packet size to be sent in the Packet Size window.
3. When you are ready, click PING. The button will display **Processing**. Do not interrupt the process.
4. After a few moments or longer, depending on the size of the values you entered above, the ping results will be shown.

The ping action is a one-time action and does not repeat indefinitely.

11.7.3. Trace

This is a trace route tool.

1. Enter the IP address of the target to which you want to carry out the trace.
2. When you are ready, click Trace. The button will display **Processing**. Do not interrupt the process.
3. The results will be shown on-screen.

11.7.4. Diagnostics File

This creates a diagnostic file to be used by RADWIN professional services and support personnel to expedite assistance.

1. Select the items for which you want information. If an item is not selected, the diagnostic file will not contain information for that item. If no items are selected, the Diagnostics icon will become disabled.
2. Click **Generate Diagnostics File**. The diagnostics process will begin, and a button will appear with the option to stop the diagnostics action.
 - > After a few seconds or minutes, a JSON file will be created, stored in the default downloads section of the managing computer.
 - > The format of this file name is **diagnostics-DATE TIME.json**.
3. Send this file to RADWIN professional services.

11.7.5. Sniffing

- The Sniffing (or “sniffer”) command captures and downloads TCP/IP packets on the line between the managing computer and the selected radio device.
- You can select sniffing using full mode or capture only the headers.
- Click **Start** to start the sniffing process. It will continue until you click **Stop**, or until the file reaches its maximum size (5MB).
- The process can be run in the background.
- Once you stop the process, click **Download** to download the *.pcap file.

- This *.pcap file is downloaded to the default download section of the managing computer. You can use an application, such as WinShark, to read this file.

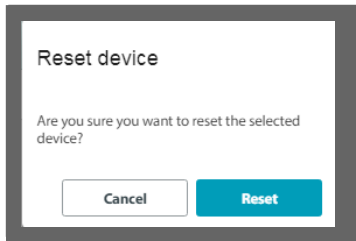
11.8. Operations



This icon allows you to perform a reset, restore the factory default settings, perform a license-dependent upgrade, or change the mode on the selected device.

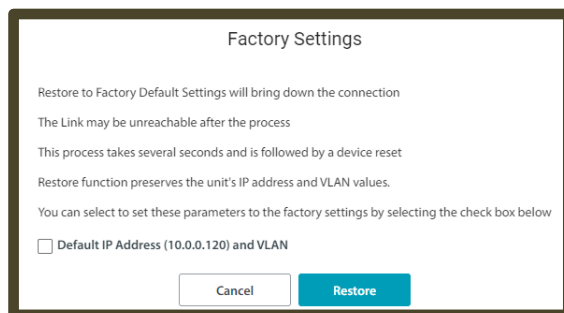
11.8.1. Reset

When you choose Reset, you are asked to confirm. If you are sure, click **Reset**.



11.8.2. Factory Default

When you choose Factory Default, you are asked to confirm. Since Factory Default involves a reset, it is traffic-affecting. You have an option to restore the default IP address (10.0.0.120) by clicking the box next to Default IP address. If you do not click this box, the device will retain its previous IP address and management VLAN. Once you are sure, click **Restore Defaults**, otherwise, click **Cancel**.



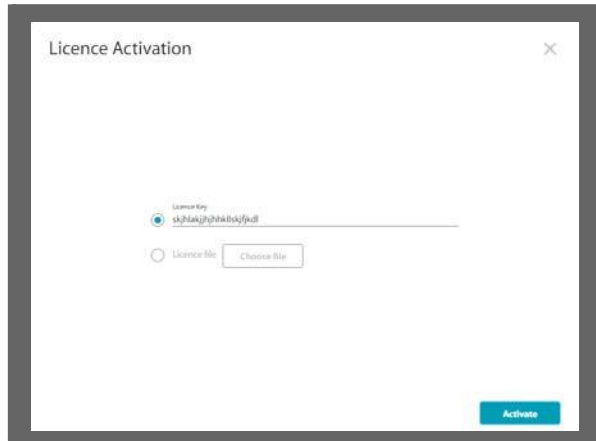
11.8.3. Licenses

To carry out a license-dependent upgrade, you must first acquire a license key. Do this as follows:

1. Catalogue number: Contact your RADWIN representative and get a catalogue number of the upgrade you want. Purchase as many of these upgrades as you deem necessary.
2. PAKs: You will receive a list of Product Activation Keys (PAK) for each upgrade instance. A PAK number can be used on any compatible RADWIN product; they are not specific to any one given item of equipment.
3. Activate PAKs: Associate each PAK to a specific item of equipment: Access the License Key Application website: <http://tools.radwin.com/updates/licensekey/lk-radwin.htm>, and follow the instructions there to activate each PAK for the specific

item of equipment you need to upgrade.

