AN-80i

Advanced Broadband Wireless Infrastructure Solutions

User Manual

Copyright Information

Disclaimer

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

Software Versions

This manual describes PTP operation using software release v4.0x, and PMP operation using software release v13.0x. This document may include references to features that are different or unavailable in previous software releases. Refer to the product Release Notes for information about specific software releases.

CONTENTS SUMMARY

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Safety & Service Notices

1.1 Service & Safety

1.1.1 Safety Warnings

1. Lightning and Grounding

> ⚠ **WARNING to Service Personnel**
>
> *The system __must__ be installed by a professional installer who is familiar with both data network issues and RF installations including grounding and lightning protection.*
>
> The system must be properly grounded to protect against power surges and accumulated static electricity. It is the user's responsibility to install this device in accordance with the local electrical codes: correct installation procedures for grounding of the modem, mast, lead-in wire and line protection, location of line protection, size of grounding conductors and connection requirements for grounding electrodes.

2. ⚠ PoE power adapter caution:

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

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

1.1.2 Warning Symbols

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

Electro-Magnetic Radiation

High Voltage

1.1.3 Lightning Protection

WARNING: The following notes are general recommendations for the system. The wireless equipment should be installed by a qualified professional installer who is knowledgeable of and follows local and national codes for electrical grounding and safety. Failure to meet safety requirements and/or use of non-standard practices and procedures could result in personal injury and damage to equipment.

All outdoor wireless equipment is susceptible to lightning damage from a direct hit or induced current from a near strike. A direct lightning strike may cause serious damage even if these guidelines are followed. Lightning protection and grounding practices in local and national electrical codes serve to minimize equipment damage, service outages, and serious injury. Reasons for lightning damage are summarized as:

a) Poorly grounded antenna sites that can conduct high lightning strike energy into equipment.

b) Lack of properly installed lightning protection equipment can cause equipment failures from lightning induced currents.

A lighting protection system provides a means by which the energy may enter earth without passing through and damaging parts of a structure. A lightning protection system does not prevent lightning from striking; it provides a means for preventing damage to equipment by providing a low resistance path for the discharge of energy to travel safely to ground. Improperly grounded connections are also a source of noise that can cause sensitive equipment to malfunction.

A good grounding system disperses most of the surge energy from a lightning strike away from the building and equipment. The remaining energy on the Ethernet cable shield and conductors can be directed safely to ground by installing a lightning arrestor in series with the cable.

If you have determined that it is appropriate to install lightning protection for your system, the following general industry practices are provided as a guideline only:

1. The AC wall outlet ground for the indoor POE adapter should be connected to the building grounding system.
2. Install a primary lightning arrestor (LP) device in series with the Ethernet cable at the point of entry to the building. The grounding wire should be connected to the same termination point used for the tower or mast.
3. Install a secondary lightning arrestor (LP) device in series with the Ethernet cable as close to the outdoors unit as practical. The grounding wire should be connected to the same termination point used for the tower or mast.
4. Provide direct grounding from the unit, the mounting bracket, the antenna, and the Ethernet cable surge protection to the same ground bus on the building. Use the grounding screws provided for terminating the ground wires.

1.1.4 Service & Warranty Information

1. Refer all repairs to qualified service personnel. Do not remove the covers or modify any part of this device, as this action will void the warranty.
2. Locate the serial numbers and record these on your registration card for future reference. Use the space below to affix serial number stickers. Also, record the MAC address identified on the unit product label.
3. Redline does not endorse or support the use of outdoor cable assemblies: i) not supplied by Redline, ii) third-party products that do not meet Redline's cable and connector assembly specifications, or iii) cables not installed and weatherproofed as specified in the Installation Guidelines manual (70-00073-01-XX). Refer to the Redline Limited Standard Warranty and RedCare service agreements.

1.2 Regulatory Notices

1.2.1 Deployment in the USA and Canada

FCC & IC Notices

1. The Model AN-80i and its antenna must be professionally installed.
2. ⚠WARNING -- FCC & IC RF Exposure Warnings

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

Table 1: FCC & IC RF Recommended Safe Separation Distances

Frequency (GHz)	Mode	Separation Distance
3.3 - 3.8	PTP / PMP	130 cm (52 in) or more
4.9 - 5.3	PTP / PMP	255 cm (101 in) or more
5.4	PTP / PMP	40 cm (16 in) or more
5.8	PMP	20 cm (8 in) or more
	PTP	310 cm (122 in) or more

   To ensure compliance, operation at closer than these distances is not recommended. The antenna used for this transmitter must not be collocated in conjunction with any other antenna or transmitter.
3. High power radars are allocated as primary users (meaning they have priority) of 5.250-5.350 MHz and 5.650-5.850 GHz and these radars could cause interference and/or damage to LE-LAN devices.
4. FCC Information to Users @ FCC 15.105:

   This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

   Where DFS is required by regional regulations, this function is permanently enabled at the factory and can not be disabled by the installer or end-user.
5. FCC Information to Users @ FCC 15.21:

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

Installation and Operation

USA

FCC Part 90 guidelines for deployment of AN-80i systems in the frequency band of 3.650-3.700 GHz for “restricted” CBP (Contention Based Protocol) in USA includes restrictions on the maximum EIRP.

To comply with the above guidelines, the following EIRP limitations are applied for deployment in this band:

i) Max EIRP of 25 Watts/25 MHz (equivalent to 1 Watt/1 MHz)

ii)Peak EIRP Power Density of 1 Watt in any 1 MHz slice of spectrum.

To ensure compliance with these restrictions, see the following important notices:

1. The AN-80i outdoor transceiver and antenna must be professionally installed.
2. The 3.650-3.700 GHz (USA) and 3.450-3.650 GHz (CAN) frequency ranges are licensed bands and operators must have a valid spectrum license to operate AN-80i equipment using these bands.
3. The AN-80i requires a Redline FCC-specific options key that is mandatory for operation within the USA. This options key enforces the FCC approved operating range of 3.650-3.675 GHz. Do not operate an AN-80i outdoor transceiver until you have confirmed the FCC-specific options key is loaded and active (operating range restricted to 3.650-3.675 GHz). When the FCC-specific options key is installed, the operator is not able to set an RF frequency that exceeds the allowed range of 3.650-3.675 GHz.
4. The AN-80i transmit power settings must not exceed values stated in the AN-80i User Manual.
5. Changes or modifications not expressly approved by Redline Communications could void the user’s authority to operate the equipment.

Canada

IC regulations governing operation in the 3.450-3.650 GHz band are subject to licensing, pursuant to subsection 4(1) of the Radiocommunication Act.

Power Settings

USA: FCC regulation part 90.1321 (governing operation in the 3.650-3.700 GHz band in the US) states that base station transmissions are limited to a maximum transmit power of 1 Watt/MHz (peak EIRP).

Canada: IC regulations governing operation in the 3.450-3.650 GHz band states that base station transmissions are limited to a m aximum transmit power of 1 Watt/MHz (peak EIRP).

Recommendations to UNII band Users

Redline, in complete cooperation with the FCC, strongly recommends the operators of this equipment in the UNII band to deploy following these guidelines:

1. Avoid operation in the TDWR band of 5600-5650 MHz.
2. Review the following table of Terminal Doppler Weather Radar (TDWR) system locations.
3. Operate at least 30 MHz away from the TDWR operation frequencies when installing devices within 22 miles (35 km) or in line-of-sight of a TDWR site.

Table 2: FCC: TDWR System Locations						
STATE	CITY	LONGITUDE	LATITUDE	FREQUENCY	TERRAIN ELEVATION (MSL) [ft]	ANTENNA HEIGHT [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
KS	WICHITA	W 097 26 13	N 37 30 26	5603 MHz	1270	80
KY	COVINGTON CINCINNATI	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 21 39	5608 MHz	807	113
NC	RALEIGH DURHAM	W 078 41 50	N 36 00 07	5647 MHz	400	113
NJ	WOODBRIDGE	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 INTERCONTL	W 095 34 01	N 30 03 54	5605 MHz	154	97
TX	PEARLAND	W 095 14 30	N 29 30 59	5645 MHz	36	80

Additional information:

http://spectrumbridge.com/udrs/home.aspx

http://www.wispa.org/?page_id=2341

1.2.2 UL Information

1. The suitability of the supplied Ethernet cable is subject to the approval of Authority Having Jurisdiction and must comply with the local electrical code.
2. The equipment must be properly grounded according with NEC and other local safety code and building code requirements
3. To meet the over-voltage safety requirements on the telecommunications cables, a minimum 26 AWG telecommunication line cord must be used.
4. "Pour être en conformance avec les exigences finies de sûreté de sur-tension sur les câbles de télécommunications un fil de télécommunication ayant un calibre minimum de 26 AWG doit être utilisé."
5. Reminder to all the BWA system installers: Attention to Section 820-40 of the NEC which provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as is practical.
6. AN-80i must be installed in compliance with relevant articles in National Electrical Code-NEC (and equivalent Canadian Code-CEC) including referenced articles 725, 800 and 810 in NEC.
7. RF coaxial cable connecting an antenna to the AN-80i must comply with the local electrical code.

1.2.3 WEEE Product Return Process

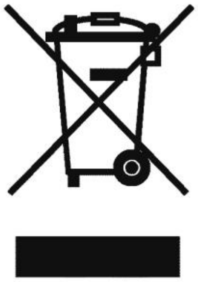


Figure 1: Notices - WEEE Logo

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

Chapter 2

2 System Overview

The Access Node 80i system is manufactured by Redline Communications -- a world leader in design and production of Broadband Fixed Wireless (BFW) systems.

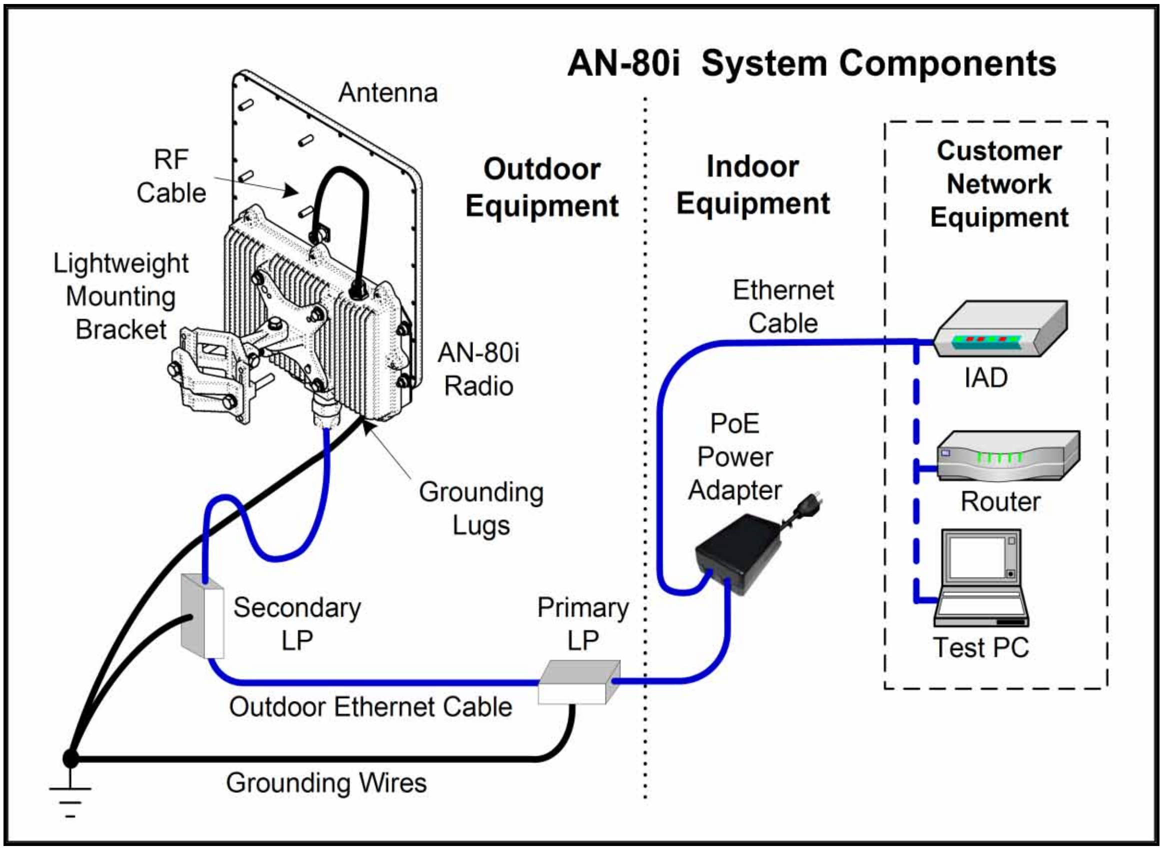


Fig. 2: Intro - AN-80i System Components

AN-80i is a high-performance, high-speed wireless Ethernet bridge for use in a commercial, industrial, business, or government environment. The system can operate with a 3.3 - 3.8 GHz, 5.4 GHz, 4.9 - 5.3 GHz, or 5.8 GHz radio (factory installed) using a time division duplexing (TDD) RF transceiver to transmit and receive on the same channel. Main features include advanced technologies to address inter-cell interference, enhanced security features through over-the-air encryption schemes, and Automatic Transmitter Power Control (ATPC) to maintain optimum performance.

The outdoor unit can be used with a wide selection of external antennas. When equipped with a narrow beam antenna, the AN-80i supports long-range operations of over 50 miles (80 km) in clear line of sight (LOS) conditions for PTP applications. The AN-80i outdoor unit is housed in a weatherproof aluminum alloy case. An indoor PoE power adapter provides operational power for the AN-80i and connection to the Ethernet network.

One AN-80i is software configurable as a PTP Master or PMP Sector Controller and controls the wireless link. This function is transparent to all Ethernet operations. The Master/Sector Controller uses a scheduled request/grant mechanism to arbitrate bandwidth requests from the remote unit (PTP Slave / PMP Subscriber) to provide non contention-based traffic with predictable transmission characteristics.

2.1 Ethernet Port

The Ethernet port is a female RJ-45 connector. The AN-80i receives DC power and exchanges data with the indoor network through the Ethernet port. The AN-80i Ethernet port connects to the PoE Adapter using a weatherproof CAT-5E Ethernet cable. The maximum total length of the Ethernet cable is 91.5 m (300 ft). For example, 90 m (295 ft) from the AN-80i to the PoE and 1.5 m (5 ft) from the PoE to the network equipment.

2.2 RF Port

The RF port is a female N-type connector. The RF port is used to send and receive RF signals to and from the antenna. A short coaxial cable is provided to connect the transceiver to an external antenna.

2.3 Mounting Brackets

There are three mounting brackets available for the AN-80i. The lightweight (two-point) mounting bracket (80i-LW-MNT) provides convenient mounting of one foot flat panel antennas. The heavy-duty (four-point) mounting bracket (80i-HD-MNT) is available for mounting two-foot flat panel and small parabolic antennas. A simple stand-alone mounting bracket (80i-SA-MNT) is available that is allows the use of hose clamps to mount only the AN-80i unit (for example, a large parabolic antenna must have separate mounting hardware).

2.4 Grounding Connection

A ground-lug is provided on the AN-80i chassis. Use this connection to terminate a grounding wire.

2.5 Indoor PoE Power Adapter

The PoE power adapter provides power to the AN-80i and connectivity to the local Ethernet network.

2.5.1 AC Power Adapter

The AC power adapter input is auto-sensing 110/220/240 VAC 50/60 Hz.

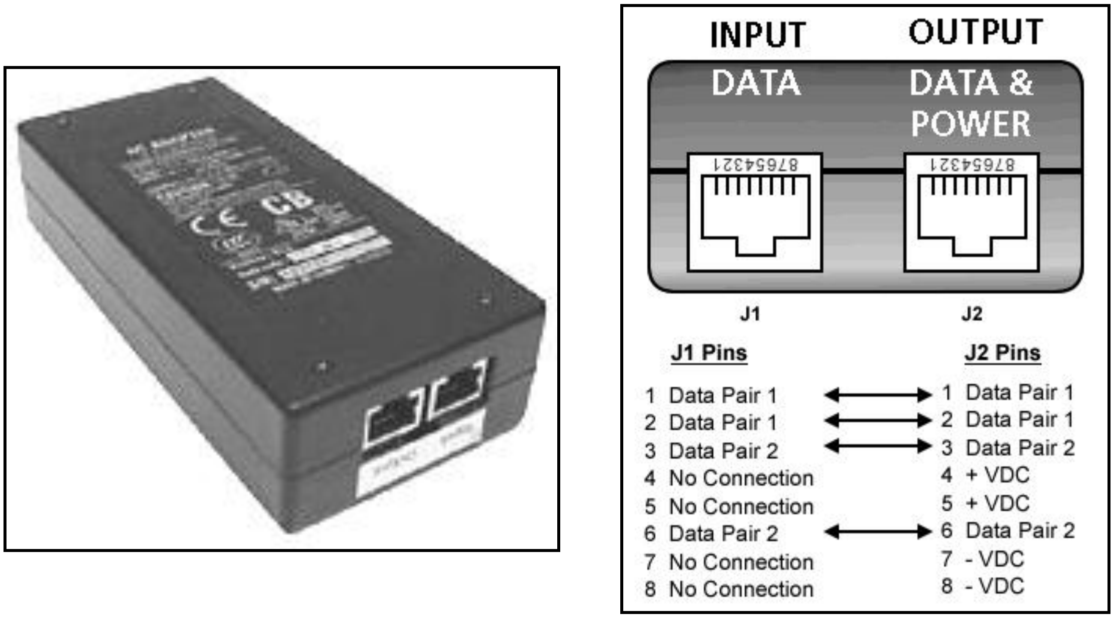
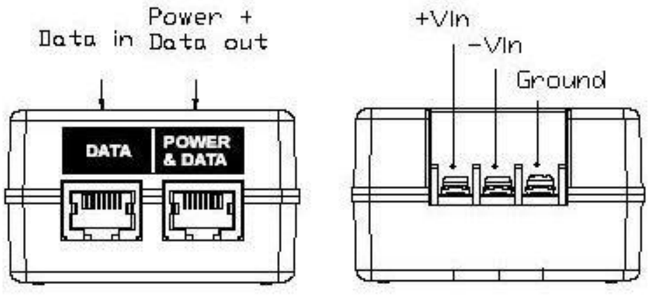


Fig. 3: Intro - Indoor Power-over-Ethernet (PoE) Module - AC Model

2.5.2 DC Power Adapter

The DC power adapter input is auto-sensing 18 - 60 VDC.



PIN CONNECTION		
Pin	Data in	Data out
1.	TX(+)	TX(+)
2.	TX(-)	TX(-)
3.	RX(+)	RX(+)
4.	NC	DC+
5.	NC	DC+
6.	RX(-)	RX(-)
7.	NC	DC
8.	NC	DC

Fig. 4: Intro - Indoor Power-over-Ethernet (PoE) Module - DC Model

Warning to Service Personnel: 48 VDC

Customer equipment including personal computers, routers, etc., must be connected only to the INPUT (DATA) port on the PoE unit.

Only the outdoors Ethernet interface cable connecting to the AN-80i can be safely connected to the OUTPUT (DATA & POWER) connector. Connecting customer premises Ethernet equipment directly to the OUTPUT (DATA & POWER) connector on the Power-over-Ethernet power adapter may damage customer equipment.

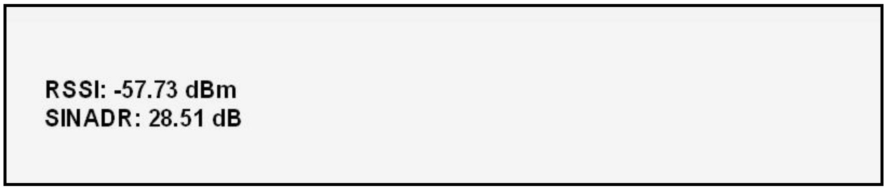
2.6 Antenna Alignment

The AN-80i includes both an audible alignment tool and a web-based alignment tool to assist in pointing the antenna.

2.6.1 Web Page Alignment

The web page can be accessed directly from a link on the System Status screen (Antenna Alignment).

The most reliable method for obtaining optimum performance from a wireless link is by fine alignment of the antenna to the position providing the highest RSSI (Received Signal Strength Indication) and best SINADR (Signal to Noise And Distortion Ratio). The web page assists alignment by providing continuous 1-second updates of RSSI and SINADR values.



```
RSSI: -57.73 dBm
SINADR: 28.51 dB
```

Fig. 5: Intro - Web Antenna Alignment Tool

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

http:// [AN-80i IP Address] / usr / aa.html

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

Note: SINADR is available only on PTP systems.

2.6.2 Audible Alignment

When enabled, the audible alignment signal will sound infrequently when a low signal is detected, and more often as the signal strength increases. The audible antenna alignment tool provides only rough adjustment for the subscriber antennas. It is recommended to monitor the RSSI measurements to achieve maximum signal strength when performing fine adjustments to the subscriber antenna. See the AN-80i Installation Guidelines for detailed instructions.

To enable or disable the audible tool through the user interface:

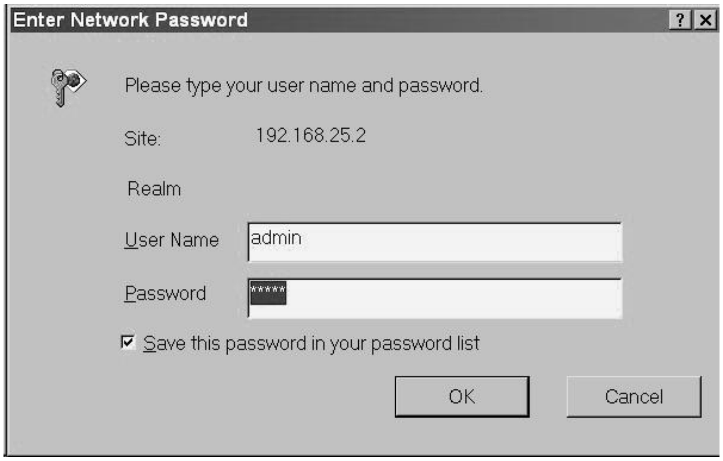
Web: See *Antenna Alignment Buzzer Enable* in Web System Configuration screen.

Telnet: See '*buzzer*' in CLI 'set' commands.

2.7 Managing the AN-80i

2.7.1 Web Browser (HTTP)

On the PC, open a Web browser (Internet Explorer 6 or higher recommended) and enter the unit IP address. For new systems, the default IP address is 192.168.25.2. The following login dialog should be displayed:



Enter Network Password

Please type your user name and password.

Site: 192.168.25.2

Realm

User Name: admin

Password: *****

☑ Save this password in your password list

Fig. 6: Intro - Web (Browser) Login to the AN-80i

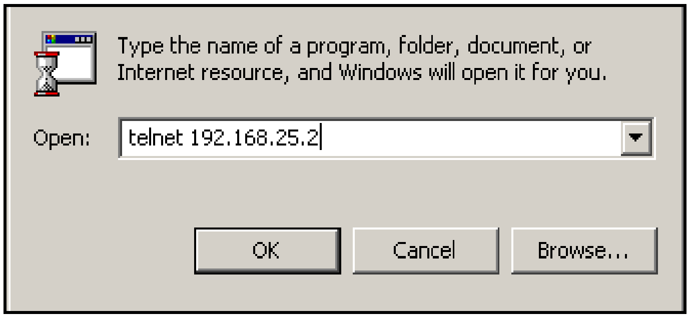
If the IP address, username and/or password have been modified since installation, contact the network administrator to determine the current settings. If the IP address, or the user name and password cannot be determined. See section 7.1: Long Reset (Recover from Lost IP or Password on page 105.