4. Get License Keys: The License Key Application will then give you a list of license keys. These numbers *are* unique for the specific upgrade and specific item of equipment. We recommend saving this list as a text file in a convenient location.
5. Select the device for which you want to apply a license-dependent upgrade.
6. Choose **Operations** -> **License**. The License Activation window will open.



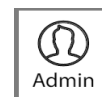
7. Enter the license code in the field, or click **License file**, then **Choose file** to where you want to save the license file.
8. Once you are ready, click **Activate**.
9. The unit will be reset, after which it will be upgraded using the new license.

11.8.4. Change Mode

Also called Change ODU Mode, this option allows you to change the unit from a Client site to a Hub site and vice versa.

- All units are shipped as being a Client site, and when you first set up the link, you must define one as being a Hub site. Do that here.
- Note that when you change the mode, the settings on the selected radio unit will be restored to factory default.
- To change to a Hub site from a Client site: Click **Switch to HBS**
- To change to a Client site from an Hub site: Click **Switch to HSU**

11.9. User Profile Icon



Admin, Observer, Operator, Installer

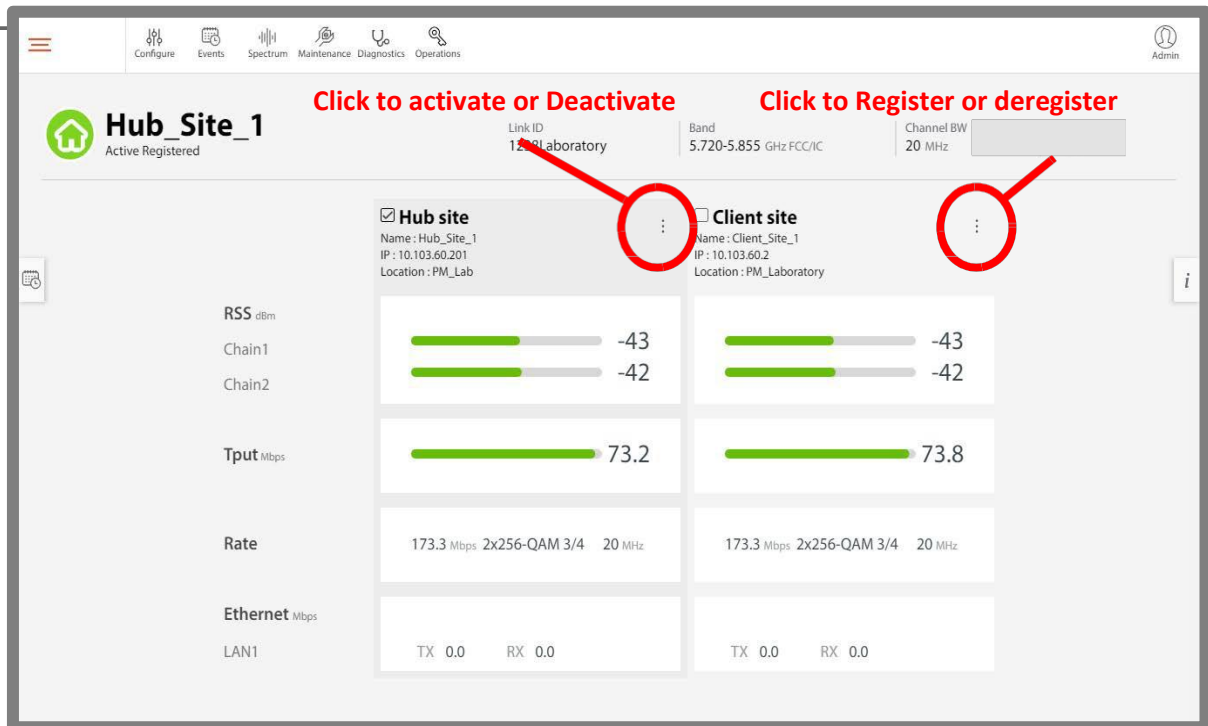
The name of the user profile will appear on the icon. Click this icon to log out of the unit.

11.10. Radio List

The mid-section of the user interface shows the status of the units.

- Unit name
- IP address

- Location
- RSS for each stream (RSS1 and RSS2), on both the Hub site side and the Client site side
- Throughput for the uplink and downlink
- Tx/Rx ratio for each line (LAN1 and LAN2)



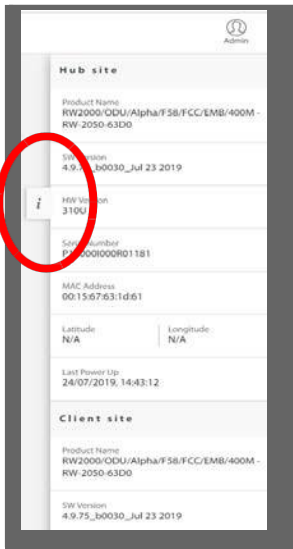
- To activate a Hub site, click on its pull-down menu, and select **Activate**.
- To de-activate a Hub site, click on its pull-down menu, and select **Deactivate**.
- To register a Client site, click on its pull-down menu, and select **Register**.
- To de-register a Client site, click on its pull-down menu, and select **Deregister**.