2.7.2 Telnet (CLI)

The AN-80i supports two concurrent Telnet sessions. One session has full capabilities and the second session is read-only (e.g., monitor or show parameter settings).

To connect to the AN-80i CLI management, open a Telnet session to the IP address of the AN-80i. On a Windows™ PC, open the Run command and type 'telnet' followed by the IP address of the AN-80i. When the command prompt screen appears, login to the AN-80i. The unit may now be configured using the Commands.

The AN-80i supports two concurrent Telnet sessions. One session has full capabilities and the second session is read-only (e.g., monitor or show parameter settings).



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.25.2

Fig. 7: Intro - Open a Telnet Session to the AN-80i

2.7.3 SNMP

The AN-80i can be managed using SNMP (Simple Network Management Protocol) v2c or v3. The system MIBS information is provided separately. Contact your Redline sales representative for information about Redline device management products.

3 PTP Operation

The Web Interface provides all required settings and statistics necessary to configure and monitor the operation of the AN-80i using a standard web browser. An operator can access and control the AN-80i remotely from any geographical location with HTTP connectivity to that unit.

3.1 PTP System Menu

Following a successful login, the General Information screen is displayed. On the left is a menu of all available screens. Point and click on the blue text of the main menu to display that screen.

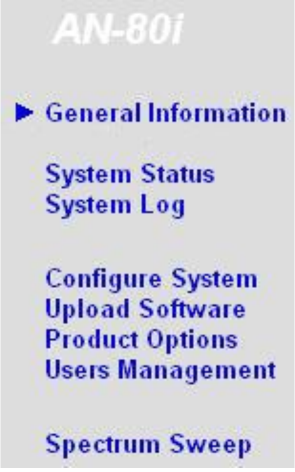


Fig. 8: Web - PTP System Menu

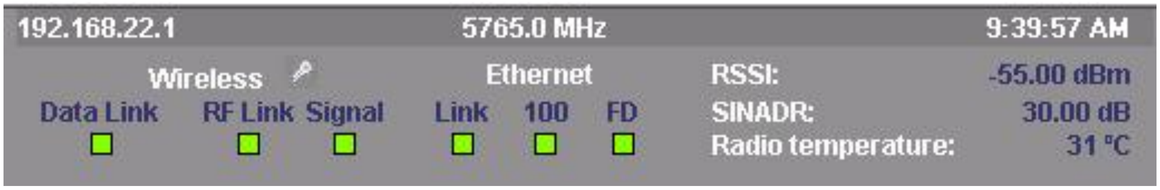
The administrator (admin) has unrestricted access to all screens. All other users have viewing access only. See 5.2.5: User and Admin Account Permissions on page 68 for details.

3.2 PTP System Information Screen

Click **General Information** to view the system overview screen (read-only). See the **System Configuration** screen for information about changing these settings.

3.2.1 Dashboard

The dashboard at the top of the **General Information** screen displays a summary of important operational information and status indicators.



192.168.22.1 5765.0 MHz 9:39:57 AM

Wireless Ethernet RSSI: -55.00 dBm

Data Link 🟩 RF Link 🟩 Signal 🟩 Link 🟩 100 🟩 FD 🟩

SINADR: 30.00 dB

Radio temperature: 31 °C

Fig. 9: Web - PTP Dashboard Display

General

IP Address: IP address setting of this unit.

Wireless Frequency: RF channel frequency.

Time: Displays time obtained from operator's Web browser.

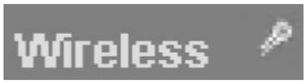
RSSI: Received signal strength indicator measured since the last screen refresh.

SINADR: Average signal to interference, noise, and distortion ratio.

Radio Temperature: Internal temperature of the radio.

Wireless Led Indicators

When data sent over the wireless interface is being encrypted, a key symbol is displayed adjacent to the 'Wireless' title in the dashboard. See the Wireless Security Configuration settings on the **System Configuration** screen.



Wireless

Fig. 10: Web - PTP - Dashboard Display - Wireless Key Symbol

Wireless Data Link LED

This indication is valid only when the RF Link LED is on solid green.

Off: Data can not be transmitted across the wireless interface (e.g., incorrect security settings).

On: Data can be transmitted across the wireless interface.

Wireless RF Link LED

Off: Wireless RF link is not established.

On: Sector controller: Wireless RF link is operational to one or more subscribers.
Subscriber: Wireless RF link to the sector controller is operational.

Wireless Signal LED

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

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

Blink: Wireless link is operating below the requested UBR.

Ethernet LED Indicators

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

Link LED

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

On: Ethernet connection is detected and Ethernet traffic is not detected.

Blink: Ethernet connection is detected and Ethernet traffic is detected.

100 LED

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

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

FD LED

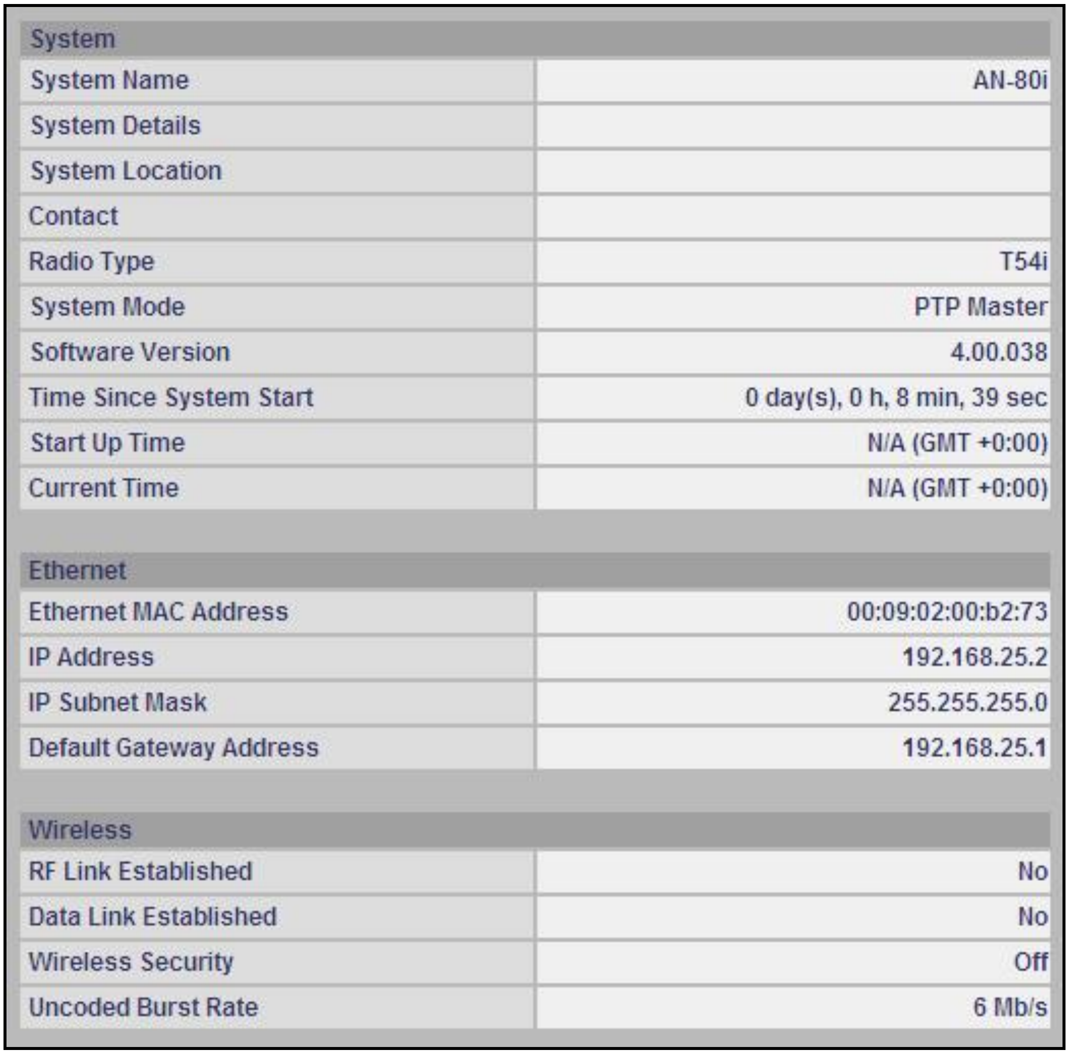
Off: Ethernet connection is operating in half-duplex mode.

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

Blink: Collisions are detected on the Ethernet port.

3.2.2 General Information Screen

The General Information screen provides additional detail about the unit.



System	
System Name	AN-80i
System Details	
System Location	
Contact	
Radio Type	T54i
System Mode	PTP Master
Software Version	4.00.038
Time Since System Start	0 day(s), 0 h, 8 min, 39 sec
Start Up Time	N/A (GMT +0:00)
Current Time	N/A (GMT +0:00)
Ethernet	
Ethernet MAC Address	00:09:02:00:b2:73
IP Address	192.168.25.2
IP Subnet Mask	255.255.255.0
Default Gateway Address	192.168.25.1
Wireless	
RF Link Established	No
Data Link Established	No
Wireless Security	Off
Uncoded Burst Rate	6 Mb/s

Fig. 11: Web - PTP General Information Screen

General

System Name: User-assigned name for this AN-80i.

System Details: User-assigned system details information.

System Location: User-assigned system location information.

Contact: User-assigned contact information.

Radio Type: Displays the factory installed radio type. Refer to section 8.1 System Specifications.

System Mode: Select the mode of operation for this unit.

> **PTP Master**: This unit begins transmitting automatically, sends poll messages to locate the remote AN-80i Slave, and negotiates operating settings for the link. Only one system in a wireless link must be set for PTP Master mode.
>
> **PTP Slave**: This unit passively monitors the selected channel(s) until polled by the PTP Master.

Software Version: Displays the software version in use.

Time Since System Start: Time since the system was last reset/powered-on.

Start Up Time: Time and date the system was last reset/powered-on.

Current Time: Current time setting on this AN-80i.

Ethernet

Ethernet MAC Address: Hardware (MAC) address of this AN-80i. This address is also recorded on the chassis label.

IP Address: IP address.

IP Subnet Mask: IP subnet mask.

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

Wireless

RF Link Established: Status of the wireless link.

> **Yes** - RF link successfully established with remote-end unit.
>
> **No** - RF link not established with remote-end unit.

Data Link Established: Status of the data link to the remote unit.

> **Yes** - Data link successfully established with remote-end unit.
>
> **No** - Data link not established with remote-end unit.

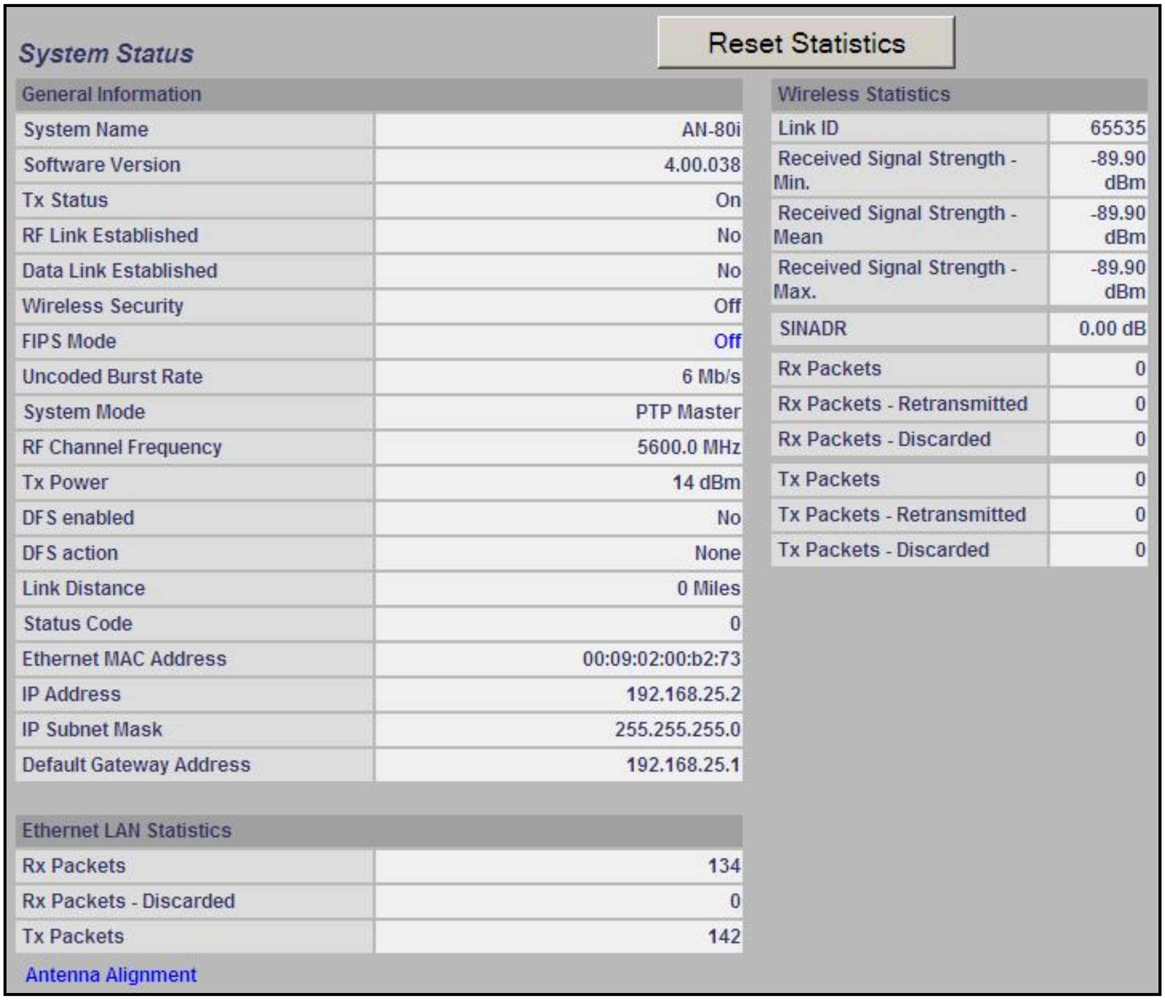
Wireless Security: Status of the wireless security selection.

> **Off** - No wireless security. Data is not encrypted.
>
> **On** - Data sent over the wireless interface is encrypted.

Uncoded Burst Rate: The current uncoded burst rate for the link (Mb/s).

3.3 PTP System Status Screen

Click **System Status** in the main menu to view all AN-80i interface statistics.



General Information	
System Name	AN-80i
Software Version	4.00.038
Tx Status	On
RF Link Established	No
Data Link Established	No
Wireless Security	Off
FIPS Mode	Off
Uncoded Burst Rate	6 Mb/s
System Mode	PTP Master
RF Channel Frequency	5600.0 MHz
Tx Power	14 dBm
DFS enabled	No
DFS action	None
Link Distance	0 Miles
Status Code	0
Ethernet MAC Address	00:09:02:00:b2:73
IP Address	192.168.25.2
IP Subnet Mask	255.255.255.0
Default Gateway Address	192.168.25.1

Ethernet LAN Statistics	
Rx Packets	134
Rx Packets - Discarded	0
Tx Packets	142

Wireless Statistics	
Link ID	65535
Received Signal Strength - Min.	-89.90 dBm
Received Signal Strength - Mean	-89.90 dBm
Received Signal Strength - Max.	-89.90 dBm
SINADR	0.00 dB
Rx Packets	0
Rx Packets - Retransmitted	0
Rx Packets - Discarded	0
Tx Packets	0
Tx Packets - Retransmitted	0
Tx Packets - Discarded	0

Fig. 12: Web - PTP System Status Screen

3.3.1 General information

System Name: User-assigned system name.

Software Version: Displays the software version in use.

Tx Status: State of the wireless interface (FIPS mode only). The unit performs continuous self-tests for the RNG, DSA generator, and signature modules. If any of these tests fails, the transmitter is disabled.

Off - Wireless security has disabled the transmitter.

On - Wireless security has enabled the transmitter.

RF Link Established: State of the wireless link connection.

Yes - Data link has been successfully established with the remote-end unit.

No - Data link has not been established with the remote-end unit. This may be caused by mismatched security settings (e.g., link name, Peer MAC, encryption settings, etc.).

Data Link Established: State of the data link connection.

Yes - RF link has been successfully established with the remote-end unit.

No - RF link has not been established with the remote-end unit.

Wireless Security: Status of the wireless security selection.

Off - No wireless security.

On - Data sent over the wireless interface is encrypted.

FIPS Mode: State of the FIPS security option. Click the status (**Off/On**) link to view the status of all FIPS components. Refer to page 118 for a complete description of this feature.

Off - FIPS mode is not active.

On - FIPS mode is active and monitoring all security issues.

Uncoded Burst Rate: The current uncoded burst rate (UBR) for the wireless link.

System Mode: Choose if this unit will operate as master or slave on the wireless link.

PTP Master: This unit transmits automatically; sending poll messages to the remote unit and negotiating the UBR (modulation and coding) for the wireless link.

PTP Slave: This unit waits passively until polled by the PTP Master.

RF Channel Frequency: RF channel frequency in use.

Tx Power: The current transmit power level. If ATPC is enabled, this value may be different from the Tx Power setting in the **System Configuration** screen.

DFS Enabled: Indicate the state of the DFS function. See 3.4.2 Wireless Configuration for a complete description of the DFS feature.

Disabled: The DFS function is disabled.

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

DFS Action: The avoidance action taken when radar signals are detected. See 3.4.2 Wireless Configuration for a complete description of the DFS feature. All DFS actions are recorded in the event log.

None: The DFS feature is disabled.

Tx Off: Transmitter was switched off for 30 minutes.

Chg Freq: Transmitter was switched to a different frequency.

Link Distance: Distance between wireless systems. This may be the calculated or user-assigned distance (**System Configuration** screen).

Status Code: Code indicating the status of the AN-80i system. Status codes are specific to PMP and PTP operation. Code '0' indicates normal operation. Refer to section 6: Diagnostics and Troubleshooting.

Ethernet MAC Address: System hardware address (also printed on product label).

IP Address: User-assigned IP address of the AN-80i.

IP Subnet Mask: User-assigned IP subnet mask.

Default Gateway Address: User-assigned IP for the default router or gateway.

3.3.2 Ethernet LAN Statistics

Rx Packets: Total packets received on the Ethernet port.

Rx Packets: **Discarded**: Total valid Ethernet frames (received on the Ethernet port) that are discarded due to lack of buffer space.

Tx Packets: Number of packets transmitted on the Ethernet port (including Ethernet frames and error correction bytes).

3.3.3 Wireless Statistics

Link ID: A new session identifier each time the wireless link is established.

Received Signal Strength: **Min**: Minimum measured RSSI value.

Received Signal Strength: **Mean**: Average measured RSSI value.

Received Signal Strength: **Max**: Maximum measured RSSI value.

SINADR: Ave. signal to interference, noise, and distortion ratio (updated each refresh).

Rx Packets: Total number of packets received over the wireless interface.

Rx Packets: **Retransmitted** Number of packets received over the wireless interface retransmitted by the remote-end system (ARQ retransmit of unacknowledged packets).

Rx Packets - Discarded: Number of received packets discarded due to errors.

Tx Packets: Number of packets transmitted over the wireless interface.

Tx Packets - Retransmitted: Number of packets re-transmitted over the wireless interface (ARQ mechanism re-transmitting unacknowledged packets).

Tx Packets: **Discarded**: Total number of packets transmitted over the wireless interface that where no acknowledge was received (discarded by remote-end due to errors).

3.3.4 Statistics Controls

Reset Statistics: Click to zero all Wireless and Ethernet LAN statistics.

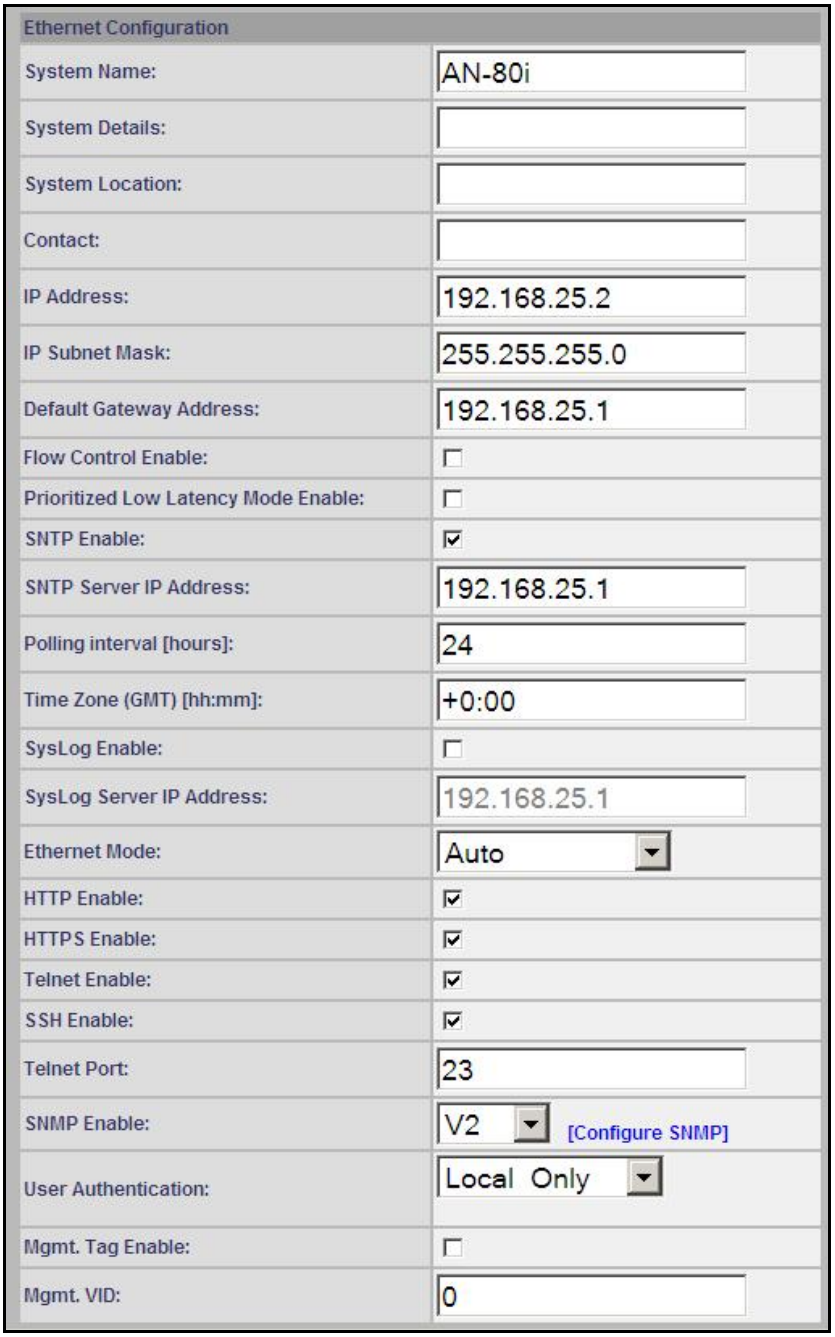
Antenna Alignment: Click to the blue text to launch the web alignment tool. See section 2.6.1: Web Page Alignment on page 20.

3.4 PTP System Configuration Screen

Click **Configure System** in the main menu to view and adjust configuration settings for general system identification, Ethernet, and the wireless interface.

3.4.1 Ethernet Configuration

Use settings on this section of the screen to configure the AN-80i Ethernet interface.



Ethernet Configuration	
System Name:	AN-80i
System Details:	
System Location:	
Contact:	
IP Address:	192.168.25.2
IP Subnet Mask:	255.255.255.0
Default Gateway Address:	192.168.25.1
Flow Control Enable:	□
Prioritized Low Latency Mode Enable:	□
SNTP Enable:	☑
SNTP Server IP Address:	192.168.25.1
Polling interval [hours]:	24
Time Zone (GMT) [hh:mm]:	+0:00
SysLog Enable:	□
SysLog Server IP Address:	192.168.25.1
Ethernet Mode:	Auto
HTTP Enable:	☑
HTTPS Enable:	☑
Telnet Enable:	☑
SSH Enable:	☑
Telnet Port:	23
SNMP Enable:	V2 [Configure SNMP]
User Authentication:	Local Only
Mgmt. Tag Enable:	□
Mgmt. VID:	0

Fig. 13: Web - PTP System and Ethernet Configuration Screen

System Name: Enter the name for this AN-80i. The name may be up to thirty (30) alphanumeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

System Details: Enter additional descriptive details about this AN-80i. The system details may be up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

System Location: Enter additional descriptive details about this AN-80i. The system location information may be up to thirty (30) alphanumeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

Contact: Enter additional descriptive details about this AN-80i. The contact information may be up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

IP Address: Enter the IP address for this AN-80i. The IP address is routable both through the Ethernet port and over the wireless interface.

IP Subnet Mask: Enter the IP subnet mask.

Default Gateway Address: Enter the IP address of the default gateway or router on the Ethernet segment connected to the AN-80i Ethernet port.

Flow Control Enable: (PTP only) Check this box ☑ to enable flow control functions (802.3x) on the AN-80i Ethernet port. Enabling this feature allows the AN-80i to request Ethernet devices to pause transmissions during busy periods.

Prioritized Low Latency Mode Enable: (PTP only) Check this box ☑ to enable priority handling of 802.1p tagged traffic. When enabled, this ensures prioritized traffic is transmitted with the lowest achievable latency, even under conditions of high IP data traffic loading.

Table 3: **PTP - 802.1p Priority Settings**

Priority	Setting
Highest	6, 7
	4, 5
	0, 3, no tag
Lowest	1, 2

SNTP Enable: Check this box ☑ to enable the SNTP protocol support. This feature allows AN-80i systems to time-stamp log messages using a network time server. When enabled, you must enter the network address of the SNTP server in the SNTP Server IP Address field.

SNTP Server IP Address: Enter the network address of the SNTP server. Valid only when the SNTP Enable field is checked.

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

Time Zone (GMT) [hh:mm]: Enter the hours offset from GMT for this time zone. Valid only when the SNTP Enable field is checked.

Syslog Enable: Check this box ☑ to enable the Syslog protocol support. This feature allows AN-80i log messages to be saved in a central repository. When enabled, you must enter the network address of the Syslog server in the Syslog Server IP Address field.

Syslog Server IP Address: Enter the network address of the Syslog server. Valid only when the Syslog Enable field is checked.

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

Auto - Automatically negotiate the connection speed and duplex.

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

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

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

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

> ***Important**: The auto-negotiate feature does not detect the speed and duplex of manually set Ethernet equipment. The auto-negotiate function works correctly only when both communicating Ethernet devices are configured for auto-negotiate. Duplex mismatches may result in an unexpected loss of communications.*
>
> *It is recommended to manually configure Ethernet devices to 100Base-T / full duplex.*

HTTP Enable: Check this box ☑ to enable the HTTP (Web) interface. If the option is deselected, only Commands will be available.

HTTPS Enable: Check this box to enable HTTPS operation (secure/encrypted Web session). Refer to page 118 for a complete description of this feature.

Telnet Enable: Check this box ☑ to enable a Telnet access (CLI) to the AN-80i.

SSH Enable: Check this box to enable SSH operation (secure/encrypted CLI). Refer to page 118 for a complete description of this feature.

Telnet Port: Enter Telnet port address (default is 23).

SNMP Enable: Select the version of Simple Network Management Protocol (SNMP).

none: SNMP is disabled.

v2: Supports SNMP v1 and v2c commands.

v3: Supports SNMP v3 exclusively (v1 and v2c commands not accepted).

When SNMP is selected, click on the blue text **Configure SNMP** adjacent to the check box to display the SNMP Configuration screen. See section 5.3.2 SNMP Configuration Screen on page 70.

User Authentication: The AN-80i supports secure centralized authentication management using a RADIUS server. At least one method is always enabled, and both services may be enabled to operate together.

The AN-80i can be configured for the following authentication modes:

Local Only: Use only AN-80i local authentication functions (default). Local authentication uses user names and password information managed by the AN-80i. This method is supported by all versions of AN-80i software.

RADIUS Only: Use only RADIUS for user authentication.

An access request to the AN-80i is forwarded to the RADIUS server. At least one RADIUS server must be enabled in this mode. The configuration can be done through the CLI or HTTP. The following parameters must be specified for each RADIUS server (primary server and optional backup server):

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

When RADIUS is selected, click on the blue text **Configure RADIUS** adjacent to the check box to display the RADIUS Configuration screen. See section 5.3.1: RADIUS Setup Screen on page 69.

Note: When user authentication is set to RADIUS Only or Local + RADIUS, the authorization data is retrieved from the RADIUS server at ten minute intervals. For example, if a user's authorization is changed on the RADIUS server, it may be up to ten minutes (max.) before the AN-80i is updated.

Mgmt. Tag Enable: Check ☑ this box to enable VLAN tagged management traffic.

Disabled (□): AN-80i unit can be managed using untagged traffic.

Enabled (☑): AN-80i unit can be managed only using VLAN traffic tagged with the value specified in the Mgmt. VID field.

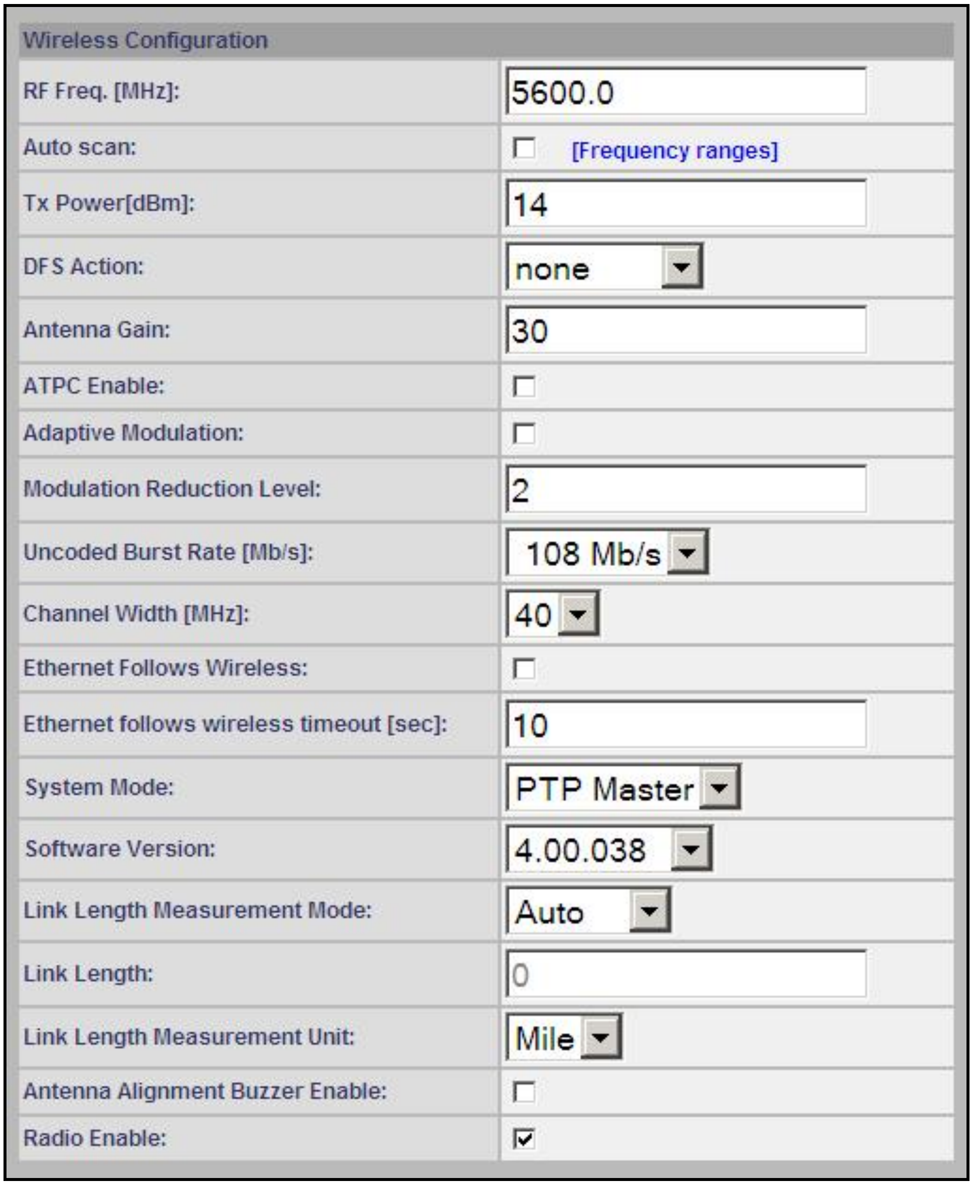
If the Mgmt. Tag feature is to be used, it is strongly recommended to create and test the VLAN connectivity before activating the Mgmt Tag Enable function. Otherwise, management function may become unavailable and the unit may require a long reset to recover control (refer to page 105). Set appropriate QoS and priority values to ensure management traffic has adequate priority and bandwidth during system operation.

> ***Important***: On all PMP systems, over-the-air management is possible only after creating a Group for device management and adding a Connection for each subscriber. For installation and setup, it is recommended to use Pass Through settings for this group and each member connection.

Mgmt. VID: Enter the VLAN ID. When Mgmt. Tag Enable is selected, the system recognizes only management commands with this VLAN ID. Refer to the Mgmt. Tag Enable field for more information.

3.4.2 Wireless Configuration

Use settings on this section of the screen to configure the AN-80i wireless interface.



Wireless Configuration	
RF Freq. [MHz]:	5600.0
Auto scan:	□ [Frequency ranges]
Tx Power[dBm]:	14
DFS Action:	none
Antenna Gain:	30
ATPC Enable:	□
Adaptive Modulation:	□
Modulation Reduction Level:	2
Uncoded Burst Rate [Mb/s]:	108 Mb/s
Channel Width [MHz]:	40
Ethernet Follows Wireless:	□
Ethernet follows wireless timeout [sec]:	10
System Mode:	PTP Master
Software Version:	4.00.038
Link Length Measurement Mode:	Auto
Link Length:	0
Link Length Measurement Unit:	Mile
Antenna Alignment Buzzer Enable:	□
Radio Enable:	☑

Fig. 14: Web - PTP Wireless Configuration Screen

RF Freq. [MHz]: Enter the center frequency for the RF channel. This setting must be identical for both AN-80i systems operating as a wireless link. The options key controls channel availability. See Table 73: Spec. - Regional Identification Codes on page 144 for available channels. Use the Autoscan feature to enable use of multiple channels.

When the Auto Scan field is not checked, the PTP Slave will only register with a PTP Master operating at the frequency specified in the RF Freq. [MHz] field.

> ***Important**: To minimize interference, the channel frequencies for AN-80i links operating in close proximity should be separated by a minimum of the channel size in use (to avoid overlapping bands).*

Auto scan: Check this box ☑ to enable the PTP Slave to automatically scan available channels to locate and register with an AN-80i PTP Master.

Click the blue text **[Frequency Ranges]** adjacent to the check box to display the Frequency Management screen (see Frequency Range on page 75).

PTP Master: The PTP Master can be programmed with a master list of frequency ranges. When a PTP Slave registers with the PTP Master, the programmed frequency ranges are downloaded by the PTP Slave (displayed as Remote Frequency Ranges on the PTP Slave). The downloaded range settings are used exclusively by the PTP Slave during autoscan and remain in effect until the PTP Slave is rebooted (setting are discarded at reboot.

PTP Slave: When no frequency ranges are entered (default), the PTP Slave scans all available frequency ranges for that region (refer to 9.5: Regional Codes on page 144). When one or more frequency ranges have been entered (or downloaded from the PTP Master), only these frequency ranges are scanned. If all entered frequency ranges are scanned (x3) without registering with a P TP Master, the PTP Slave defaults to scanning all enabled frequencies.

Tx Power [dBm]: Enter the transmit power level (dBm). This setting is for the transceiver output only. The actual EIRP depends on the gain of the connected antenna. See the following tables to determine the maximum transmit power level available at each modulation setting. When ATPC is enabled, the Tx power is automatically adjusted to achieve optimum performance. When DFS is enabled, the subscriber Tx power may be automatically adjusted (regardless of ATPC setting) to avoid false DFS triggering.

Table 4: PTP & PMP - Maximum TX Power Settings (dBm)

Modulation	**BPSK**		**QPSK**		**16 QAM**		**64 QAM**	
Code Rate	**1/2**	**3/4**	**1/2**	**3/4**	**1/2**	**3/4**	**2/3**	**3/4**
Max. Tx Power: **T35 Radio**	25	25	25	25	25	23	22	21
Max. Tx Power: T49, T54, and T58 Radios	25	25	23	22	21	20	18	17

Notes:

1.Tx power settings apply to PTP v3.00 and higher and v11.00 and higher.

2.See Table 5: PTP & PMP - Modulation/Coding for UBR on page 38 for modulation/coding.

11.

***Important**: EIRP Levels: Where required by local regulations, the maximum operational power per channel for a specific antenna must not exceed the maximum allowable EIRP levels. See the FCC and CE notices in this manual. The RF output power settings must be professionally programmed by the manufacturer or a trained professional installer.*

DFS Action: Select the mode of operation for DFS.

The system set to PTP Master monitors for interference from radar devices and other equipment using the same channel frequency. When interference is detected, the system automatically takes the action selected using the drop-down menu.

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

None: The DFS function is disabled.

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

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

Antenna Gain: Enter the manufacturers specified gain (dBm) for the system antenna.

It is important to enter the correct value. If this value is set higher than the true gain, the sensitivity will be too low and the AN-80i will <u>not</u> be operating in compliance with the UK/ETSI standard. If this value is set lower than the true gain, the AN-80i is more sensitive to interference and may experience false triggers.

ATPC Enable: (PTP only) Check this box ☑ to enable the AN-80i to monitor the received signal and request that the remote system adjustment its transmit level for optimum performance. The ATPC feature must be enabled on both units.

***Important**: When ATPC is enabled, use adaptive modulation for best results.*

Adaptive Modulation: Check this box ☑ to enable the AN-80i adaptive modulation.

PTP: When enabled, the modulation/coding is automatically set to achieve the highest UBR where packet error rates are lower than 1x10e-6. Higher packet error rates cause the system to reduce modulation/code rate to maintain the wireless link quality (e.g., change from 16 QAM 3/4 to 16 QAM 1/2). When adaptive modulation is disabled, the AN-80i will operate only at the modulation/coding corresponding to the UBR value in the Uncoded Burst Rate field (refer to Table 5: PTP & PMP - Modulation/Coding for UBR). The maximum UBR is limited to the Uncoded Burst Rate setting (v3.00/v11.00 or higher).

PMP: See section 4.8.2: Link Configuration on page 52.

Modulation Reduction Level: (PTP only) Enter the number of modulation/coding levels to step down during re-transmission of wireless packets. Each step down lowers the UBR (e.g., change from 16 QAM 3/4 to 16 QAM 1/2). The level can be set from 0 to 7 (recommended value = 2). See Table 5: PTP & PMP - Modulation/Coding for UBR.

Uncoded Burst Rate [Mb/s]: Select the desired maximum UBR for the link *(maximum UBR is limited by the options key). See the following table. When Adaptive Modulation is enabled, this sets the maximum modulation/coding.

When Adaptive Modulation is disabled, the AN-80i will transmit using only the modulation/coding corresponding to the specified UBR. S ee the following table. The wireless link will be operational only if the AN-80i can meet the required BER.

Table 5: PTP & PMP - Modulation/Coding for UBR Settings

		Channel Sizes (MHz)							
		3.5	5	7	10	14	20	28*	40*
Modulation	**Coding**			**Uncoded**	**Burst**	**Rate**	**(Mbps)**		
64 QAM	3/4	9.5	13.5	19.0	27.0	38.0	54.0	76.0	108.0
64 QAM	2/3	8.4	12.0	16.8	24.0	33.5	48.0	67.0	96.0
16 QAM	3/4	6.3	9.0	12.5	18.0	25.0	36.0	50.0	72.0
16 QAM	1/2	4.3	6.0	8.5	12.0	17.0	24.0	34.0	48.0
QPSK	3/4	3.1	4.5	6.3	9.0	12.5	18.0	25.0	36.0
QPSK	1/2	2.1	3.0	4.3	6.0	8.5	12.0	17.0	24.0
BPSK	3/4	1.6	2.3	3.2	4.5	6.3	9.0	12.6	18.0
BPSK	1/2	1.0	1.5	2.0	3.0	4.0	6.0	8.0	12.0

* PTP Only

Channel Width [MHz]: Select the channel bandwidth. See Table 73: Spec. - Regional Identification Codes on page 144 for available channel widths.

Ethernet Follows Wireless: (PTP only) Check this box ☑ to have the AN-80i disable and enable the Ethernet port function based on the status of the wireless interface. This feature allows switches and routers to trigger configuration changes based on changes to the AN-80i Ethernet port status.

Disabled (□): The AN-80i Ethernet port is always enabled.

Enabled (☑):Ethernet port is controlled based on the status of the wireless interface.

> ***Important**: The Ethernet Follows Wireless setting affects all data and management traffic (HTTP, TELNET, and SNMP). While activated, it is not possible to manage the AN-80i using the Ethernet port.*

Table 6: PTP - Ethernet Follows Wireless Port Status Indication

Wireless interface Status	Ethernet Port Status
Link Up	Enabled
Link Down	Disabled

Ethernet follows wireless timeout [sec]: (PTP only) Enter the period (in seconds) the Ethernet port will remain disabled following loss of connectivity on the wireless interface. Following this interval, the Ethernet port will be automatically re-enabled to allow management of the AN-80i.

> ***Important**: When Ethernet Follows Wireless Timeout is enabled, external switches/routers monitoring the Ethernet port must be programmed to not switch automatically when the Ethernet port function is restored -- the wireless interface may not be operational.*

System Mode: Set the operating mode for each AN-80i system.

PTP Master: This unit begins transmitting automatically; sends poll messages to the remote AN-80i, and negotiates the wireless link.

PTP Slave: This unit waits passively, monitoring the selected channel(s) until polled by the PTP Master, and participates in negotiating the wireless link.

Software Version: Select the version of system software to load when the AN-80i is rebooted. The system holds two independent software images.

Link Length Measurement Mode: (PTP only) Select the mode for setting/measuring the distance between this and the remote-end unit.

Auto: Distance is calculated automatically by the AN-80i.

Manual: Enter the link distance manually in the Link Length field.

Link Length: (PTP only) Enter the actual length of the path that the radio wave travels between the two units. The link length is used to calculate the transmission-to-response interval and reject reflections of the transmitted signal. This setting is valid only when the Link Length Mode is set to Manual.

Link Length Measurements Unit: (PTP only) Select the units for the Link Length field.

Mile: Link length distance is displayed in miles.

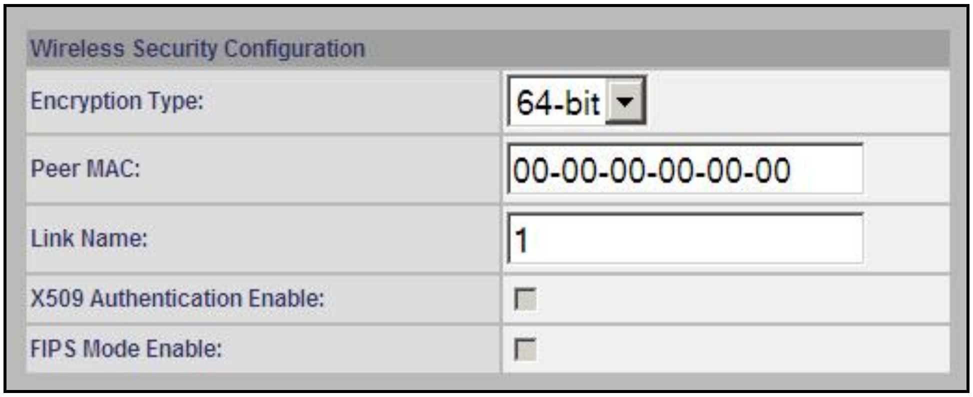
Km: Link length distance is displayed in kilometers.

Antenna Alignment Buzzer Enable: Check this box ☑ to enable the antenna alignment audible tone generator in the transceiver. The rate of the tone is proportional to the receive signal strength (faster = stronger signal).

Radio Enable: Check this box ☑ to enable the radio transmitter. It is not be possible to establish a wireless link when this box is unchecked.

3.4.3 Wireless Security

Use settings on this section of the screen to configure the AN-80i wireless security.



Wireless Security Configuration

Encryption Type:	64-bit ▾
Peer MAC:	00-00-00-00-00-00
Link Name:	1
X509 Authentication Enable:	□
FIPS Mode Enable:	□

Fig. 15: Web - PTP Wireless Configuration Screen

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

None: Encryption is disabled.*

64-bit: Redline proprietary encryption scheme. Compatible with AN-50e. The Peer MAC setting (below) must be set to match the communicating AN-80i/AN-50e).

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

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

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

Peer MAC: Use this field to identify the communicating AN-80i/AN-50e. The MAC address of the communicating AN-80i/AN-50e must be entered at both the PTP Master and PTP Slave when using one of the following applications:

- **Encryption Type** is set to **64-bit** (Redline proprietary encryption).

- Link is being monitored by the Redline Management System (RMS).

Link Name: Enter the shared name to uniquely identify this wireless link to both the local and remote-end systems.

On power-up/reboot or auto scan following deregistration or DFS event, the wireless link will only be established between two units having identical link names. The name may be blank or contain up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

> **Important**: A PTP wireless link can be established only between pairs of AN-80i or AN-80i-AN-50e systems having identical **Link Name** settings. The AN-80i **Link Name** field must be blank (delete all characters) to establish a wireless link with an AN-50e.