11.11. Right Pane

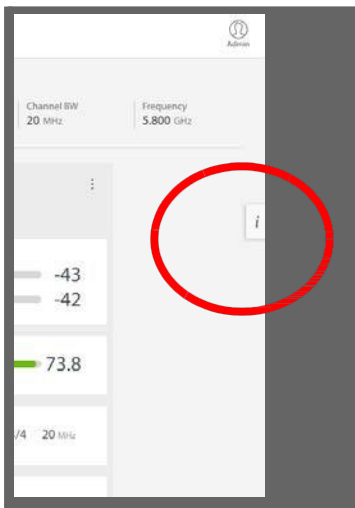
The right pane of the user interface gives a brief overview of the equipment of the link, showing the following:

- Both Hub site and Client site product name
- Software version of target (SW Version)
- Hardware version (HW Version)
- Serial Number
- MAC Address
- The unit's latitude and longitude
- The unit's up time since last reset

To minimize the right pane, click on the minimize symbol:



- To restore the right pane, click on the minimize symbol again:



11.12. First-Time Use

When working with an Alpha EMB/Int base station for the first time, carry out these tasks:

Update Connection Parameters - Change the IP address of both Alpha EMB/Int units, and any other connection parameters in accordance with your radio plan. Although this can be done later, we recommend doing this as soon as possible.

Define one unit as the Master ODU - units are shipped as “Slave ODUs”. Define the other one as a “Master ODU”

Activate the Alpha EMB/Int - this must be done for each unit.

Register the Client site Unit

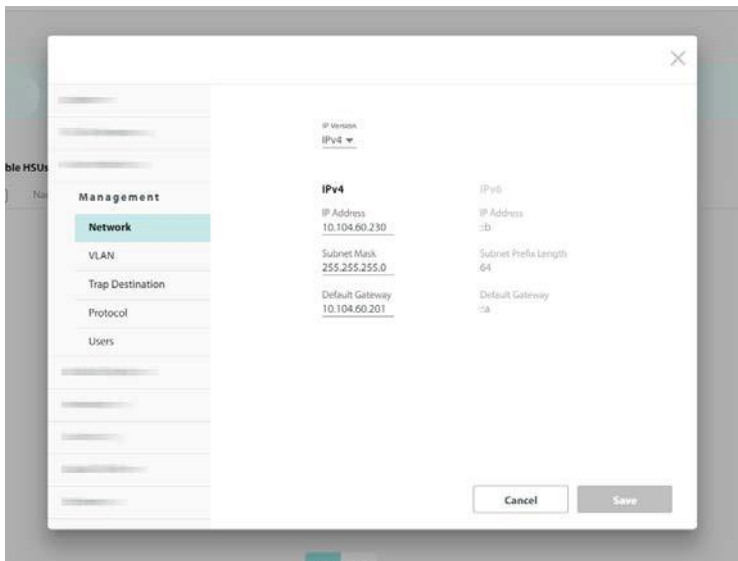
11.12.1. Update Connection Parameters

When first logging on to a new Alpha EMB/Int radio, you should change its IP address in accordance with your radio plan.

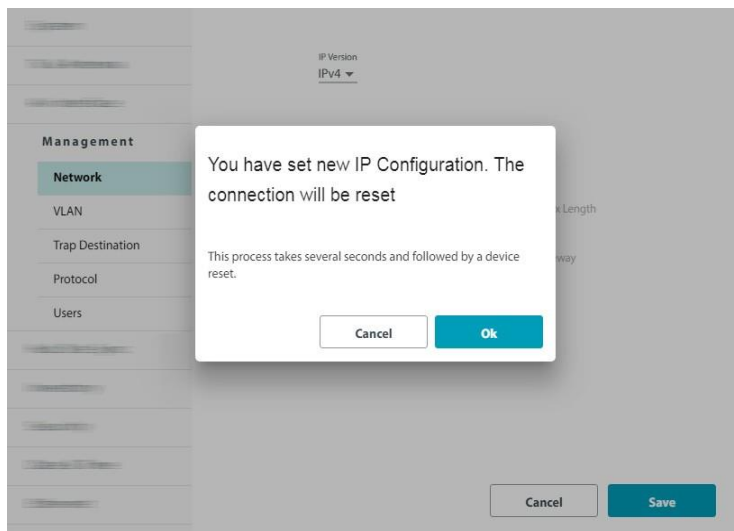
1. Connect the radio to the network and voltage via its input port.
2. Enter its IP address in a web browser (default value: 10.0.0.120).
3. Enter username **admin** and password **netwireless**.