X509 Authentication Enable: Check this box ☑ to require authentication using an installed X.509 certificate. The user-defined unit certificate, authority certificate, and RSA private key must be downloaded using the CLI 'load' command. Uncheck this box to allow network connections without requiring authentication.

Note: AN-50e systems do not support X.509 authentication.

FIPS Mode Enable: Check this box ☑ to enable FIPS mode. The unit will enter FIPS mode only if the AN-80i is configured according to the FIPS standards. In FIPS mode, only FIPS approved algorithms are used for SSH, HTTPS and wireless security.

Notes:

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

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

3. FIPS X.509 certificates can be loaded only when the AN-80i is in FIPS mode.

Configuration Controls

Save: Click to activate and permanently save changes made in this screen. Changes to some parameters cause a system reboot when the Save button is selected. If the Save button is not clicked, all unsaved changes will be discarded on the next system reboot.

Test: Click to activate the changes made in this screen for a period of five minutes. During this test period, click the Save button at any time to permanently save the running configuration and disable the timer. If the Save button is not selected before the timer expires, the AN-80i is rebooted using the last saved configuration.

Reboot: Click to immediately reboot the AN-80i. All statistics are reset and unsaved changes are discarded. Operator confirmation is required.

Def Cfg: Click to overwrite the current saved configuration with the factory default settings. The AN-80i will reboot. Operator confirmation is required.

Chg Ver: Click to change to the other saved version of software (System Version field) and reboot. Operator confirmation is required.

Chapter 4

4 PMP Operation

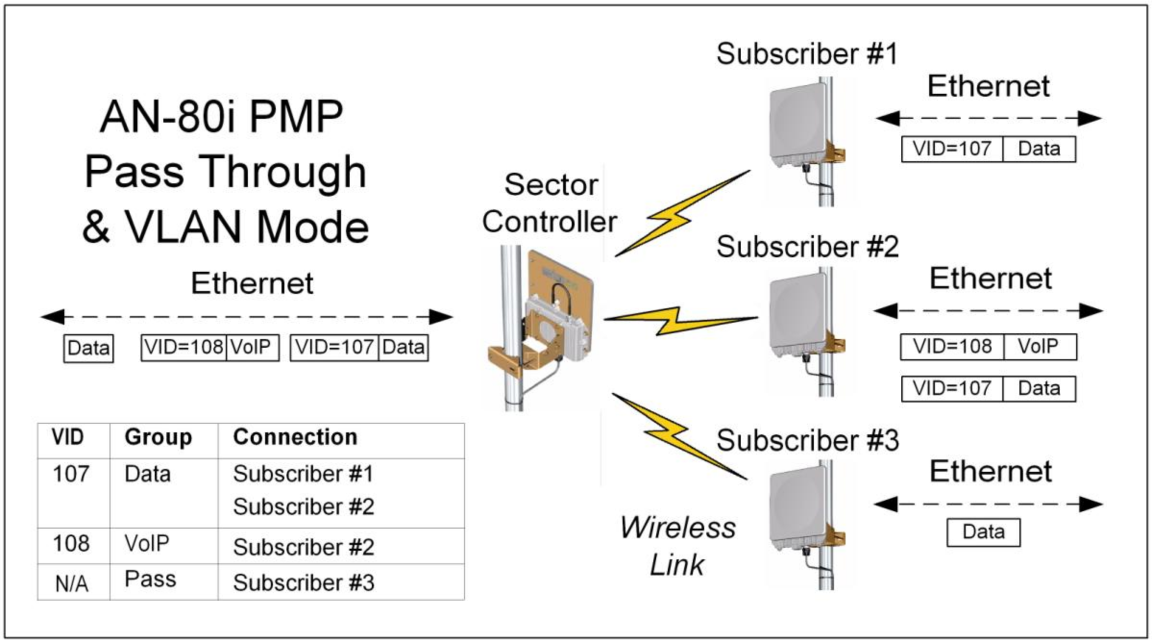
4.1 PMP General Operation

This section describes only the additional parameters required for configuring PMP support, and an overview about defining and using VLAN and pass-through groups.

The AN-80i PMP software provides the following main features:

- IEEE 802.1Q standard compliance
- Multiple TLS transport based on VLAN ID classification
- Multiple VLAN Connections per subscriber
- QoS provisioning with individual CIR setting per connection
- VLAN Groups span subscribers
- VLAN tagged management traffic
- VLAN trunking with tag insert/delete/re-map

For additional information, see the AN-80i PMP Operation Guide provided on the CD-ROM, and the Quick Install Guide later in this guide and separately on the CD-ROM. The deployed AN-80i wireless network can function as a standard wireless bridge (pass-through mode), as a VLAN-aware wireless switch, or a combination of both.



VID	Group	Connection
107	Data	Subscriber #1 Subscriber #2
108	VoIP	Subscriber #2
N/A	Pass	Subscriber #3

Fig. 16: Web - PMP - VLAN Tagged Traffic Example

The diagram illustrates a network implementation using two VLAN groups and a pass through group. The packets tagged with VID=107 are classified as data traffic, and the packets tagged with VID=108 are classified as voice (VoIP) traffic. Subscribers #1 and #2 are members of the Data group, while only subscriber #2 is a member of the Voice group. Subscriber #3 is a member of the Pass through group and receives traffic that does not match the VID of the Data or Voice groups.

4.1.1 Minimum Setup Requirements

A minimum set of parameters must be configured to enable data and management traffic on any PMP deployment:

1. **Links:** Links identify each subscriber in the sector (by MAC address) and set the maximum uplink and downlink throughput (UBR) for each wireless link.
2. **Groups:** Groups classify and filter traffic to/from core network (sector controller Ethernet port). A Group definition must be created for each VLAN to be forwarded over the sector controller wireless interface. The Group also defines multicast characteristics for traffic using this VID. A 'pass through' Group can be created to manage traffic not matched by any VLAN Group.
3. **Connections:** Connections classify and filter traffic to/from the remote network (subscriber Ethernet port). A Connection definition must be created for each VLAN to be forwarded over the subscriber wireless interface. The Connection also defines the unicast uplink and downlink QoS for this traffic.

Notes:

1. Redline's PMP Configuration Tool must be used to obtain accurate QoS values for Groups and Connections.
2. Use the pass through Group to transparently pass VLAN traffic across the wireless interface.
3. Re-map VLANs between the core network (Group VID) and the subscribers local network (Connection VID).
4. Operation is restricted to one pass through Group on the sector controller and one pass through Connection on each subscriber.

4.2 PMP System Menu

The Web Interface provides all required settings and statistics necessary to configure and monitor the operation of the AN-80i using a standard web browser. An operator can access and control the AN-80i remotely from any geographical location with HTTP connectivity to that unit.

The following menu items are available for configuring and monitoring the PMP functions. Note that the Browse Groups and all IDs items are available (**blue text**) only on the sector controller (PMP SC) menu.

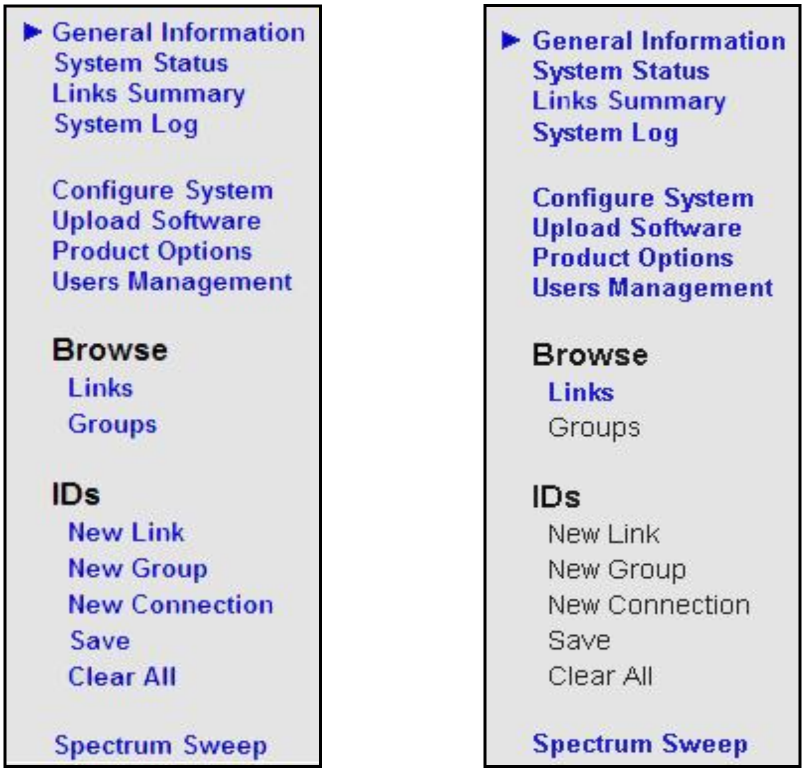
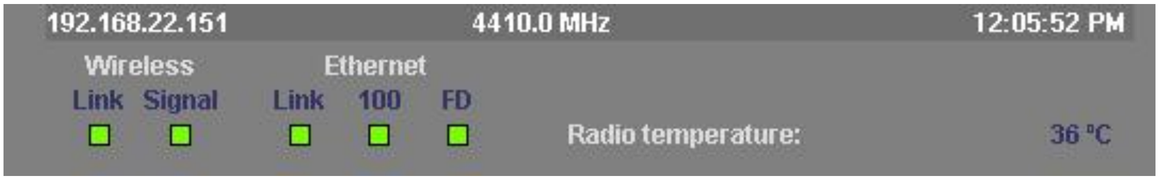


Fig. 17: Web - PMP Menu for Sector Controller (left) and Subscriber (right)

4.3 PMP Dashboard Display

4.3.1 General Information

The dashboard display at the top of all screens shows summary of important operational information including: the unit IP address, operating frequency, current time (web user's platform), wireless status, Ethernet status, and the radio temperature.



192.168.22.151 4410.0 MHz 12:05:52 PM

Radio temperature: 36 °C

Fig. 18: Web - PMP - Dashboard Display

IP Address: Current IP address setting of this unit.

Wireless Frequency: Current RF channel frequency.

Time: Time obtained from user's Web browser.

Radio Temperature: Internal temperature of the radio.

4.3.2 Wireless Leds

Wireless Link LED

The wireless Link LED lights solid green under the following conditions:

Sector Controller: Wireless link is established to one or more subscribers.

Subscriber: Wireless link is established to the sector controller.

If the LED is off, it may indicate one of the issues listed in the following table:

Wireless Signal LED

The wireless Signal LED operation is based on the adaptive modulation setting for each subscriber:

Enabled: LED lights solid green when the wireless link is operating at the rate equal to the Uncoded Burst Rate setting, and blinks when operating at a lower rate.

Disabled: LED lights solid green when the wireless link is established.

4.3.3 Ethernet LEDs

Ethernet Link LED

The Ethernet Link LED lights solid green when there is an Ethernet connection and no traffic, and blinks when traffic is detected. If the LED is off, it may indicate one of the issues listed in the following table:

Ethernet 100 LED

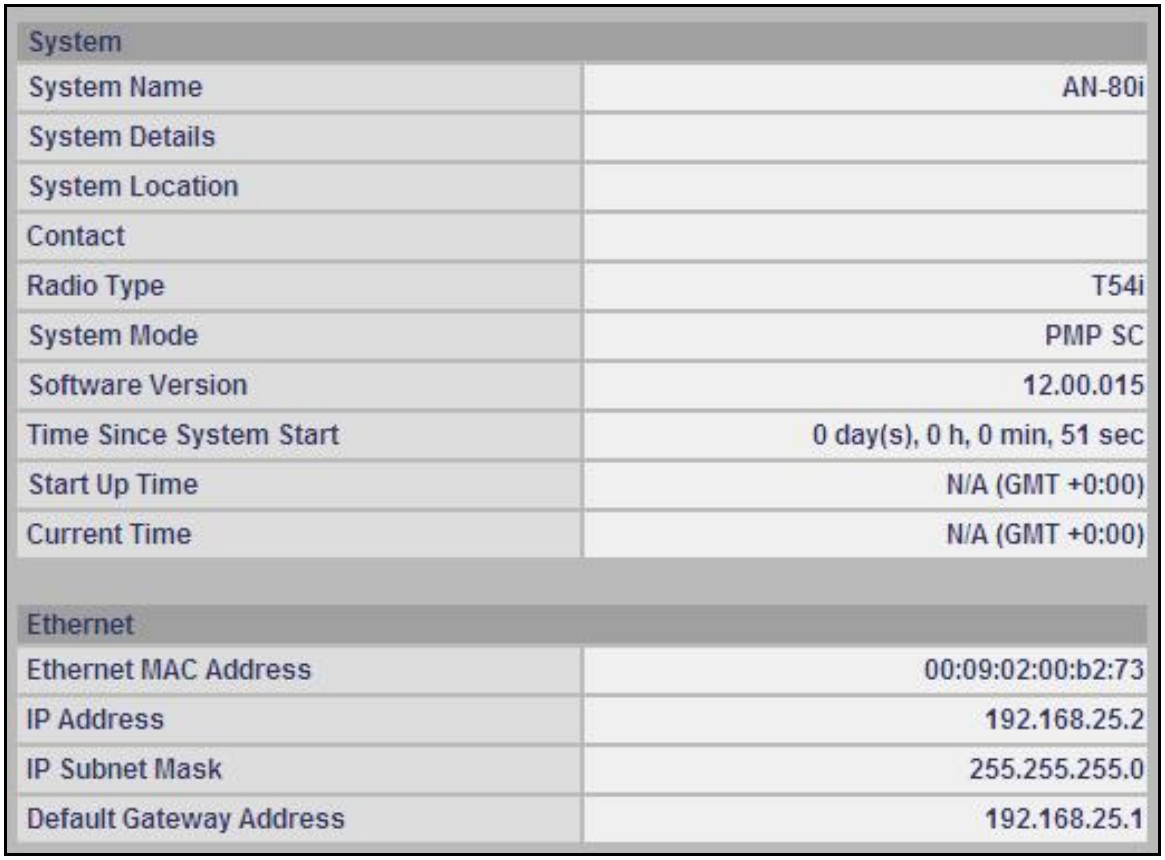
The Ethernet 100 LED lights solid green when the Ethernet port is operating at 100 Mb/s and the LED is off when operating at 10 Mb/s. If the LED is off, it may indicate one of the issues listed in the following table:

Ethernet FD LED

The FD LED lights solid green when the Ethernet connection is operating in full duplex mode and blinks when collisions are detected on the Ethernet port. If the LED is blinking, it may indicate one of the issues listed in the following table:

4.4 PMP General Information Screen

The General Information screen provides details about the system and the Ethernet interface. See the General Information screen for details.



System	
System Name	AN-80i
System Details	
System Location	
Contact	
Radio Type	T54i
System Mode	PMP SC
Software Version	12.00.015
Time Since System Start	0 day(s), 0 h, 0 min, 51 sec
Start Up Time	N/A (GMT +0:00)
Current Time	N/A (GMT +0:00)

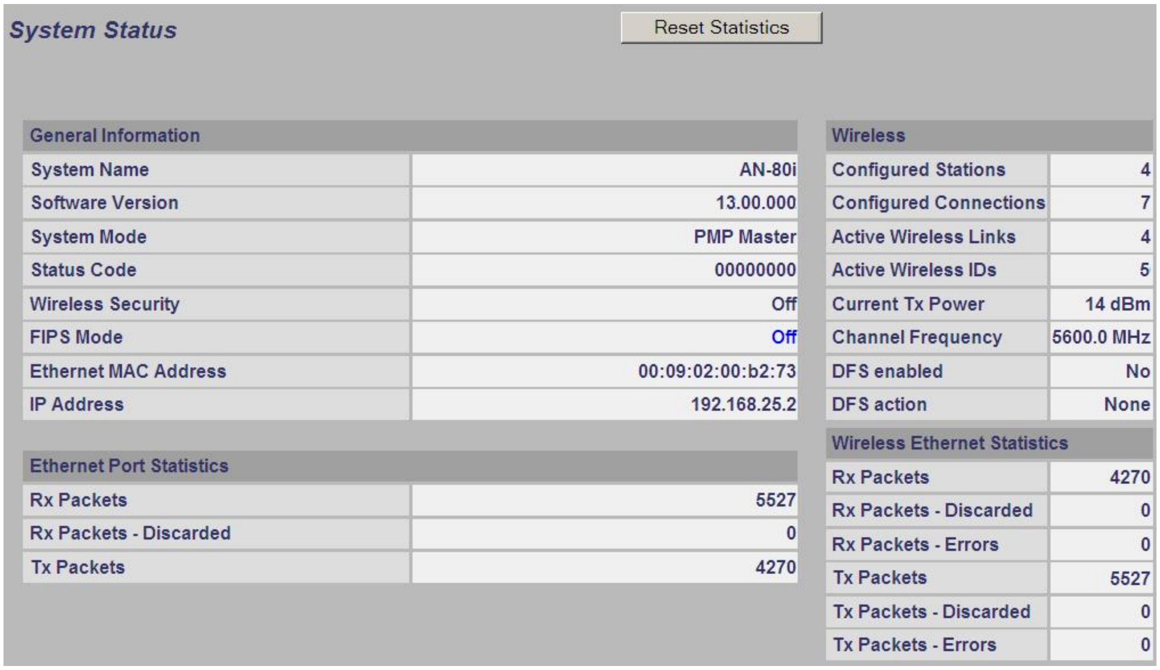
Ethernet	
Ethernet MAC Address	00:09:02:00:b2:73
IP Address	192.168.25.2
IP Subnet Mask	255.255.255.0
Default Gateway Address	192.168.25.1

Fig. 19: Web - PMP General Information Screen

These fields are common for operation in PMP and PTP mode. See the General Information screen for details about these fields.

4.5 PMP System Status Screen

Click **System Status** in the main menu to view system, Ethernet statistics, and wireless interface statistics.



General Information	
System Name	AN-80i
Software Version	13.00.000
System Mode	PMP Master
Status Code	00000000
Wireless Security	Off
FIPS Mode	Off
Ethernet MAC Address	00:09:02:00:b2:73
IP Address	192.168.25.2

Ethernet Port Statistics	
Rx Packets	5527
Rx Packets - Discarded	0
Tx Packets	4270

Wireless	
Configured Stations	4
Configured Connections	7
Active Wireless Links	4
Active Wireless IDs	5
Current Tx Power	14 dBm
Channel Frequency	5600.0 MHz
DFS enabled	No
DFS action	None

Wireless Ethernet Statistics	
Rx Packets	4270
Rx Packets - Discarded	0
Rx Packets - Errors	0
Tx Packets	5527
Tx Packets - Discarded	0
Tx Packets - Errors	0

Fig. 20: Web - PMP System Status Screen

The following fields are specific to operation in PMP mode. See 3.3: PTP System Status Screen on page 28 for information on all other fields.

Configured Stations: Number of Links defined (to subscribers).

Configured Connections: Number of Connections defined for all subscribers.

Active Wireless Links: The number of registered subscribers.

Active Wireless IDs: The number of connections to registered subscribers.

Current Tx Power: The current transmit power level.

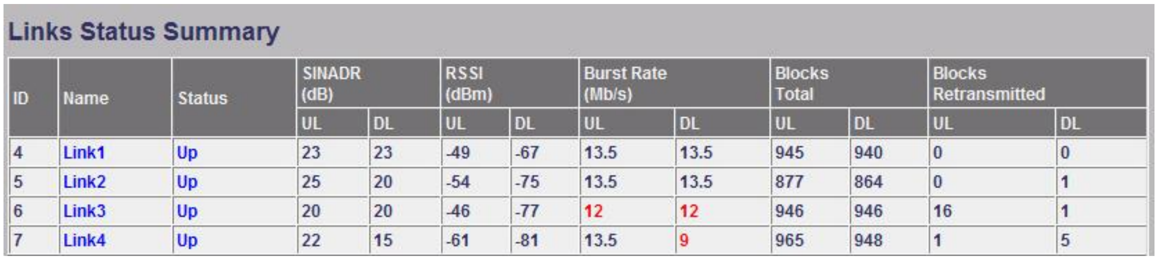
Current Frequency: Current RF channel frequency.

4.6 PMP Links Summary Screen

Click **Links Summary** in the main menu to view system, Ethernet statistics, and wireless interface statistics.

The Link Status Summary page displays information about all wireless links. This information includes: ID, name, status, and uplink/downlink statistics for SINADR, RSSI, burst rate, total blocks transmitted, and blocks retransmitted.

This table also provides direct links to the link configuration and statistics pages.



Links Status Summary

ID	Name	Status	SINADR (dB)		RSSI (dBm)		Burst Rate (Mb/s)		Blocks Total		Blocks Retransmitted	
			UL	DL	UL	DL	UL	DL	UL	DL	UL	DL
4	Link1	Up	23	23	-49	-67	13.5	13.5	945	940	0	0
5	Link2	Up	25	20	-54	-75	13.5	13.5	877	864	0	1
6	Link3	Up	20	20	-46	-77	12	12	946	946	16	1
7	Link4	Up	22	15	-61	-81	13.5	9	965	948	1	5

Fig. 21: Web - PMP Links Summary Screen

ID: Unique ID assigned to this link.

Name: Click on the Name field e.g., Link-1) to display the associated configuration page,

Status: Click on the Status field (e.g., Up) to display wireless and Ethernet statistics for this link.

SINADR (dB): Average signal to interference, noise, and distortion ratio.

RSSI (dBm): Received signal strength indicator.

Burst Rate (Mb/s): The current uncoded burst rate for the link. The DL Burst Rate for this link is displayed in red when adaptive modulation is enabled and the DL UBR selected by adaptive modulation does not support the current setting. Refer to section 4.8.2: Link Configuration on page 52.

Blocks Total: Blocks transmitted over the wireless interface.

Blocks Retransmitted: Blocks retransmitted over the wireless interface.

4.7 PMP System Configuration Screen

Click **Configure System** in the main menu to view and adjust configuration settings for general system identification, Ethernet, and the wireless interface. The fields specific to PMP are highlighted.

4.7.1 Ethernet Interface

Use settings in the Ethernet section of the screen to configure the AN-80i Ethernet interface. These fields are common for PTP and PMP modes of operation with the following exceptions:

Flow Control: PTP only.

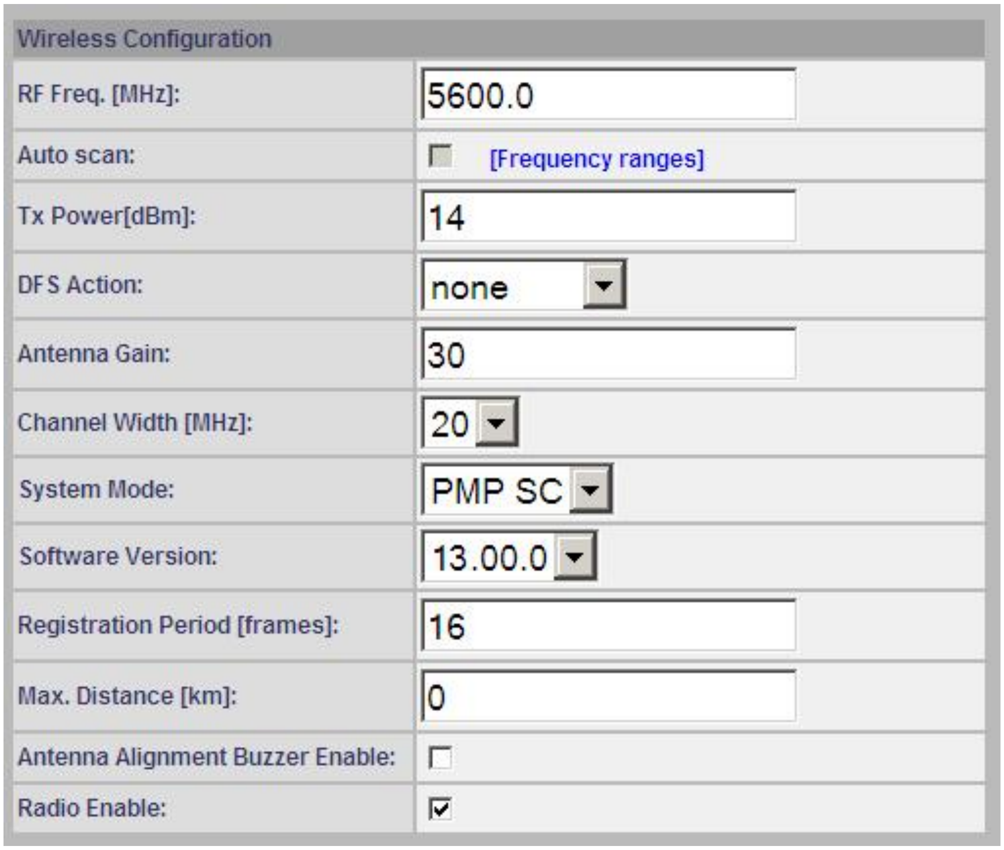
Prioritized Low Latency Mode: PTP Only

SNMP Enable: SNMP v2 only in PMP mode.

See 3.4.1: Ethernet on page 31 for information on all Ethernet fields.

4.7.2 Wireless Interface

Use settings on this section of the screen to configure the AN-80i wireless interface. This section describes fields specific to PMP mode. See the PTP section Wireless on page 27 for details about all other fields.



Wireless Configuration	
RF Freq. [MHz]:	5600.0
Auto scan:	□ [Frequency ranges]
Tx Power[dBm]:	14
DFS Action:	none
Antenna Gain:	30
Channel Width [MHz]:	20
System Mode:	PMP SC
Software Version:	13.00.0
Registration Period [frames]:	16
Max. Distance [km]:	0
Antenna Alignment Buzzer Enable:	□
Radio Enable:	☑

Fig. 22: Web - PMP - Wireless Configuration Screen

Auto scan: (PMP SS only) Check this box ☑ to enable the subscriber to automatically scan available channels to locate and register with a sector controller.

Click the blue text **[Frequency Ranges]** adjacent to the check box to display the Frequency Management screen (see Frequency Range on page 75). The sector controller can be programmed with a master list of frequency ranges. When a subscriber registers with the sector controller, the programmed frequency ranges are downloaded by the subscriber (displayed as Remote Frequency Ranges on the subscriber). The downloaded range settings are used exclusively by the subscriber during autoscan and remain in effect until the subscriber is rebooted (setting are discarded at reboot.

PMP SS: When no frequency ranges are entered (default), the subscriber scans all available frequency ranges for that region (refer to 9.5: Regional Codes on page 144). When one or more frequency ranges have been entered (or downloaded from the sector controller), only these frequency ranges are scanned. If all entered frequency ranges are scanned (x3) without registering with a sector controller, the subscriber defaults to scanning all enabled frequencies.

System Mode: The system designated as sector controller establishes and manages the bi-directional data link with a remote end AN-80i. Only one system in a wireless link must be set for Sector Controller mode (PMP SC).

PMP SC: AN-80i begins transmitting automatically, sends poll messages to locate and register remote AN-80i subscribers, and negotiates operating settings for the link.

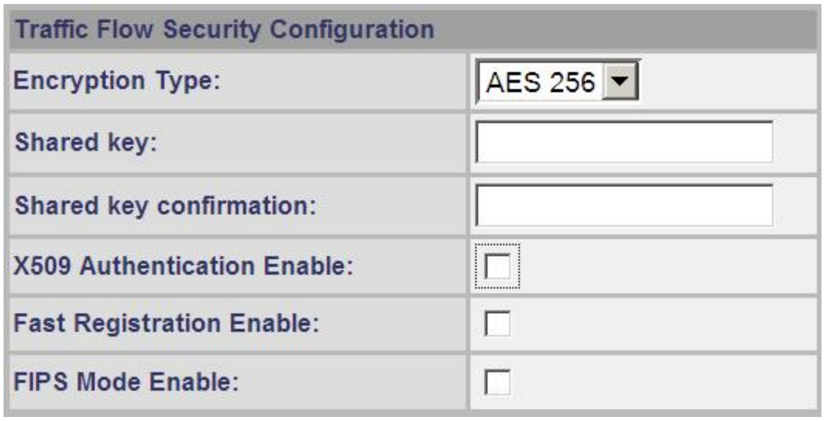
PMP SS: AN-80i monitors the selected channel(s) until polled by the PMP Sector Controller.

Registration Period: The polling period for detecting new subscribers. This period is based on the number of wireless frames transmitted. Permitted values are 1 to 400 frames. It is recommended to use four frames as the default registration period.

Max. Distance [km]: Enter the distance to the subscriber located farthest away from the sector controller (outer boundary of sector). This parameter is used to optimize communications with the subscribers.

4.7.3 Wireless Security

Use these settings to configure the AN-80i wireless security features.



Traffic Flow Security Configuration

Encryption Type:	AES 256 ▾
Shared key:	
Shared key confirmation:	
X509 Authentication Enable:	□
Fast Registration Enable:	□
FIPS Mode Enable:	□

Fig. 23: Web - PMP - Wireless Configuration Screen

Encryption Type: Select an encryption type for data transmitted over the wireless interface. All units in a sector must be set to the same encryption type.

None: Encryption is disabled.*

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

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

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

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

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

X509 Authentication Enable: Check this box ☑ to require authentication using an installed X.509 certificate. The user-defined unit certificate, authority certificate, and RSA private key must be downloaded using the CLI 'load' command. Uncheck this box to allow network connections without requiring authentication.

Note: AN-50e systems do not support X.509 authentication.

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

FIPS Mode Enable: Check this box ☑ to enable FIPS mode. The unit will enter FIPS mode only if the AN-80i is configured according to the FIPS standards. In FIPS mode, only FIPS approved algorithms are used for SSH, HTTPS and wireless security.

BS MAC: (Subscriber only) MAC address of the sector controller. The subscriber will establish a wireless link only with the base station having the MAC address recorded in this field. If this field is zero (00-00-00-00-00-00), the subscriber will establish a wireless link with any base station.

Notes:

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

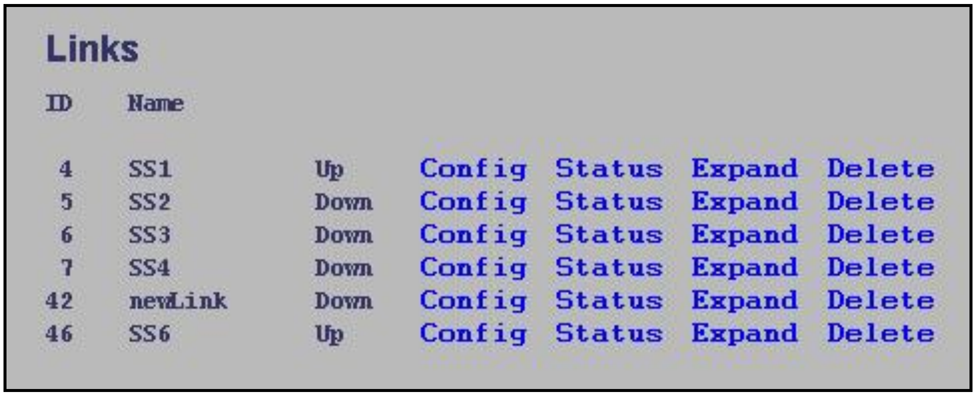
2. AES encryption is not available until the X.509 certificate and key files have been loaded (usr_wacert_<mac>.der, usr_wcert_<mac>.der, and usr_wkey_<mac>.der).

3. FIPS X.509 certificates can be loaded only when the AN-80i is in FIPS mode.

4.8 PMP Link Screens

4.8.1 Links Browse Screen

Click **Links** in the main menu to display the links browse screen. This is a list of all configured wireless links. Click **New Links** in the main menu to create a link.



Links

ID	Name					
4	SS1	Up	Config	Status	Expand	Delete
5	SS2	Down	Config	Status	Expand	Delete
6	SS3	Down	Config	Status	Expand	Delete
7	SS4	Down	Config	Status	Expand	Delete
42	newLink	Down	Config	Status	Expand	Delete
46	SS6	Up	Config	Status	Expand	Delete

Fig. 24: Web - PMP - Links Browse Screen

ID: Unique number identifying each link.

Name: User-assigned name for each link.

Status: Field indicates the current status of the wireless link.

Up: The subscriber is registered.

Down: The subscriber is not registered.

Config: Click **Config** to display the **Link Configuration** screen for that Link.

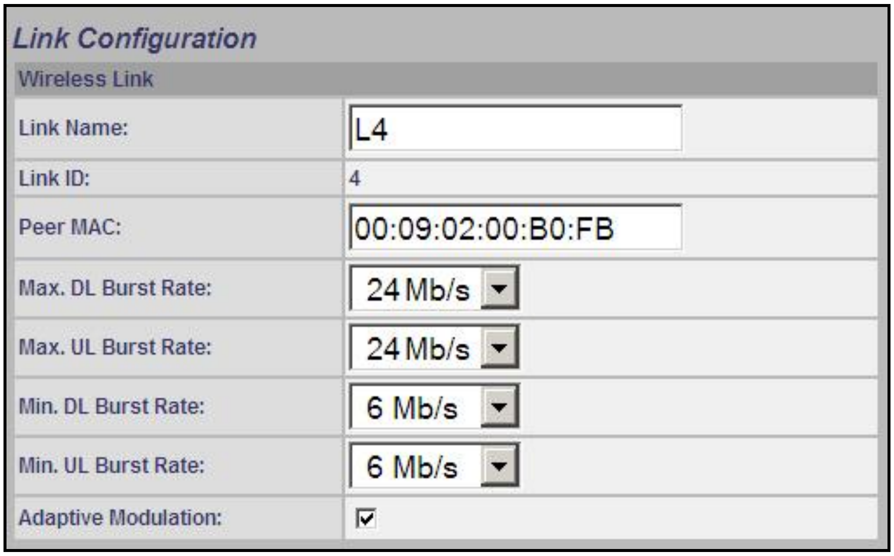
Status: Click **Status** to display the **Link Statistics** screen for that Link. This includes uplink and downlink statistics for the link.

Expand: Click **Expand** to display the **Connections** browse screen showing all Connections for that Link.

Delete: Click **Delete** to delete that Link. A link can not be deleted until all Connections referencing this link are deleted.

4.8.2 Link Configuration

Use this screen to display and modify existing link settings. Access existing links through the Links Browse screen or click **New Links** in the main menu to add a new link.



Link Configuration

Wireless Link

Link Name:	L4
Link ID:	4
Peer MAC:	00:09:02:00:B0:FB
Max. DL Burst Rate:	24 Mb/s
Max. UL Burst Rate:	24 Mb/s
Min. DL Burst Rate:	6 Mb/s
Min. UL Burst Rate:	6 Mb/s
Adaptive Modulation:	☑

Fig. 25: Web - PMP - Link Configuration Screen

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

Link ID: (Read only) A unique ID is automatically generated when a Link is created.

Peer MAC: MAC address of the subscriber station. The sector controller will establish a wireless link only if the subscriber MAC address is recorded in this field.

Note: This behavior is different in PTP mode.

Max. DL Burst Rate: Set the desired maximum downlink burst rate for unicast traffic from the sector controller to the subscriber. This setting determines the maximum modulation/coding setting for this link.

Max. UL Burst Rate: Set the desired maximum uplink burst rate for unicast traffic from the subscriber to the sector controller. This setting determines the maximum modulation/coding setting for this link.

Min. DL Burst Rate: Set the minimum desired downlink burst rate for unicast traffic from the sector controller to the subscriber when adaptive modulation is enabled. If the DL UBR selected by adaptive modulation does not support the current setting, the DL Burst Rate for this link is displayed in red on the Link Status Summary page.

The Min. Burst Rate setting should be calculated using the PMP configuration tool.

Min UL Burst Rate: Set the minimum desired uplink burst rate for unicast traffic from the subscriber to the sector controller when adaptive modulation is enabled. If the UL UBR selected by adaptive modulation does not support the current setting, the UL Burst Rate for this link is displayed in red on the Link Status Summary page.

> ***Important**: Burst rate settings affect operation of the entire sector and should be verified using the latest version of the Redline PMP configuration tool.*

Adaptive Modulation: Select the adaptive modulation mode.

The adaptive modulation feature provides automatic adjustments to maintain wireless link operation during periods of transient interference, power variations (fade), and reflections. This feature is enabled and disabled individually for each Subscriber Link.

Enabled (☑):Automatically adjust the modulation and coding to achieve the highest throughput where packet error rates (PER) are lower than a pre-set value. When packet error rates exceed the threshold, the modulation/code combination is adjusted to maintain the connection at a lower throughput rate (graceful degradation).

Automatic adjustments to the modulation/coding result in relative changes to the PIR of all connections on that wireless link. This ensures the degradation of any single link does not affect the throughput of other links in the sector.

When adaptive modulation adjusts the uplink or downlink modulation/coding settings of a wireless link to below the desired minimum burst rate setting, the burst rates are displayed in red, and the PIR values for all Services and Service Groups are temporarily proportionally reduced.

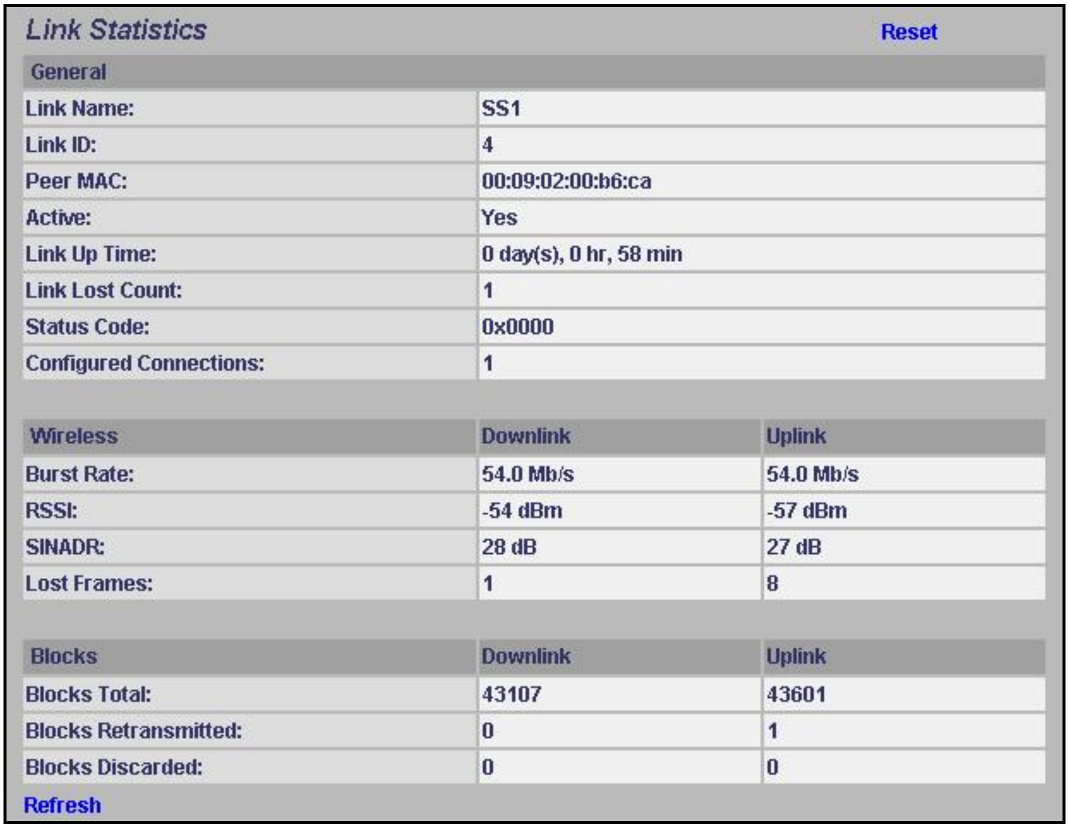
Example: In a link operating at 16 QAM 3/4, transient interference may result in a temporary change from to 16 QAM 1/2 to maintain the required PER. The AN-80i will periodically test transmission at a higher rate and resume operation at the normal rate after the interference has cleared.

Disabled (□): Modulation and coding values are fixed at settings required to achieve the operator selected UBR (Max. UL Burst Rate / Max. DL Burst Rate).

Note: Adaptive modulation is 'disabled' by default when upgrading from PMP versions earlier than v12.00.

4.8.3 Link Statistics

The Link Statistics screen is accessible only from the Links browse screen (refer to 4.8: PMP Link Screens on page 51). Click **Links** in the main menu to locate the desired link and then click **Status** to display the link statistics screen.



Link Statistics

Reset

General		
Link Name:	SS1	
Link ID:	4	
Peer MAC:	00:09:02:00:b6:ca	
Active:	Yes	
Link Up Time:	0 day(s), 0 hr, 58 min	
Link Lost Count:	1	
Status Code:	0x0000	
Configured Connections:	1	
Wireless	**Downlink**	**Uplink**
Burst Rate:	54.0 Mb/s	54.0 Mb/s
RSSI:	-54 dBm	-57 dBm
SINADR:	28 dB	27 dB
Lost Frames:	1	8
Blocks	**Downlink**	**Uplink**
Blocks Total:	43107	43601
Blocks Retransmitted:	0	1
Blocks Discarded:	0	0

Refresh

Fig. 26: Web - PMP - Link Statistics Screen

General

Link Name: User-assigned name for this link.

Link ID: Unique number identifying this link.

Peer MAC: MAC Address of the subscriber.

Active: Indicates if wireless link is operational (Active=YES).

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

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

Status Code: Code indicating the condition of the AN-80i system. Status indications are specific for PMP and PTP operation.

Configured Connections: The number of Connections configured on this link.

Wireless

The following statistics are displayed for both uplink and downlink.

Burst Rate: The current uncoded burst rate for the link.

RSSI: Received signal strength indicator.

SINADR: Average signal to interference, noise, and distortion ratio.

Lost Frames: Number of frames lost.

Blocks

Blocks Total: Total number of blocks transmitted over the wireless interface.

Blocks Retransmitted: Number of blocks retransmitted over the wireless interface.

Blocks Discarded: Number of blocks discarded (could not be sent over the wireless).

Controls

Refresh: Click **Refresh** (bottom left) to update the statistics display.

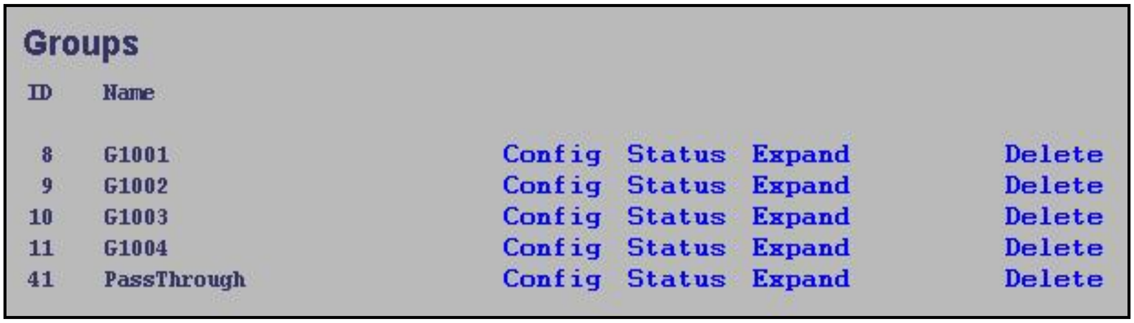
Reset: Click **Reset** (top right) to zero the counters for the wireless and Ethernet LAN Statistics displayed on this page.

4.9 PMP Group Screens

4.9.1 Groups Browse Screen

Click **Groups** in the main menu to display the Groups browse screen. This is a list of all configured Groups. Click **New Group** in the main menu to create a Group.

The Group configuration defines how Ethernet packets are handled on the sector controller. A unique Group must be created for each VLAN.



Groups

ID	Name				
8	G1001	Config	Status	Expand	Delete
9	G1002	Config	Status	Expand	Delete
10	G1003	Config	Status	Expand	Delete
11	G1004	Config	Status	Expand	Delete
41	PassThrough	Config	Status	Expand	Delete

Fig. 27: Web - PMP - Groups Browse Screen

ID: Unique number identifying each Group.

Name: User-assigned name for each Group.

Config: Click **Config** on a line to display the **Group Configuration** screen associated with that Group.

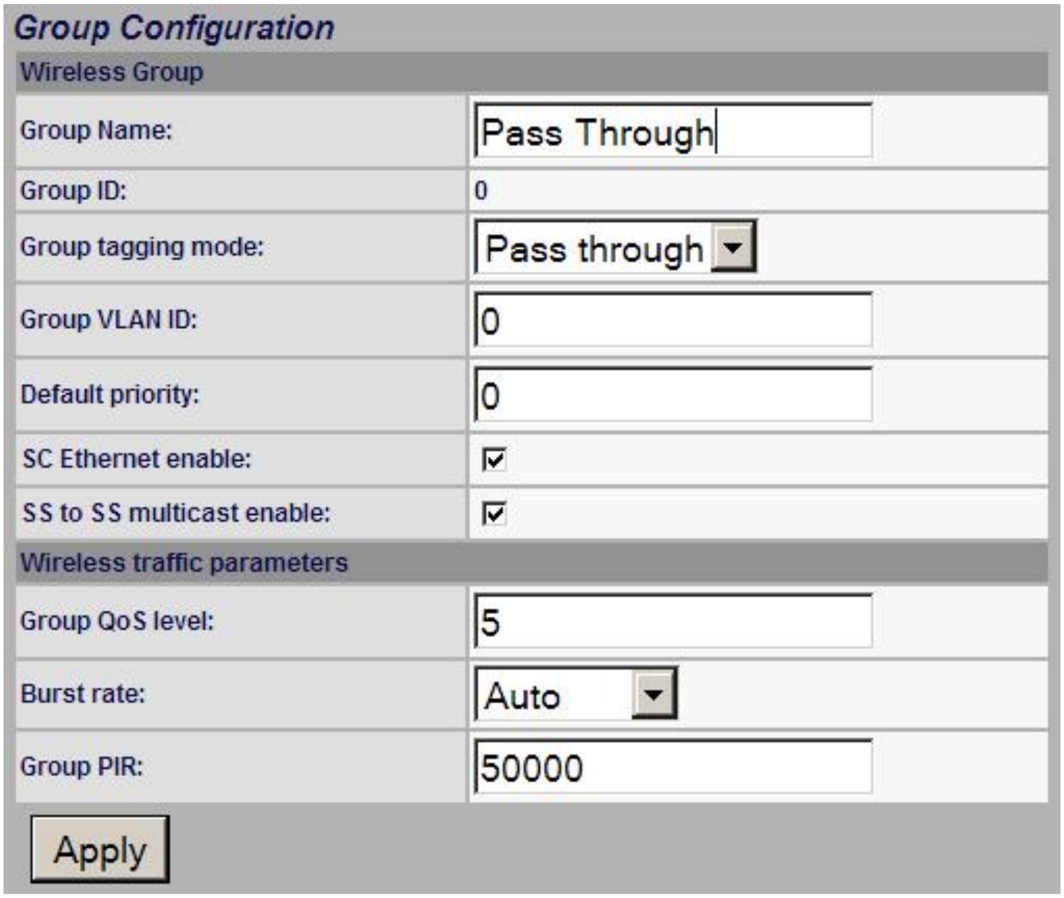
Status: Click **Status** on a line to display the **Group Statistics** screen associated with that Group. This includes uplink and downlink statistics for the Group.