4. Click the **Configure** icon ().

5. Select **Management -> Network**:



6. Enter the new IP address, Subnet Mask and Default Gateway in accordance with your radio plan, then click **Save**.
7. You will be warned that you will be logged out, and the device will be reset. If all the values are correct, click **OK**.

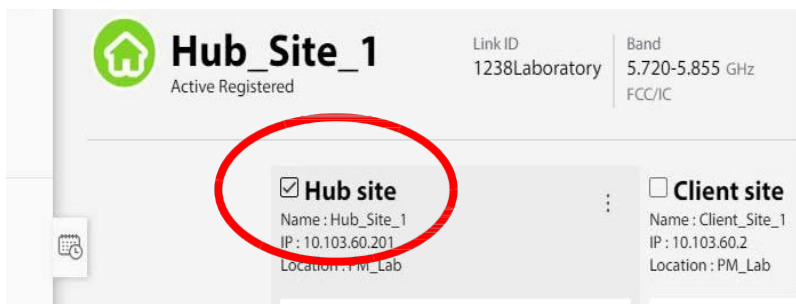


8. Once the unit is reset, log in again, using the new IP address.

11.12.2. Define one unit as the Master ODU

All units are shipped as a “Slave ODU”. You must define the other one as a “Master ODU”.

1. Enter the IP address of the radio that is to be the Master ODU (Hub site) in a web browser.
2. From the login page, enter username **admin** and password **netwireless**.
3. Select the unit that is to be the Hub site by placing a checkmark next to its name:



4. Click the **Operations** icon 

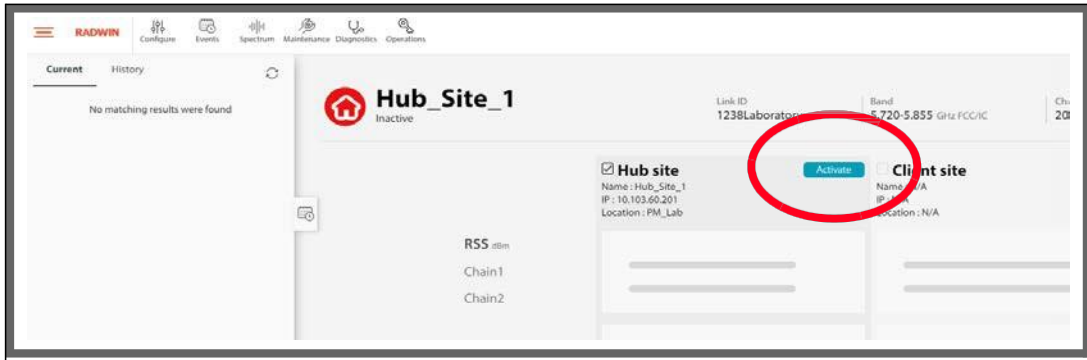
5. Select **Change Mode**.


6. You will be warned that changing the mode will disconnect the link. This is not a problem if you have a direct connection to the unit. Note also that any previous settings on the unit will be deleted. If this is acceptable, click **Switch to HBS**.

7. The unit will reset. Once the login page reappears, log in again.

8. Verify that the mode has changed to Hub site.

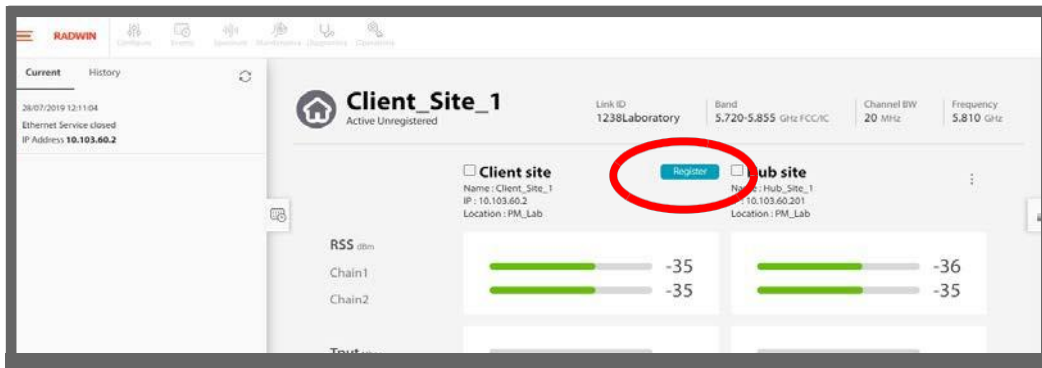
11.12.3. Activate the Alpha EMB/Int



1. Click the **Operations** icon (), then select **Activate**.
2. Fill out the information in the window that appears: Sector ID (equivalent to Link ID), sector name (equivalent to unit name), and Location. The Sector ID is used by both units; make a note of this value.
Set also its geographical location. There is an option to change the Link Password, if needed. When you are finished, click **Next**.
3. The operating channel and channel bandwidth will appear. We recommend you use the default values, but depending on the specific version of the product, these can be changed.
4. We also recommend you select Automatic Channel Selection, although you can select specific frequencies if your radio plan requires it. You must select at least two frequencies.
5. Click **Next**.
6. The Antenna window appears. Check the parameter values in this window and change any that need to be changed. Depending on the specific product in use, and especially the regulatory environment in which you are working, not all parameters can be changed.
7. Once everything is ready, click **Activate**.
8. If the activation is successful, a short message will appear, name of the unit will appear as active.