Expand: Click **Expand** on a line to display the **Connections** browse screen showing all Connections associated with that Group.

Delete: Click **Delete** on a line to delete that Group. A Group can not be deleted until all Connections referencing this Group are deleted.

4.9.2 Group Configuration

Click **New Group** in the main menu to display the Group Configuration screen and define a new Group. Use the Group browse screen (refer to 4.9 PMP Group Screens on page 56) to view/modify existing Groups. Click **Groups** in the main menu to locate the desired Group and then click **Config** to display the Group Configuration screen.



Group Configuration

Wireless Group	
Group Name:	Pass Through
Group ID:	0
Group tagging mode:	Pass through
Group VLAN ID:	0
Default priority:	0
SC Ethernet enable:	☑
SS to SS multicast enable:	☑
Wireless traffic parameters	
Group QoS level:	5
Burst rate:	Auto
Group PIR:	50000

Fig. 28: Web - PMP - Group Configuration Screen

Wireless Group

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

Group ID: (Read only) A unique ID is automatically generated when a Group is created.

Group Tagging Mode: Select the classification mode for this group.

Classified (matching) packets are forwarded to all members of this group.

> **Tagged**: Classify only packets that have the VLAN ID entered in the Group VLAN ID field for this Group.
>
> **Pass-through**: Classify all packets that do not have a VLAN ID, or where the outermost VLAN ID tag does not match the VLAN ID for any tagged Group.

Group VLAN ID: Enter the VID associated with this Group definition.

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

Default Priority: Enter the default 802.1p priority setting (0-7).

The Group Default Priority value is used when adding the 802.1Q tag (Connection VLAN ID) to a packet being forwarded only when the Group Tagging Mode is 'pass-through' and the destination Connection Tagging Mode is set to 'Tagged'.

SC ethernet enable: Controls the function of the sector controller Ethernet port for group multicast traffic.

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

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

SS To SS multicast enable:

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

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

Wireless Traffic Parameters

Changes to these settings affect the CIR and PIR for all groups and connections on the wireless link.

Group QoS Level: This is the approximate CIR for downlink broadcast and multicast traffic belonging to this group. This value represents a range of CIR.

It is strongly recommended to calculate the Group QoS Level using the Redline AN-80i PMP Configuration Tool. To set this value without using the tool, first identify the member wireless link operating at the lowest UBR, and then calculate the Group QoS Level using the following formula:

Burst Rate - 1.

Note: A zero setting disables all DL broadcast and multicast traffic for this group.

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

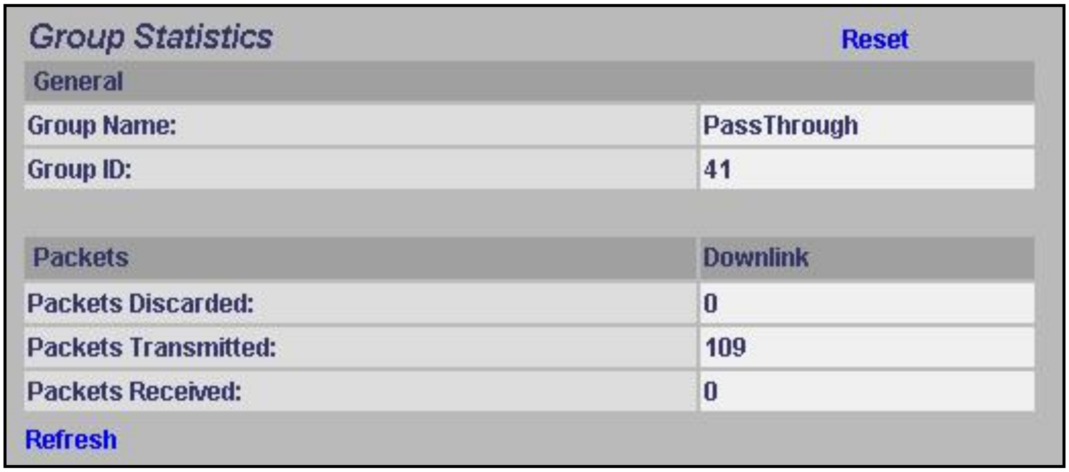
Max DL Burst Rate - 1

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

Group PIR: Set the PIR for downlink broadcast and multicast traffic belonging to this group. A single PIR setting is applied for each group. When adaptive modulation is enabled, automatic adjustments to the modulation/coding will result in relative changes to the PIR of all groups and connections on that wireless link.

4.9.3 Group Statistics

Use the Group statistics screen to view statistics for all downlink traffic on Connections to this Group. Click **Groups** in the main menu to display the Groups browse screen. Click **Status** to display downlink statistics for a Group.



Group Statistics

General	
Group Name:	PassThrough
Group ID:	41

Packets	Downlink
Packets Discarded:	0
Packets Transmitted:	109
Packets Received:	0

Fig. 29: Web - PMP - Group Statistics Screen

General

Group Name: Name assigned to this Group.

Group ID: Unique numeric identifier for this Group.

Packet (Downlink)

Packets Discarded: Number of Ethernet packets discarded (not sent over wireless).

Packets Transmitted: Number of Ethernet packets transmitted over the wireless interface.

Packets Received: Number of Ethernet packets received over the wireless interface.

Controls

Reset: Click **Reset** to zero the statistics values.

Refresh: Click **Refresh** to update the statistics display.

4.10 PMP Connection Screens

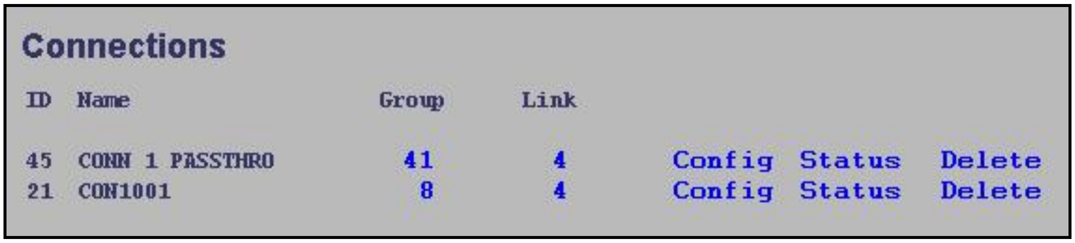
4.10.1 Connections Browse Screen

This is a list of all configured Connections. Click **New Connection** in the main menu to create a connection.

The Connections browse screen is accessible from the Links browse screen (refer to 4.8: PMP Link Screens on page 51). Click **Links** in the main menu to locate the desired link and then click **Expand** to display the Connections browse screen. The Connections are displayed sorted by Link.

The Connections browse screen is accessible from the Groups browse screen (refer to 56 PMP Group Screens on page 56).

Click **Groups** in the main menu to locate the desired Group and then click **Expand** to display the Connections browse screen. The Connections are displayed sorted by Group.



Connections

ID	Name	Group	Link			
45	CONN 1 PASSTHRO	41	4	Config	Status	Delete
21	CON1001	8	4	Config	Status	Delete

Fig. 30: Web - PMP - Link (Expand) Connections Screen

ID: Unique number identifying each Connection.

Name: User-assigned name for each Connection.

Group: Click the Group number (e.g., **41**) on a line to display the **Group Configuration** screen associated with this Connection.

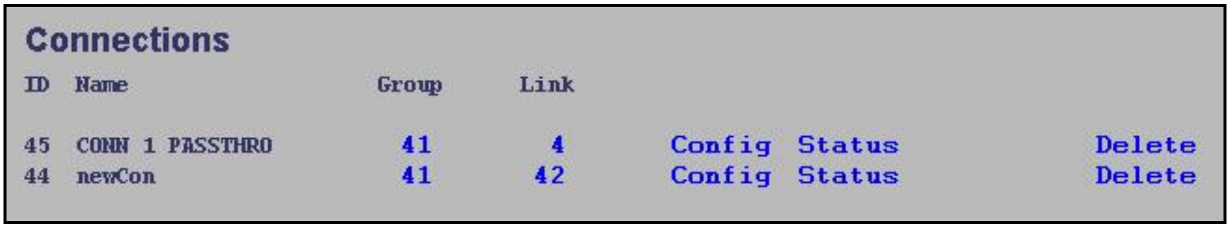
Link: Click the link number (e.g., **4**) on a line to display **Link Configuration** screen for that link.

Config (Configure): Click **Config** on a line to display the **Connection Configuration** screen for that Connection.

Status (Statistics): Click **Status** to display the Connection Statistics screen for that Connection.

Expand: Click **Expand** on a line to display the **Connections** browse screen.

Delete (Delete): Click **Delete** on a line to delete that Connection.



Connections

ID	Name	Group	Link			
45	CONN 1 PASSTHRO	41	4	Config	Status	Delete
44	newCon	41	42	Config	Status	Delete

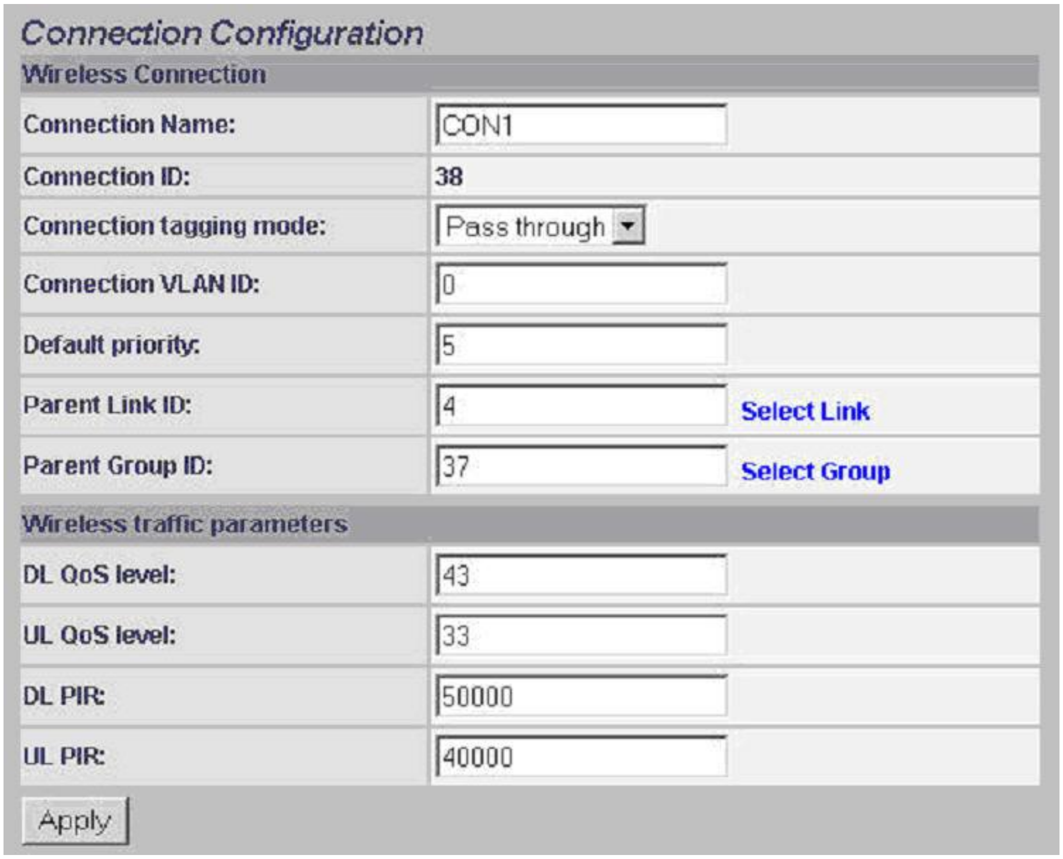
Fig. 31: Web - PMP - Connections Screen (Example: by Group)

4.10.2 Connection Configuration Screen

Click **New Connection** in the main menu to display the Connection Configuration screen and add a new connection (Link + Group).

Use the Links browse screen (refer to 4.8: PMP Link Screens on page 51) to view/modify existing Connections. Click **Links** in the main menu to locate the desired link and then click **Expand** to display the Connections browse screen. Click **Config** to display the Connection Configuration screen.

Use the Groups browse screen (refer to 4.9 PMP Group Screens on page 56) to view/modify existing Connections. Click **Groups** in the main menu to locate the desired Connection and then click **Expand** to display the Connections brows e screen. Click **Config** to display the Connection Configuration screen.



Connection Configuration

Wireless Connection

Connection Name:	CON1	
Connection ID:	38	
Connection tagging mode:	Pass through	
Connection VLAN ID:	0	
Default priority:	5	
Parent Link ID:	4	Select Link
Parent Group ID:	37	Select Group

Wireless traffic parameters

DL QoS level:	43
UL QoS level:	33
DL PIR:	50000
UL PIR:	40000

Fig. 32: Web - PMP - Connection Configuration Screen

Wireless Connection

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

Connection ID: (Read only) A unique ID is automatically generated when a Connection is created.

Connection tagging mode: Select the classification mode for this Connection.

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

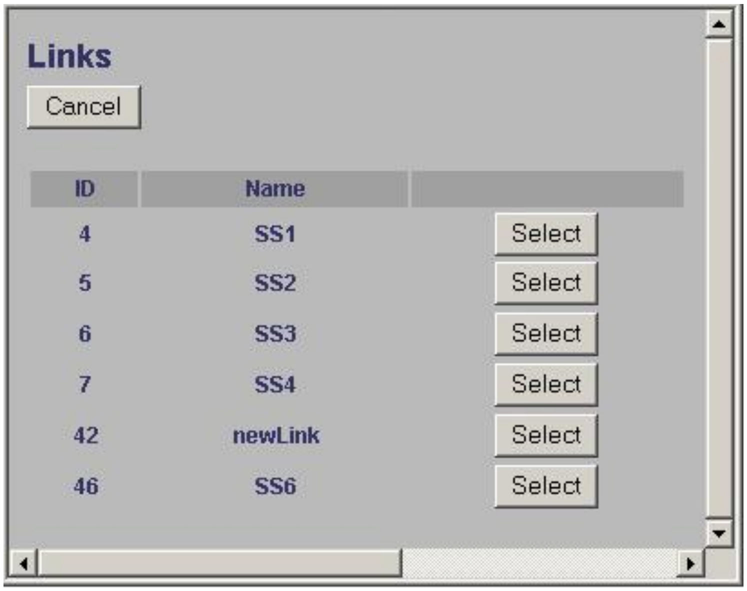
Pass-through: Classify all packets that do not have a VLAN ID, or where the outermost VLAN ID tag does not match the VLAN ID for any tagged Connection.

Connection VLAN ID: Enter the VLAN ID tag associated with this Connection definition. This field is used only when 'Tagged' is selected in the Connection Tagging Mode field.

Default priority: Enter the default 802.1p priority setting.

The default priority setting is used only when Connection Tagging Mode is 'pass-through' and the associated Group Tagging Mode is 'Tagged'. The Connection Default Priority value is 5.

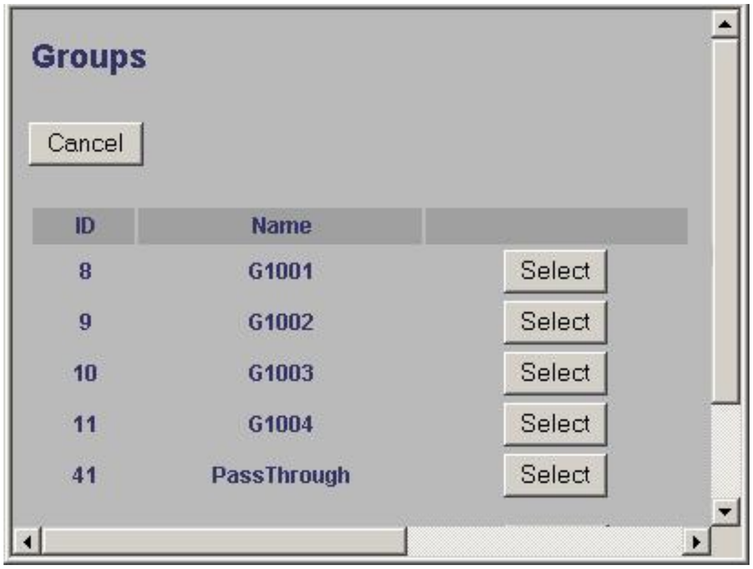
Parent Link ID: The connection is assigned to this subscriber link. Click the text **Select Link** and choose the subscriber line (click the Select button adjacent to desired link).



ID	Name	
4	SS1	Select
5	SS2	Select
6	SS3	Select
7	SS4	Select
42	newLink	Select
46	SS6	Select

Fig. 33: Web - PMP - Connection Links Selection Screen

Parent Group ID: The connection is a member of this Group. Click the text **Select Groups** and choose the required Group (click the Select button adjacent to desired group).



ID	Name	
8	G1001	Select
9	G1002	Select
10	G1003	Select
11	G1004	Select
41	PassThrough	Select

Fig. 34: Web - PMP - Connection Groups Selection Screen

Wireless Traffic Parameters

DL QoS Level: Enter the QoS level for downlink unicast traffic for this connection.

UL QoS Level: Enter the QoS level for uplink unicast traffic for this connection.

It is *strongly* recommended to calculate QoS levels using the Redline PMP Configuration Tool (contact your Redline representative to obtain a copy of this tool). The sector controller allocates bandwidth for all subscribers using the Weighted Round Robin algorithm with the combined total of all QoS levels acting as weights. The aggregate QoS settings affect packet delay and jitter values for the entire sector.

To estimate these settings, identify the maximum UL and DL burst rate required for any connection on the wireless link, and then calculate the highest available level using the formula 'Burst Rate - 1'.

DL PIR: Enter the peak information rate for downlink traffic (50 - 50000 Kbps).

UL PIR: Enter the peak information rate for uplink traffic (50 - 50000 Kbps).

The amount of data each connection transmits over the wireless interface is monitored and PIR settings are enforced. The metered interval is a common one-second (clock tick) and the statistics for all connections are reset at the beginning of each interval. If the maximum throughput is reached before the end of the current interval, that connection is excluded from sending additional data until the next clock tick.

For example, if a connection transmits its full data allocation in the first 650 ms of the current metering interval, the connection will receive no additional bandwidth allocation until the next clock tick (a forced pause of 350 ms).

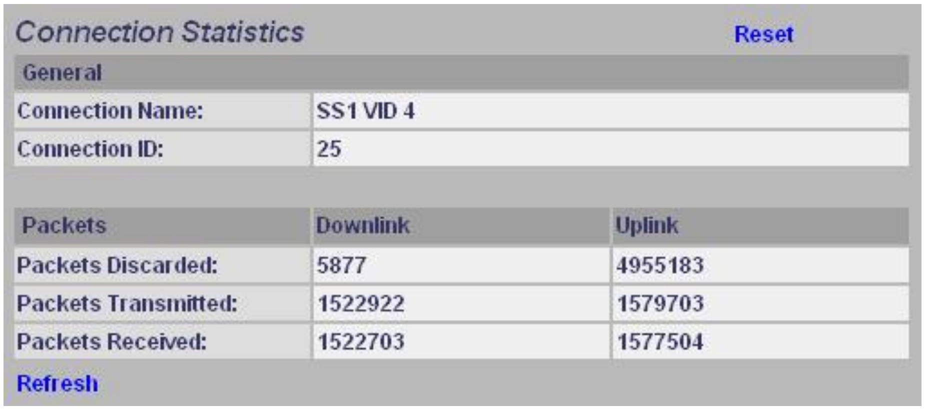
A single PIR setting is applied for each Group. When adaptive modulation is enabled, automatic adjustments to the modulation/coding will result in relative changes to the PIR of all connections using that wireless link. Incorrect PIR settings may result in excessive latency or dropped packets *(buffer full condition).*

4.10.3 Connection Statistics

The Connection Statistics screen is accessible only from the Connection browse screen (refer to 4.10.2: Connection Configuration Screen on page 61). Use the Connection Statistics screen to view statistics for all uplink and downlink traffic on the selected Connection.

Click **Links** in the main menu to locate the desired link and then click **Expand** to display the Connections browse screen. Click **Status** to display the Connection Statistics screen for a Connection.

Click **Groups** in the main menu to locate the desired Group and then click **Expand** to display the Connections browse screen. Click **Status** to display the Connection Statistics screen for a Connection.



Connection Statistics

General	
Connection Name:	SS1 VID 4
Connection ID:	25

Packets	Downlink	Uplink
Packets Discarded:	5877	4955183
Packets Transmitted:	1522922	1579703
Packets Received:	1522703	1577504

Fig. 35: Web - PMP - Connection Statistics Screen

General

Connection Name: Name assigned to this Connection.

Connection ID: Unique numeric identifier for this Connection.

Packet

Packets Discarded: Number of Ethernet packets discarded (could not be s ent over the wireless interface).

Packets Transmitted: Number of Ethernet packets transmitted over the wireless interface.

Packets Received: Number of Ethernet packets received over the wireless interface.

Controls

Reset: Click the **Reset** text (top right) to zero the statistics values.

Refresh: Click the **Refresh** text (bottom left) to update the statistics display.

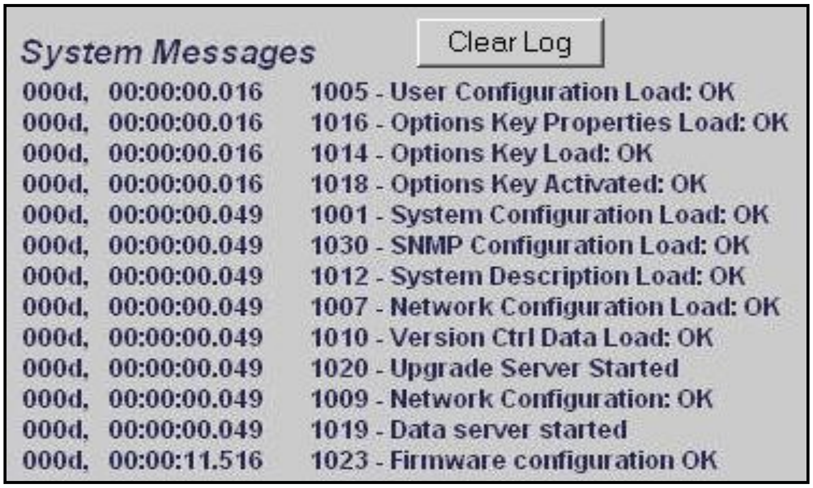
Chapter 5

5 Common Web Screens

This section describes the screens common for PTP and PMP operation.

5.1 System Log Screen

Click **System Log** in the main menu to view the system activity and error messages recorded by the AN-80i.



```
000d, 00:00:00.016    1005 - User Configuration Load: OK
000d, 00:00:00.016    1016 - Options Key Properties Load: OK
000d, 00:00:00.016    1014 - Options Key Load: OK
000d, 00:00:00.016    1018 - Options Key Activated: OK
000d, 00:00:00.049    1001 - System Configuration Load: OK
000d, 00:00:00.049    1030 - SNMP Configuration Load: OK
000d, 00:00:00.049    1012 - System Description Load: OK
000d, 00:00:00.049    1007 - Network Configuration Load: OK
000d, 00:00:00.049    1010 - Version Ctrl Data Load: OK
000d, 00:00:00.049    1020 - Upgrade Server Started
000d, 00:00:00.049    1009 - Network Configuration: OK
000d, 00:00:00.049    1019 - Data server started
000d, 00:00:11.516    1023 - Firmware configuration OK
```

Fig. 36: Web - System Log Messages

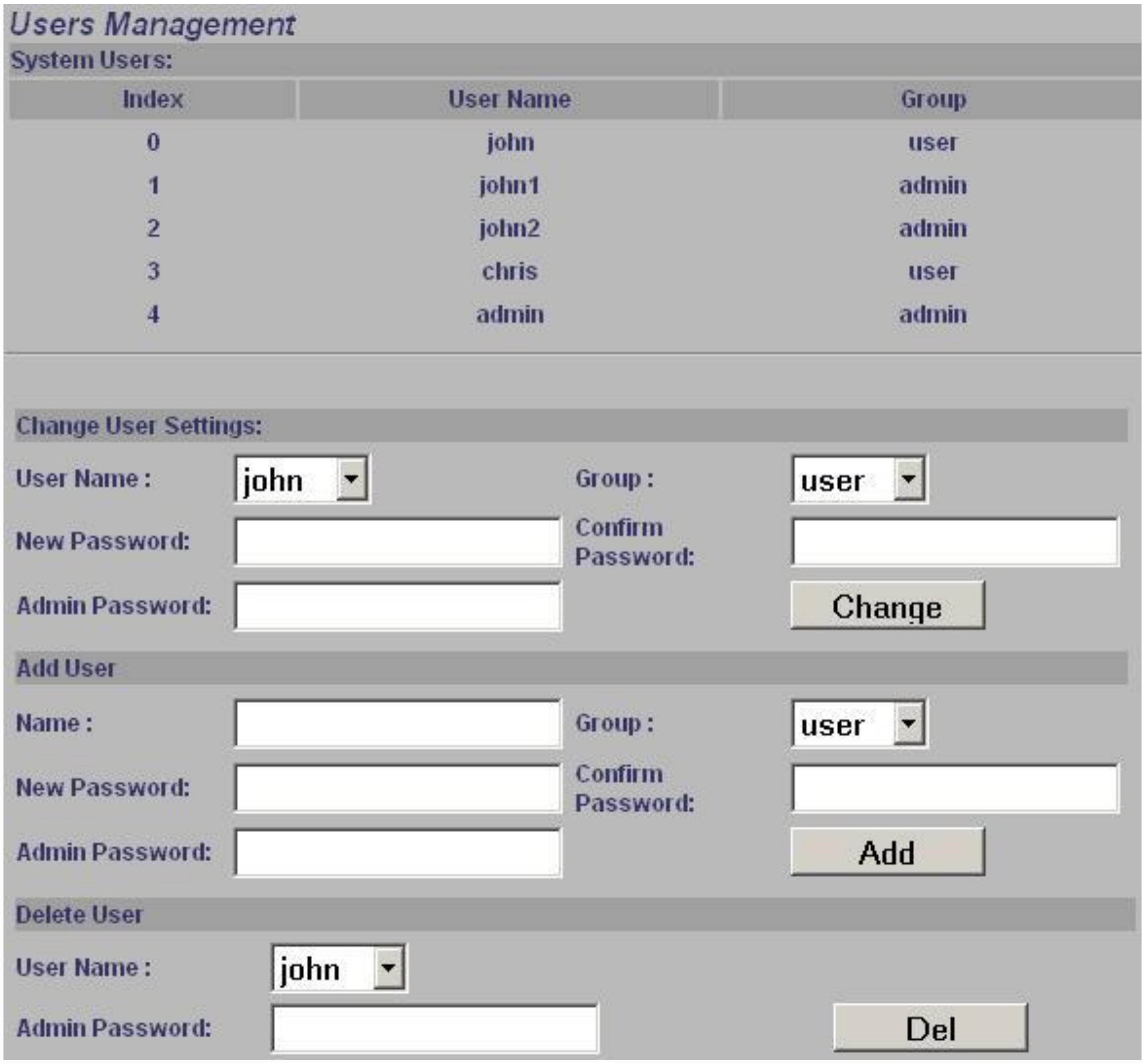
Log Controls

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

Refer to Table 52**:** Diag. - System Log Messages on page 113 for a brief description of the key system messages.

5.2 Users Management Screen

Click **Users Management** in the left hand menu to display the System Password screen. This screen allows the operator to modify the system passwords.



Users Management

System Users:

Index	User Name	Group
0	john	user
1	john1	admin
2	john2	admin
3	chris	user
4	admin	admin

Change User Settings:

User Name : john

Group : user

New Password:

Confirm Password:

Admin Password:

Add User

Name :

Group : user

New Password:

Confirm Password:

Admin Password:

Delete User

User Name : john

Admin Password:

Fig. 37: Web - System Password Screen

The AN-80i supports administrator and user accounts. See 7.5: Factory Default Settings on page 116

for the factory default login values. See Table 7**:** PTP & PMP - User Access on page 68 for permissions associated with each group.

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

> ***Important: There must always be at least one 'administrator' account active on the AN-80i. You can not manage the AN-80i if all accounts are 'user'.***

When user authentication is set to RADIUS Only or Local + RADIUS, the authorization data is retrieved from the RADIUS server at ten minute intervals. For example, if a user's authorization is changed on the RADIUS server, it may be up to ten minutes (max.) before the AN-80i is updated.

5.2.1 System Users

Index: Unique reference number (auto-generated) for this user.

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

Group: Indicates the group associated with this user. See Table 7**:** PTP & PMP - User Access table.

5.2.2 Change User Settings

Use this dialog to change the settings for an existing user.

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

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

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

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

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

Admin Password: Enter the administrator password.

Change: Click the Change button to make these changes effective.

5.2.3 Add User

Use this dialog to create a new account.

Name: Enter a name for the new user account.

Group: Select a group for the new user account. See Table 7**:** PTP & PMP - User Access table.

New Password: Enter a password for the new account.

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

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

Admin Password: Enter the administrator password.

Add: Click the Add button to create the new account.

5.2.4 Delete User

Use this dialog to delete an existing user.

User name: Select an existing user account.

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

Admin Password: Enter the administrator password.

Del: Click the Del button to make these changes effective.

5.2.5 User and Admin Account Permissions

The following table lists the permissions associated with each group.

Table 7: PTP & PMP - User Access Matrix for Web Screens

PTP	PMP SC	PMP SS	Screen	Admin Access	User Access	Description
√	√	√	General Information	X	X	View general system identification and configuration settings.
√	√	√	System Status	X	X	View system, Ethernet, and wireless statistics.
√	√	√	System Log	X	X	View the system status messages.
√	√	√	Configure System	X		View and adjust configuration system, IP address, management, and wireless settings.
√	√	√	Upload Software	X		Upload a new software binary file.
√	√	√	Users Management	X X	X	Change your login password. Add and delete users.
√	√	√	Product Options	X		View and change the product options key.
√			Spectrum Sweep	X		Scan a range of frequencies to detect other RF sources (interference).
	√	√	Links	X	X	Display user-defined Links.*
	√		Groups	X		Display user-defined Groups.*
	√		New Link	X		Create a new Link.
	√		New Group	X		Create a new Group.
	√		New Connection	X		Create a new Connection.
	√		Save	X		Save changes to ID table (Links, Groups, etc).
	√		Clear All	X		Clear all entries in the ID table.

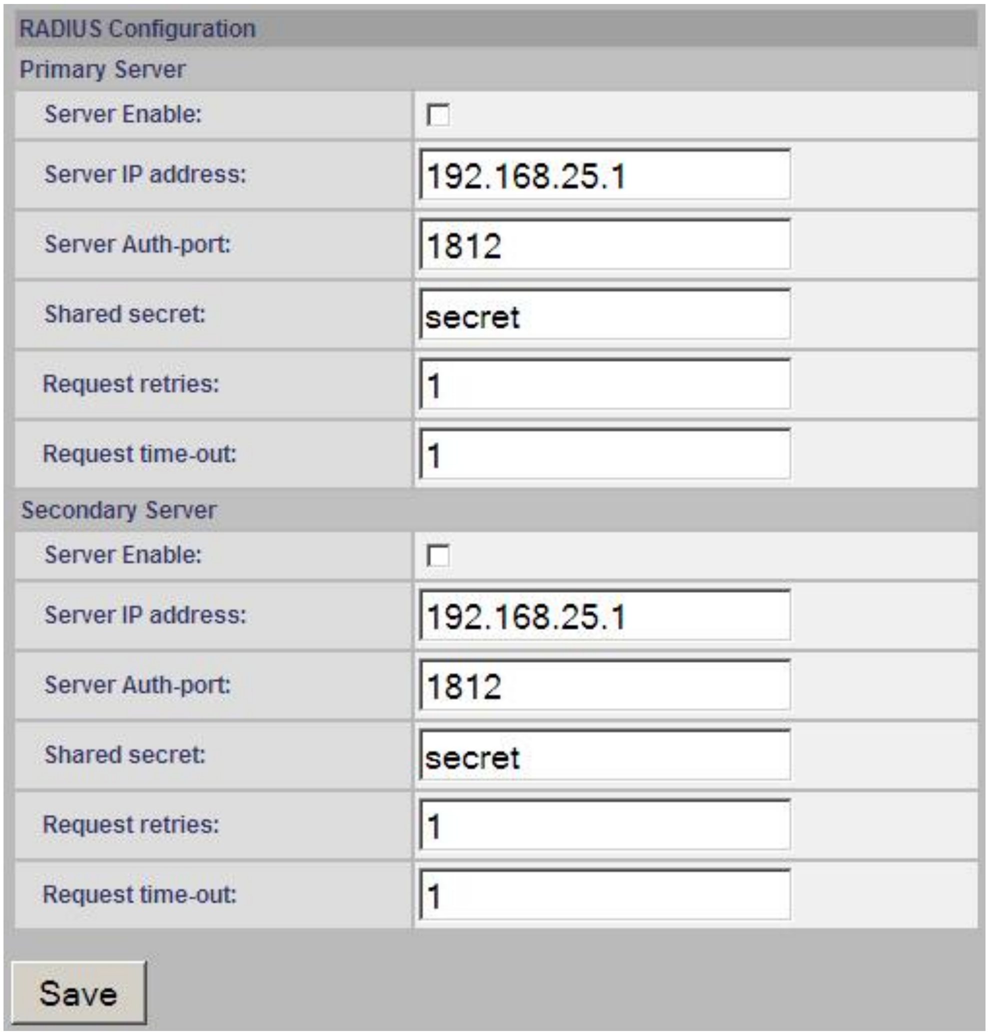
* Config and Delete options are available only to admin accounts.

5.3 Configuration Screens

The following screens are available for configuring features selected on the PTP and PMP system configuration screen.

5.3.1 RADIUS Setup Screen

When **Radius** or **Local + RADIUS** is checked on the system configuration screen, click the blue text **[Configure Radius]** adjacent to this selection to display the Radius Configuration screen.



RADIUS Configuration

Primary Server

Server Enable:	□
Server IP address:	192.168.25.1
Server Auth-port:	1812
Shared secret:	secret
Request retries:	1
Request time-out:	1

Secondary Server

Server Enable:	□
Server IP address:	192.168.25.1
Server Auth-port:	1812
Shared secret:	secret
Request retries:	1
Request time-out:	1

Fig. 38: Web - RADIUS Configuration Screen

The following fields are provided for the primary and secondary RADIUS server:

Server Enable: Check this box ☑ to enable the RADIUS server.

Server IP Address: RADIUS server IP address.

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

Shared secret: Password for RADIUS server. Must conform to security policy.

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

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

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

Table 8: PTP & PMP - Required FreeRadius Files			
Action	**File**	**File Entry**	
Define an AN-80i client.	**clients.conf**	client 192.168.0.0/16 {secret = secret shortname = AN80i }	

Add an account of type: admin	**users.conf**	admuser	Auth-Type := Local, User-Password == "abc"
			Service-Type = Administrative-User

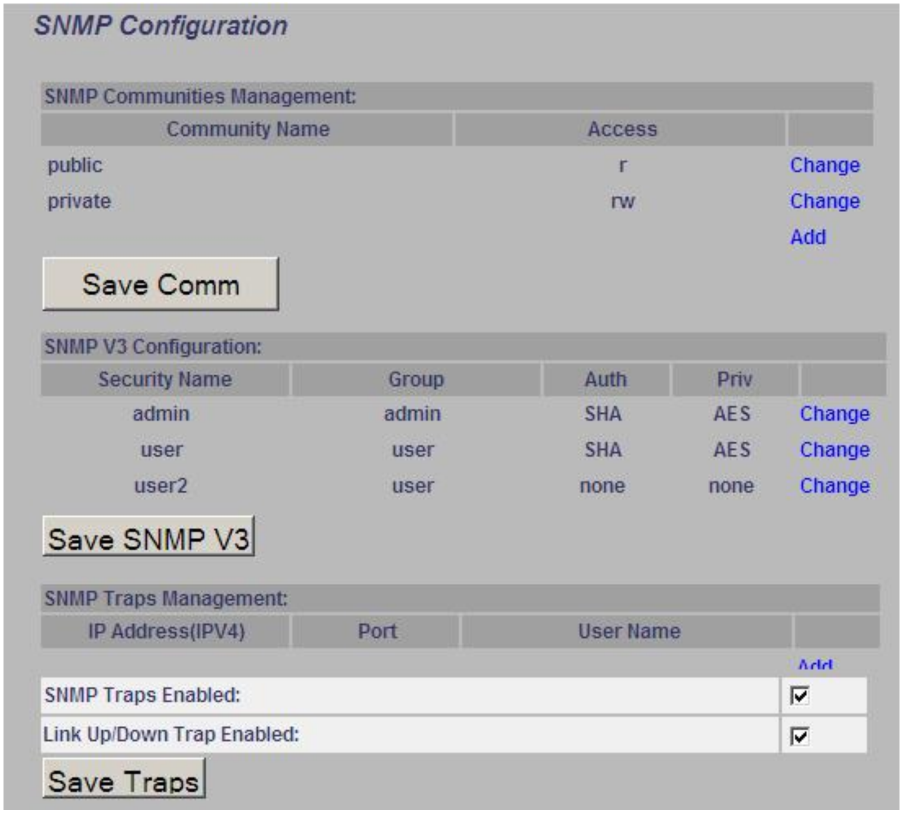
Add an account of type:user	**users.conf**	usrjoe	Auth-Type := Local, User-Password == "pass"
			Service-Type = NAS-Prompt-User

Reject an account.	**users.conf**	lameuser	Auth-Type := Reject Reply-Message = "Account has been disabled."

5.3.2 SNMP Configuration Screen

When SNMP is enabled on the system configuration screen, click **Configure SNMP** (blue text) adjacent to this selection to view and edit the SNMP settings. The hyperlink appears only if the SNMP Enable box is checked.

The SNMP protocol allows an application to interrogate information and change enabled fields within the AN-80i MIB (Management Information Base). Each section of this screen is described in detail in the following sections.



SNMP Configuration

SNMP Communities Management:

Community Name	Access	
public	r	Change
private	rw	Change
		Add

SNMP V3 Configuration:

Security Name	Group	Auth	Priv	
admin	admin	SHA	AES	Change
user	user	SHA	AES	Change
user2	user	none	none	Change

SNMP Traps Management:

IP Address(IPV4)	Port	User Name	
			Add

SNMP Traps Enabled: ☑

Link Up/Down Trap Enabled: ☑

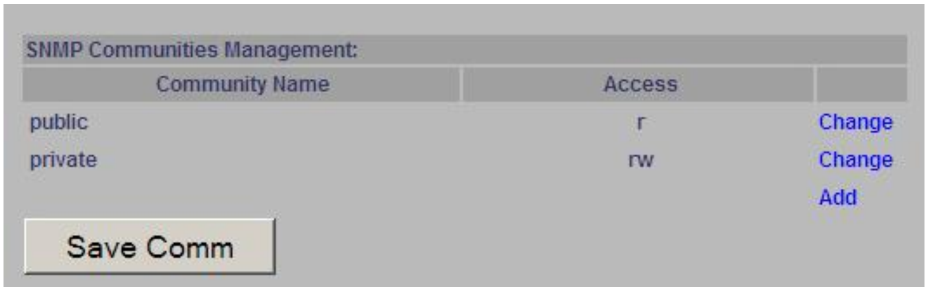
Fig. 39: Web - SNMP Configuration Screen

SNMP Communities Management

Use this section of the screen to manage the SNMP community settings. The AN-80i supports up to eight separate community strings. Community strings should be considered to be passwords. Each community name will have specific access rights (read/write). The 'public' and 'private' community strings are the default access values and should be changed to ensure secure access to AN-80 data and management functions.

SNMP Community Editor Screen

Click the **Change** or **Add** links to modify the associated SNMP settings.



SNMP Communities Management:

Community Name	Access	
public	r	Change
private	rw	Change
		Add

Fig. 40: Web - SNMP Configuration Screen - Communities Management

Community Name: Displays the SNMP community name for each entry. The AN-80i supports up to eight separate community strings.

Access: Displays the access permissions for each SNMP community.

Blank: Deny read and write permission for this community.

R: Grant read access permission only for this community. Deny write permission.

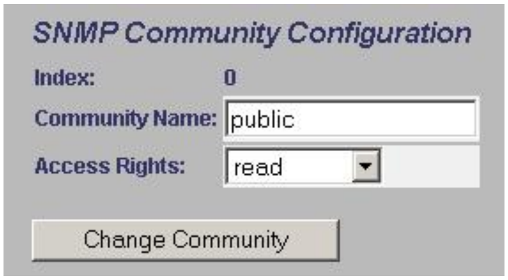
W: Grant write access permission only for this community. Deny read permission.

RW: Grant read and write access permission for this community.

Save Comm: Click to save changes to the community strings.

SNMP Community Editor Screen

Click the **Change** or **Add** links in the SNMP Configuration section of the screen for a detailed view of the SNMP community settings.



SNMP Community Configuration

Index: 0

Community Name: public

Access Rights: read

Fig. 41: Web - SNMP Configuration Screen - Communities Management Editor

Index: Display the unique reference number for this entry.

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

Access Rights: Select the access permissions for this entry.

None: Deny read and write permission for this entry.

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

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

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

Change Community: Click the Change Community button to copy these settings to the community settings table. This action does not permanently save changes. To save changes to the community settings you must also click the Save Comm button in the main SNMP Configuration screen.

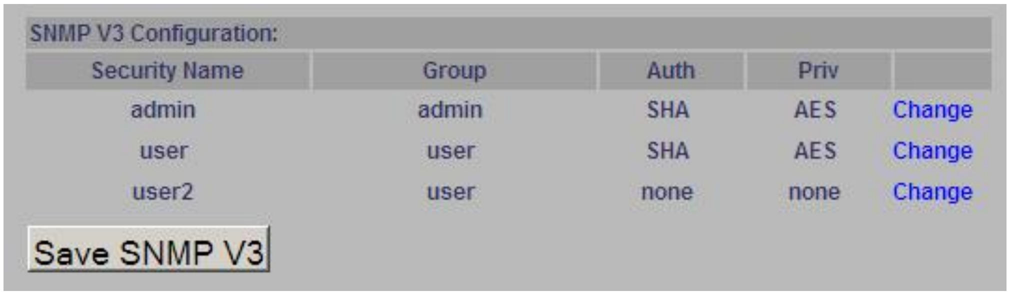
SNMP v3 Security

SNMP v3 supports authentication and privacy settings to ensure secure management when using SNMP. These security methods are associated with AN-80i user accounts.

Note: FIPS mode operation requires SHA authentication and AES privacy.

SNMP Community Security Settings

Use this section of the screen to view and modify SNMP v3 authentication and privacy.



SNMP V3 Configuration:

Security Name	Group	Auth	Priv	
admin	admin	SHA	AES	Change
user	user	SHA	AES	Change
user2	user	none	none	Change

Fig. 42: Web - SNMP Configuration Screen - v3 Configuration

Security Name: User name of account.

Group: Group association for account.

Auth: Authorization method for this account.

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

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

Priv: Privacy method for this account.

None: Deny read and write permission for this entry.

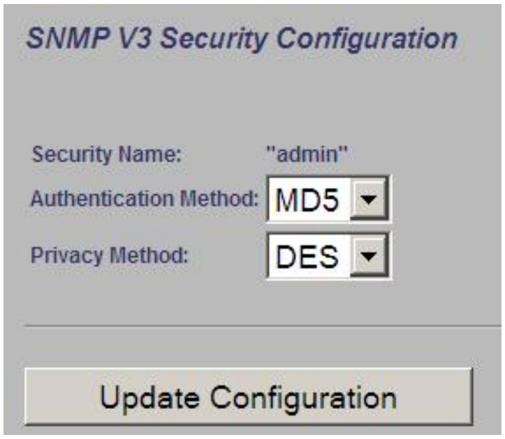
DES: DES (Data Encryption Standard) is an encryption standard.

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

Save SNMP v3: Click to save changes made in this editing screen. To save changes permanently you must also click the Save Comm button in the SNMP Configuration screen.

SNMP v3 Security Editor Screen

Click the **Change** links in the SNMP v3 Configuration section of the SNMP Configuration screen to modify these settings.



SNMP V3 Security Configuration

Security Name: "admin"

Authentication Method: MD5

Privacy Method: DES

Fig. 43: Web - SNMP Configuration Screen - v3 Configuration Editor

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

Authentication Method: Select the access permissions for this entry.

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

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

Privacy Method: Select the access permissions for this entry.

None: Deny read and write permission for this entry.