11.12.4. Register the Client site Unit

- Click **Register** next to the name of the Client site.



- You can register a Client site logged in directly to the unit, or from the Hub site.
- In a few moments, the unit will synchronize and show as being active and registered.

Appendix A: Terminology

Table A-1: Terminology (Sheet 1 of 5)

Term	Description
Assured throughput	Actual number of timeslots allocated to a radio unit.
ACS	Automatic Channel Selection. Option that instructs the radio to choose which frequency to use. Enabling or disabling this option has various ramifications, as shown in the documentation.
API	Application Program Interface
ATPC	Automatic Transmit Power Control
BE	Best Effort: A level of priority for traffic in which users receive dynamic resource allocation according to overall demand. They are not guaranteed resources. See also CIR .
BFD	Bidirectional Forwarding Detection. A network protocol used to detect faults between two forwarding engines connected by a link.
BS	Base Station: a radio that can transmit and receive to more than one point. See also HBS
CIR	Committed Information Rate: A level of priority for traffic in which users receive a guaranteed percentage of resources in addition to dynamic resources if available. See also BE .
CPE	Customer Premises Equipment
CSE	Customer Site Equipment
DBA	Dynamic Bandwidth Allocation: A method that allocates bandwidth between the various users of that same bandwidth in the network.

Term	Description
DBS	Dynamic Bandwidth Selection: When activating a base station, or when changing its bandwidth, if you choose the maximum value available for the bandwidth, the link may dynamically switch between the maximum value and values as low as 20MHz to ensure the best throughput.
DFS	Dynamic Frequency Selection: Products that have DFS enabled ensure no radar signal is present in the selected frequency channel within the band being used. If a radar signal is detected, that frequency channel is evacuated and the product will not transmit on this channel.
DHCP	Dynamic Host Configuration Protocol: a protocol that automatically assigns IP addresses and other network configuration parameters.
Diversity	A technique by which the reliability of a radio link is increased using multiple transmitting and receiving antennas, transmitting the same signal on all antennas.
Downlink	Data traffic from an HBS to an HSU, or Data traffic from an RT-A to an RT-B
DUO	Dual Band base station
EIRP	Equivalent (or Effective) Isotropically Radiated Power: The power that an antenna must emit to produce the peak power density in the direction of maximum antenna gain. In our case, this is usually: System Tx Power + Antenna Gain - Cable Loss.
FAA	Federal Aviation Administration. A U.S. federal office that manages aviation regulations throughout the United States.
Fixed (HSU)	A "fixed" HSU remains in one location, as contrasted with a nomadic or mobile HSU, which does not remain in one location.
GHSS	GPS Hub Site Synchronization
GRE	Generic Routing Encapsulation. A communication protocol used to establish a direct, point-to-point connection between network nodes. GRE lets two peers share data they wouldn't be able to share over the public network itself.
GRE Tunnel	A virtual point-to-point connection between two networks, using the GRE protocol to carry this out.
HBS	High-capacity Base Station. Same as a BS

Term	Description
HMU	High-capacity Mobility (subscriber) Unit. Similar to an HSU, but can be mobile.
HSC	Hub Sync Client: When using Hub Site Synchronization, one unit is a master (generates the sync pulses), and the other units are clients.
HSM	Hub Sync Master: When using Hub Site Synchronization, one unit is a master (generates the sync pulses), and the other units are clients.
HSU	High-capacity Subscriber Unit. Same as an SU
IGMP	Internet Group Management Protocol
ISU	Integrated Synchronization Unit: A network device that provides a synchronization signal to underground HBSs.
LFF	Large Form-Factor
MD5	Message digest algorithm: An authentication type for SNMPv3 connections.
MDL	Multiple Device Learning
MIMO	Multiple In, Multiple Out: A technique by which the capacity of a radio link is increased using multiple transmitting and receiving antennas, transmitting a different signal on all antennas.
MIR	Maximum Information Rate
Mobile (HSU)	A “mobile” HSU can move from location to location and provide service while it moves or when it is stationary.
Nomadic (HSU)	A “nomadic” HSU move from location to location but can only provide service when it is stationary.
ODU	Outdoor Unit: a generic term for any radio and can usually be exchanged for HBS or HSU.
PAWS	Protocol to Access White-Space: A protocol that allows geo-location TVWS databases to communicate with radios. PAWS specifies how a master device obtains a schedule of available spectrum at its location; it also takes into consideration the security necessary to ensure the accuracy, privacy, and confidentiality of the device’s location.
PNAM	Predecessor Neighbor Advertisement Message
PPPoE	Point-to-Point Protocol over Ethernet

Term	Description
PtMP	Point to Multi-Point: Link from an HBS to several HSUs
PtP	Point to Point
RADIUS	Remote Authentication Dial-In User Service
RSS	Radio Signal Strength
QAM	Quadrature Amplitude Modulation is the name of a family of digital modulation methods and a related family of analog modulation methods widely used in modern telecommunications to transmit information.
QoS	Quality of Service
SBM	Smart Bandwidth Management
Sector	A group of radios that consists of one HBS and several HSUs that communicate with the HBS.
SFF	Small Form-Factor
SHA1	Secure hash algorithm: An authentication type for SNMPv3 connections.
SLA	Service Level Agreement: The basic agreement between the service provider and its customer regarding certain aspects of the service provided. For example, what should be the data rate, throughput, jitter of the line, who should pay what fees, the mean time between failure (MTBF) of the equipment, and so on.
SSM	Synchronization Status Message: Provides traceability of synchronization signals and is used in the Synchronous Ethernet standard of communication.
SU	Subscriber Unit: A radio that can transmit and receive to one point. See also HSU.
Sync E or SyncE	Synchronous Ethernet: A standard of communication for ethernet that provides a synchronization signal to network elements that need such a signal.
TBS	Transportation Base Station: Similar to an HBS or BS, but used with high-speed transportation applications.
TCO	Total Cost of Ownership

Term	Description
TDWR	Terminal Doppler Weather Radar: A type of radar station used in the U.S. and other countries for weather reporting. If a radio unit is installed close enough to one of these stations, the FCC requires that certain actions must be taken on the part of the customer. Regulations in other countries varies.
TMU	Transportation Mobile Unit. Similar to an SU
TSN	Time Sensitive Network
TVWS	TV (television) White Space: A method by which certain unused frequencies in the television spectrum are put to use for BWA purposes.
Uplink	Data traffic from an HSU to an HBS, or Data traffic from an RT-B to an RT-A
VMU	Vehicular Mobile Unit
WI	Web Interface: Web-based applications that provide simple configuration capabilities for the radio units.
WISPA	Wireless Internet Service Provider Association. An organization that manages registration of wireless devices that operate close to TDWR facilities run by the FAA.
VRRP	Virtual Router Redundancy Protocol: A networking protocol that provides for automatic assignment of available IP routers to participating hosts.

Term	Description
DBS	Dynamic Bandwidth Selection: When activating a base station, or when changing its bandwidth, if you choose the maximum value available for the bandwidth, the link may dynamically switch between the maximum value and values as low as 20MHz to ensure the best throughput.
DFS	Dynamic Frequency Selection: Those products that have DFS enabled ensure that no radar signal is present in the selected frequency channel within the band being used. If a radar signal is detected, that frequency channel is evacuated and the product will not transmit on this channel.
DHCP	Dynamic Host Configuration Protocol: a protocol that automatically assigns IP addresses and other network configuration parameters.
Diversity	A technique by which the reliability of a radio link is increased using multiple transmitting and receiving antennas, transmitting the same signal on all antennas.
Downlink	Data traffic from an HBS to an HSU, or Data traffic from an RT-A to an RT-B
DUO	Dual Band base station
EIRP	Equivalent (or Effective) Isotropically Radiated Power: The power that an antenna must emit to produce the peak power density in the direction of maximum antenna gain. In our cases, this is usually: System Tx Power + Antenna Gain - Cable Loss.
FAA	Federal Aviation Administration. A U.S. federal office that manages aviation regulations throughout the United States.
Fixed (HSU)	A "fixed" HSU remains in one location, as contrasted with a nomadic or mobile HSU, which does not remain in one location.
GHSS	GPS Hub Site Synchronization
GRE	Generic Routing Encapsulation. A communication protocol used to establish a direct, point-to-point connection between network nodes. GRE lets two peers share data they wouldn't be able to share over the public network itself.
GRE Tunnel	A virtual point-to-point connection between two networks, using the GRE protocol to carry this out.
HBS	High capacity Base Station. Same as a BS

Term	Description
HMU	High capacity Mobility (subscriber) Unit. Similar to an HSU, but can be mobile.
HSC	Hub Sync Client: When using Hub Site Synchronization, one unit is a master (generates the sync pulses), and the other units are clients.
HSM	Hub Sync Master: When using Hub Site Synchronization, one unit is a master (generates the sync pulses), and the other units are clients.
HSU	High capacity Subscriber Unit. Same as an SU
IGMP	Internet Group Management Protocol
ISU	Integrated Synchronization Unit: a network device that provides a synchronization signal to underground HBSs.
LFF	Large Form-Factor
MD5	Message digest algorithm: an authentication type for SNMPv3 connections.
MDL	Multiple Device Learning
MIMO	Multiple In, Multiple Out. A technique by which the capacity of a radio link is increased using multiple transmitting and receiving antennas, transmitting a different signal on all antennas.
MIR	Maximum Information Rate
Mobile (HSU)	A “mobile” HSU can move from location to location and provide service while it moves or when it is stationary.
Nomadic (HSU)	A “nomadic” HSU move from location to location but can only provide service when it is stationary.
ODU	Outdoor Unit: a generic term for any radio, and can usually be exchanged for HBS or HSU.
PAWS	Protocol to Access White-Space; a protocol that allows geo-location TVWS databases to communicate with radios. PAWS specifies how a master device obtains a schedule of available spectrum at its location; it also takes into consideration the security necessary to ensure the accuracy, privacy, and confidentiality of the device’s location.
PNAM	Predecessor Neighbor Advertisement Message
PPPoE	Point-to-Point Protocol over Ethernet

Term	Description
PtMP	Point to Multi-Point: link from an HBS to several HSUs
PtP	Point to Point
RADIUS	Remote Authentication Dial-In User Service
RSS	Radio Signal Strength
QAM	Quadrature Amplitude Modulation is the name of a family of digital modulation methods and a related family of analog modulation methods widely used in modern telecommunications to transmit information.
QoS	Quality of Service
SBM	Smart Bandwidth Management
Sector	A group of radios that consists of one HBS and several HSUs that communicate with the HBS.
SFF	Small Form-Factor
SHA1	Secure hash algorithm: an authentication type for SNMPv3 connections.
SLA	Service Level Agreement - the basic agreement between the service provider and its customer regarding certain aspects of the service provided. For example, what should be the data rate, throughput, jitter of the line, who should pay what fees, the mean time between failure (MTBF) of the equipment, and so forth,
SSM	Synchronization Status Message: Provides traceability of synchronization signals, and is used in the Synchronous Ethernet standard of communication.
SU	Subscriber Unit: a radio that can transmit and receive to one point. See also HSU
Sync E or SyncE	Synchronous Ethernet: A standard of communication for ethernet that provides a synchronization signal to network elements that need such a signal.
TBS	Transportation Base Station. Similar to an HBS or BS, but used with high-speed transportation applications.
TCO	Total Cost of Ownership

Term	Description
TDWR	Terminal Doppler Weather Radar: a type of radar station used in the U.S. and other countries for weather reporting. If a radio unit is installed close enough to one of these stations, the FCC requires that certain actions must be taken on the part of the customer. Regulations in other countries varies.
TMU	Transportation Mobile Unit. Similar to an SU
TSN	Time Sensitive Network
TVWS	TV (television) White Space: a method by which certain unused frequencies in the television spectrum are put to use for BWA purposes.
Uplink	Data traffic from an HSU to an HBS, or Data traffic from an RT-B to an RT-A
VMU	Vehicular Mobile Unit
WI	Web Interface: web-based application that provides simple configuration capabilities for the radio units.
WISPA	Wireless Internet Service Provider Association. An organization that manages registration of wireless devices that operate close to TDWR facilities run by the FAA.
VRRP	Virtual Router Redundancy Protocol - a networking protocol that provides for automatic assignment of available IP routers to participating hosts.

Appendix B: SSH CLI

From 5.1.30, SSH protocol is supported by Alpha EMB and Alpha INT products. User can enable or disable this protocol.

The SSH login has the same user access privileges as the users who login the web UI (Admin, Operator, etc.). SSU support auto completion of the command by using the tab key.

A SSH terminal can be used to configure and monitor the devices. To start an SSH session to the IP address of the ODU, use an SSH terminal. The username for the SSH session is **cli** (no password). Once the session is open, CLI prompt "login as" will appear, enter your credentials (same as for WEB GUI, default is admin/netwireless).

Below is the list of SSH commands

Command	Explanation
help	Show available commands
quit	Disconnect
logout	Disconnect
exit	Exit from current mode
history	Show a list of previously run commands
configure terminal	Configure from the terminal. Enable access to configure terminal mode and set the login timeout in seconds. Press exit to exit the config terminal mode
display inventory	Display device inventory information
display management	Display device management information
display link all, reg, unreg, <serial>, <mac>, <name>	Display Wireless link information [param: all, reg, unreg, <serial>, <mac>, <name>]. You can select to see the information of all the connected SUs, registered SUs only, unregistered SUs only, or select a specific SU by writing its serial number, mac address or name. Examples: display link reg display link P17300I000K00160
display ethernet	Display the ethernet & SFP status and information
display ntp	Display network time information
display bands	Display Wireless bands information
set ip <ipaddr> <subnetMask> <gateway>	Set the management IP, Subnet Mask and Default Gateway
set trap <index:1-10> <ipaddr> <port:1-65535>	Enable to set trap destination index number (up to 10), IP address and port number
set syslog <server ip>	Set the set syslog server IP address, <0.0.0.0> is to disable the syslog server

set ntp <ntp-server> <offset-minutes>'	Set the NTP server of the offset time
set secID <sectorId>	Set the sector ID
set name <new name>	Set the name of the unit
set location <new location>	Set the location of the unit
set contact <new contact>	Set the contact information
set ethernet <port:LAN1> <mode:Auto,Auto_100,10H,10F,100H,100F>	Set the mode of the negotiation mode of Ethernet port
reboot	Reboot the unit
util ping [OPTIONS] IP (CTRL+C To Stop, 'util ping' for all options)	<p>Enable the ability to check the ping connectivity with a network device. The ping utility have a number of options for ping tests:</p> <p>ping [-aAbBdDfhLnOqrRUVV] [-c count] [-i interval] [-I interface] [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline] [-W timeout] [hop1 ...] destination</p> <p>Example 1: send 10 pings and stop util ping 20.0.0.150 '-c' 10</p> <p>Example 2: send pings in interval of 0.5 second (interval should be below 1) util ping 20.0.0.150 '-i' 0.5</p>
util traceroute [OPTIONS] IP [BYTES] (CTRL+C To Stop, 'util traceroute' for all options)	Enables performing traceroute tests
Link [param: <serial>, <mac>, <name>]	Not relevant to PtP

Appendix C: Revision History

Table B-1: Revision History

Cat.No/Release	Date	Description
Release 4.9.50 Rev 0.1	03.05.18	Initial release based on PtP 4.9.35
Release 4.9.50 Rev 0.2	14.05.18	External connection photographs updated
Release 4.9.70 Rev 0.3	01.04.19	Secure Sync method
Release 4.9.71 Rev 0.4	22.05.19	New product: RADWIN 2000 Alpha Integrated
Release 4.9.75 Rev 0.5	Aug, 2019	New product: RW 2000 ALPHA INT 3.x
Release 4.9.75 Rev 0.6	Oct, 2019	Removed iPerf and modified Sniffer (sniffing) comment
Release 4.9.75 Rev 0.7	Mar, 2020	Removed map view Updated user type descriptions L2 protocol transparent
Release 4.9.75 Rev 0.8	Aug, 2020	Regulatory: Changed 3.4-3.8 Alpha INT table to 2.4
Release 4.9.75 Rev 0.9	Feb, 2021	Grounding cable adjusted Regulatory warning added for external antenna connections, including TG.
Release 5.1.10 Rev 1.0	Jun, 2021	New product: Alpha Connectorized
Release 5.1.30 Rev 1.0	Feb, 2022	Release 5.1.30, WiFi for Alpha, user authentication
Release 5.1.42 Rev 11	Sep, 2022	Release 5.1.42: <ul style="list-style-type: none">• Enable / Disable management without IP• Add LQI (Quality Detection) to ALPHA• Management IP and Management VLAN at the same tab

User Handbook Notice

RADWIN 2000-Plus Family

This handbook contains information that is proprietary to RADWIN Ltd (RADWIN hereafter). No part of this publication may be reproduced in any form whatsoever without prior written approval by RADWIN.

Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this handbook and to the RADWIN products and any software components contained therein are proprietary products of RADWIN protected under international copyright law and shall be and remain solely with RADWIN.

The RADWIN name is a registered trademark of RADWIN. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark.

You shall not copy, reverse compile or reverse assemble all or any portion of the Configuration Guide or any other RADWIN documentation or products. You are prohibited from, and shall not, directly or indirectly, develop, market, distribute, license, or sell any product that supports substantially similar functionality based or derived in any way from RADWIN products. Your undertaking in this paragraph shall survive the termination of this Agreement.

This Agreement is effective upon your opening of a RADWIN product package and shall continue until terminated. RADWIN may terminate this Agreement upon the breach by you of any term thereof. Upon such termination by RADWIN, you agree to return to RADWIN any RADWIN products and documentation and all copies and portions thereof.

For further information contact RADWIN at one of the addresses under **Worldwide Contacts** below or contact your local distributor.

Disclaimer

The parameters quoted in this document must be specifically confirmed in writing before they become applicable to any particular order or contract. RADWIN reserves the right to make alterations or amendments to the detail specification at its discretion. The publication of information in this document does not imply freedom from patent or other rights of RADWIN, or others.

Trademarks

WinLink 1000, RADWIN 2000, RADWIN 5000, RADWIN 6000, RADWIN 600 and **FiberinMotion** are trademarks of RADWIN Ltd.

Windows 2000, XP Pro, Vista, Windows 7 and **Internet Explorer** are trademarks of Microsoft Inc.

Mozilla and **Firefox** are trademarks of the Mozilla Foundation.

Other product names are trademarks of their respective manufacturers.

End page

RADWIN