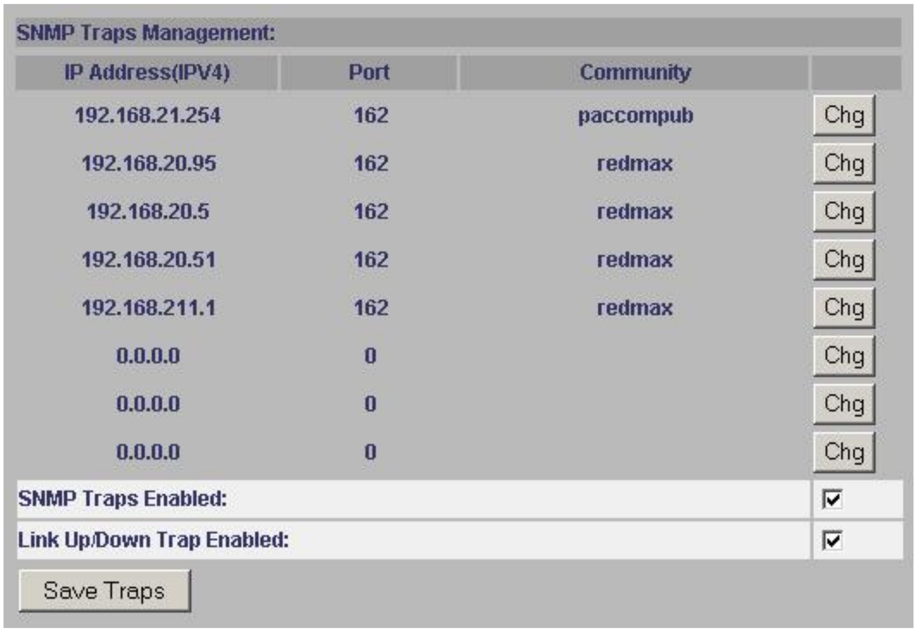
DES: DES (Data Encryption Standard) is an encryption standard.

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

Upgrade Configuration: Click to save changes made in this editing screen. To save changes permanently you must also click the Save Comm button in the SNMP Configuration screen.

SNMP Traps manageement

This section of the SNMP Configuration screen displays the SNMP trap message settings. When the SNMP Agent in the AN-80i detects an error condition, an SNMP trap message can be sent to a registered trap listener.



SNMP Traps Management:

IP Address(IPV4)	Port	Community	
192.168.21.254	162	paccompub	Chg
192.168.20.95	162	redmax	Chg
192.168.20.5	162	redmax	Chg
192.168.20.51	162	redmax	Chg
192.168.211.1	162	redmax	Chg
0.0.0.0	0		Chg
0.0.0.0	0		Chg
0.0.0.0	0		Chg

SNMP Traps Enabled: ☑

Link Up/Down Trap Enabled: ☑

Save Traps

Fig. 44: Web - SNMP Traps Management Screen

IP Address (IPv4): IP address of this trap listener.

Port: Destination port address of this trap listener.

Community: SNMP community associated with this trap listener.

Chg: Click the Chg button to modify the settings for the adjacent entry. Each of the eight entries in the SNMP Traps Management table may be changed individually.

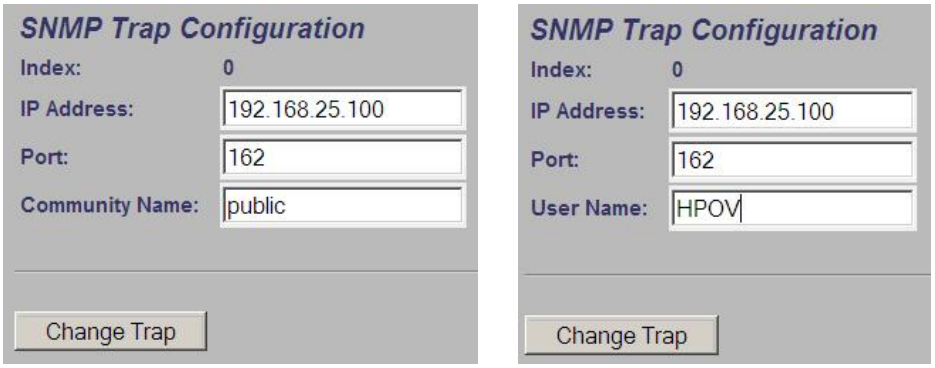
SNMP Traps Enabled: Check this box ☑ to enable SNMP traps to be sent. If the box is not checked, the AN-80i will not send any SNMP trap messages.

Link Up/Down Trap Enabled: Check this box ☑ to enable an SNMP trap to be generated when the wireless link goes offline or is restored (online).

Save Traps: Click the Save Traps button to save changes to the SNMP trap settings.

SNMP Trap Editor Screen

Click the Add button in the SNMP Traps Management section of the SNMP Configuration screen to modify the associated SNMP trap settings.



SNMP Trap Configuration

Index: 0

IP Address: 192.168.25.100

Port: 162

Community Name: public

SNMP Trap Configuration

Index: 0

IP Address: 192.168.25.100

Port: 162

User Name: HPOV

Fig. 45: Web - SNMP Traps Management - SNMP V2/V3 Editor Screens

Index: Display the table position index for this entry. Position 0 is the first entry.

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

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

Community Name: (SNMP V2) Enter the SNMP community name associated with this SNMP trap alarm.

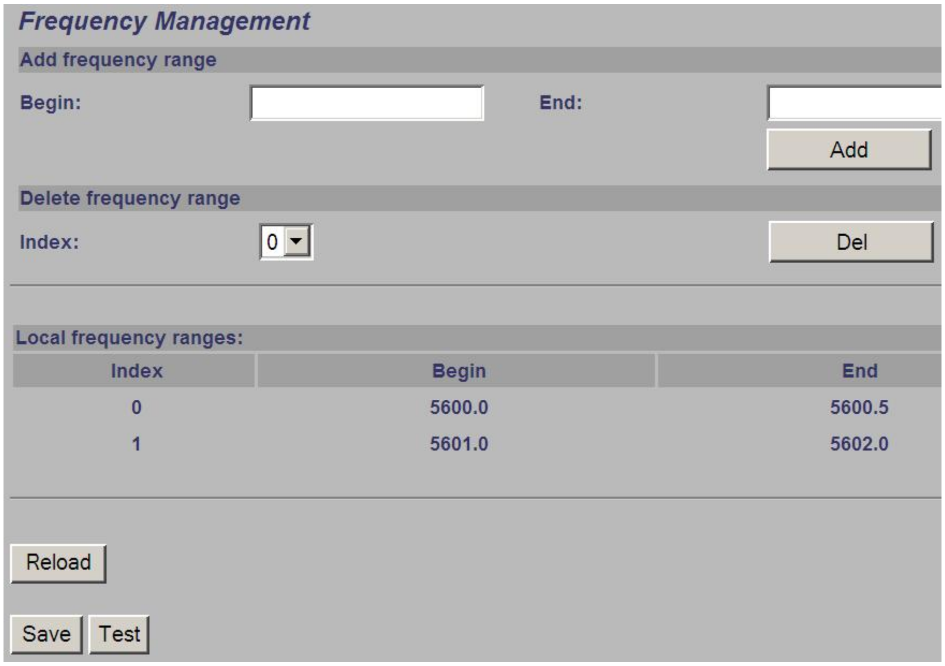
User Name: (SNMP V3) Enter the user account associated with this SNMP trap alarm.

Change Trap: Click to save changes made in this editing screen. To save changes permanently you must also click the Save Comm button in the SNMP Configuration screen.

5.3.3 Frequency Range Settings

Frequency Ranges: C

Click the blue text **Frequency Ranges** (on the system configuration screen) adjacent to the Auto Scan selection to display the Frequency Management screen. Up to 32 frequency ranges may be entered. Settings entered on the PTP Master (PMP SC) will be downloaded and used by the PTP Slave (PMP SS) if Auto scan is enabled.



Frequency Management

Add frequency range

Begin: End:

Delete frequency range

Index: 0

Local frequency ranges:

Index	Begin	End
0	5600.0	5600.5
1	5601.0	5602.0

Fig. 46: Web - Frequency Management Screen

Add Frequency Range

Begin: Enter the lower limit of the frequency scan interval (MHz). The scan interval must be a subset of the region frequency range. The unit automatically compensates for channel size when selecting the center frequency.

End: Enter the upper limit of the frequency scan interval (MHz). The scan interval must be a subset of the region frequency range. The unit automatically compensates for channel size when selecting the center frequency.

Add: Click to save the new range settings in the Local Frequency Range list. This action does not check the validity of the specified range (see Test and Save buttons at the bottom of the screen).

Delete Frequency Range

Index: Choose the index value of the scan interval to be deleted from local frequency range table.

Delete: Click the Delete button to permanently remove the selected scan interval from the local frequency range table.

Local Frequency Ranges

These settings are saved in non-volatile memory and will be loaded when the unit is rebooted.

Index: Index value of this entry in the local frequency range table.

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

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

Remote Frequency Ranges

If values have been downloaded, these settings will be used when recovering from a loss of registration. This list is not saved permanently, and is discarded when the unit is rebooted.

Controls

Reload: Reload and display the saved (Local) scan intervals. Unsaved changes are discarded.

Test: Check the validity of the current range settings in the Local Frequency Range list. This action does not save the changes. An event message is logged indicating the results of the range validation test.

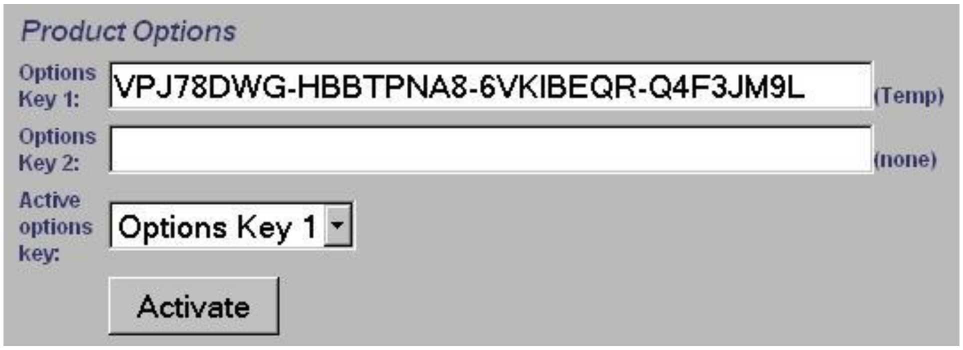
Save: Check the validity of the current range settings in the Local Frequency Range list and save these settings in non volatile memory. An event message is logged indicating the results of the range validation test.

5.4 Product Options Screen

Click **Product Options** in the left hand menu to display the Product Options screen. The options keys (a string of numbers, letters, and dashes) enable AN-80i features including the maximum uncoded burst rate and frequency ranges (region codes). Options key are unique to a specific AN-80i (keyed to MAC address).

> ***Important: If the AN-80i is placed in-service without first entering a purchased permanent options key the wireless link will experience service outages.***

At least one valid permanent options key must be purchased and installed before the AN-80i is placed in-service. A second options key (permanent or temporary key) may be added to trial new options without deleting the current key. Advance notice is provided when a temporary options key is about to expire. If the temporary options key is selected as the active key, a message is logged and an SNMP trap is generated every 6 hours during the last five days of operation.



Product Options

Options Key 1: VPJ78DWG-HBBTPNA8-6VKIBEQR-Q4F3JM9L (Temp)

Options Key 2: (none)

Active options key: Options Key 1

Activate

Fig. 47: Web - Product Options Screen

Options Key 1: Enter a valid permanent options key. A permanent options key must be entered for in-service operation.

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

Active Options Key: Use this field to select the preferred key. This selection remains in effect when switching software versions. If the selected options key expires or becomes invalid (e.g., changing mode PTP -> PMP), the AN-80i will automatically switch to the standby key (if available and valid for the new mode).

> ***Important: To prevent a service outage on the wireless link, always enter and activate a permanent options key before any temporary key expires.***

Activate: Click the Activate button to validate, save, and activate new options keys or to change to the Active Options Key setting. Both options keys are checked when the Activate button is clicked. Invalid keys are discarded and an error message is recorded in the event log.

> ***Important: If new option keys values are entered for Options key 1 and 2 in the same session (before clicking Activate), these values are saved only if both keys are valid.***

Notes:

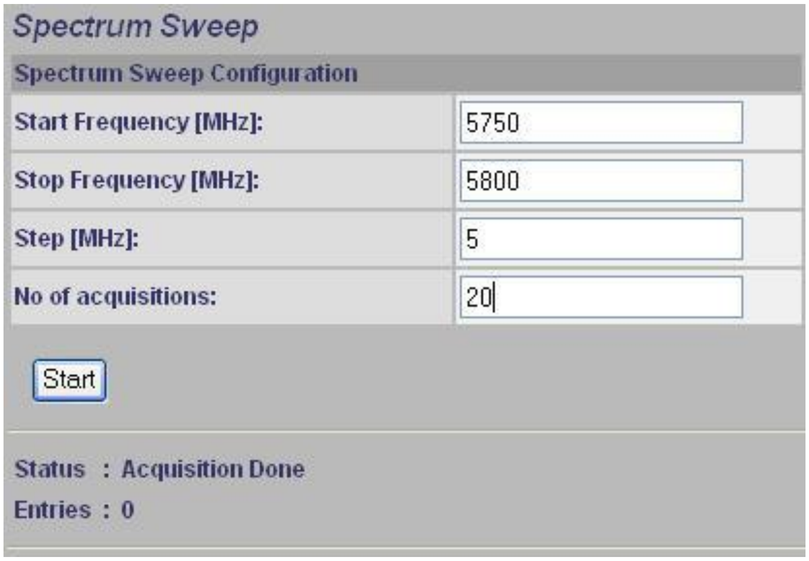
1. Keys are shared between PMP and PTP operation.
2. PTP mode has the following restricted operation when both options keys are invalid: 10 MHz channel, 3 Mbps UBR, DFS permanently enabled, region based common frequency range, no enhanced options (e.g., AES).
3. A valid options key must be entered to enable PMP mode operation.

5.5 Spectrum Sweep Screen

5.5.1 Overview

Use the AN-80i **Spectrum Sweep** feature to determine if RF spectrum is free from interference. Configurable survey settings allow you to scan a specific frequency range -- specifying both the step size and the number of samples at each step. When the sweep is completed, an output graph displays the average (blue) and maximum (red) RSSI measured at each sample step.

Click **Spectrum Sweep** in the left hand menu to display the Spectrum Sweep configuration screen. Configurable survey parameters include the high and low frequency limits, the step size, and the number of samples at each step. The output graph displays the maximum (red) and average (blue) RSSI for each step.



Spectrum Sweep

Spectrum Sweep Configuration	
Start Frequency [MHz]:	5750
Stop Frequency [MHz]:	5800
Step [MHz]:	5
No of acquisitions:	20

Status : Acquisition Done

Entries : 0

Fig. 48: Web - Spectrum Sweep Screen

Start Frequency (MHz): Enter center frequency of the lowest channel to be scanned. See Table 73: Spec. - Regional Identification Codes on page 144.

End Frequency (MHz): Enter center frequency of the highest channel to be scanned. See Table 73: Spec. - Regional Identification Codes on page 144.

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

No. of acquisitions: Enter the number of times the frequency will be sampled at each step. The recommended range is 10 to 100 samples. When a potentially clear channel is identified, reduce the frequency range and step size while increasing the sample size to monitor the channel over a longer period.

Start: Left-click the Start button to begin the scan.

5.5.2 Example: Performing a Sweep

1. Prepare the AN-80i:

   For PTP Masters or PMP Sector Controllers, t he transmitter is automatically disabled during the sweep.

   To run a sweep from a PTP Slave or PMP Subscriber location, the remote unit transmitter must be disabled for the duration of the test.

Hint: Login to the remote PTP Master or PMP sector controller, uncheck (□) the Radio Enable setting, and click Test. The radio will be disabled and the wireless link will be lost. The radio is automatically re-enabled after approximately 5 minutes.

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

    12. For example:

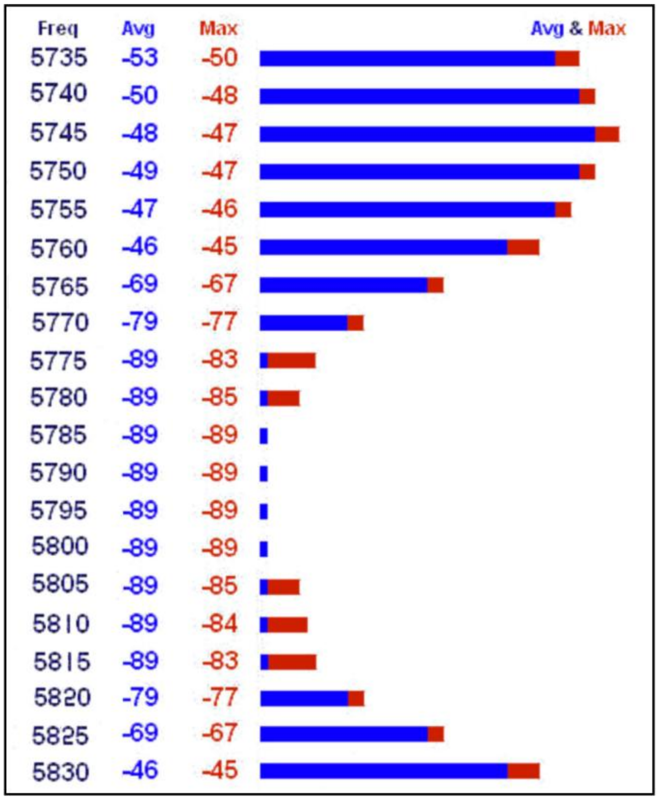
    13. *Start/Stop = 5735 / 5830*

    14. *Step [MHz] = 5*

    15. *No. of Acquisitions = 10*

3. Click the Start button to begin the sweep.

    16. When the sweep has completed, review the results. A channel may be considered 'available' when free of interference for at least +/- one-half the channel bandwidth from the desired center frequency. For example, a 20 MHz channel should have no interference detected for at least +/- 10 MHz from the candidate channel.

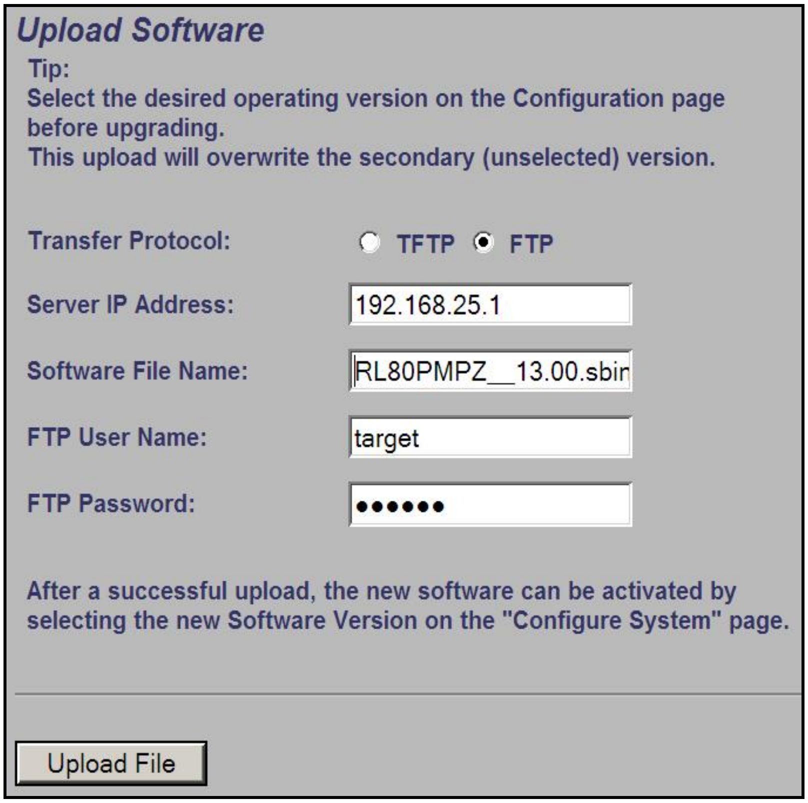


Freq	Avg	Max
5735	-53	-50
5740	-50	-48
5745	-48	-47
5750	-49	-47
5755	-47	-46
5760	-46	-45
5765	-69	-67
5770	-79	-77
5775	-89	-83
5780	-89	-85
5785	-89	-89
5790	-89	-89
5795	-89	-89
5800	-89	-89
5805	-89	-85
5810	-89	-84
5815	-89	-83
5820	-79	-77
5825	-69	-67
5830	-46	-45

Fig. 49: Web - Spectrum Sweep Example Results

5.6 Upload Software Screen

Click **Upload Software** in the left hand menu to display the Upload Software screen. This screen is used to upgrade the AN-80i with new software. The AN-80i contains non-volatile storage for two versions of the software. The upload overwrites the non-operational (unselected) version.



Upload Software

Tip:
Select the desired operating version on the Configuration page before upgrading.
This upload will overwrite the secondary (unselected) version.

Transfer Protocol: ○ TFTP ● FTP

Server IP Address: 192.168.25.1

Software File Name: RL80PMPZ__13.00.sbir

FTP User Name: target

FTP Password: ●●●●●●

After a successful upload, the new software can be activated by selecting the new Software Version on the "Configure System" page.

Fig. 50: Web - Upload Software Screen

Transfer Protocol: Select the type of server:

TFTP: Use Trivial File Transfer Protocol for file upload.

FTP: Use File Transfer Protocol for file upload.

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

Software File Name: Name of the software binary file (including file extension).

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

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

Upgrade Steps

A TFTP or FTP server must be installed and running on the computer being used to upload the new software file. The AN-80i software binary file must be located in the default upload directory of the TFTP/FTP server.

Login to the AN-80i Web interface and perform the following steps:

1. Click on Upload Software in the main menu (left side of screen).
2. Select TFTP or FTP and enter the IP Address of the computer running the server.
3. Enter the full name of the binary file (including the .bin extension).

4. Click Upload File to begin the file transfer. The transfer and saving operation may require up to eight minutes based on the data transfer rate. Do not interrupt the transfer process.
5. When the transfer is complete, the AN-80i checks the integrity of the uploaded file and registers a status message in the event log. If the upload is completed successfully, the following message is displayed on the screen:

   17. ***Upgrade Status: Ended successfully***
   18. If errors were introduced during the transfer process, the software file is discarded and the upload must be repeated.
6. When the transfer has completed successfully, use the System Configuration screen to select the software version to load on the next system reboot.

Digitally Signed Software Binary Files

New security features for uploading software have been introduced beginning with PTP v4.00. If a signed software binary is uploaded into both AN-80i software banks, it will not be possible to upload a previous version of software that is not digitally signed.

With the introduction of FIPS 140-2 level 2 security software, the AN-80i is permitted to upload only digitally signed software files (*.sbin). The use of signed software binary files provides enhanced security for all operators by verifying the authenticity of the software binary file, and that the file has not been altered in any way.

The restriction to load only digitally signed files prevents the uploading of unsigned versions of PTP or PMP software while FIPS-enabled software is active on the AN-80i. This restriction is a new general security feature and is not affected by the status of the FIPS option.

This restriction does not affect switching between the two software banks on the AN-80i. For example, after uploading and executing FIPS-capable software, use the following steps to upload an unsigned software binary file:

1. Go to the Configuration screen and select the non FIPS-capable software version (e.g., PTP v3.nn, or PMP v12.nn). Click Save and then reboot the AN-80i.
2. When the AN-80i completes the reboot cycle, use the Upload Software screen to load the desired unsigned software binary file. The uploaded file will overwrite the inactive software bank.

If you are unable to resolve an operating issue resulting from this upload restriction contact Redline customer support for assistance.

6 CLI Interface

This section describes the procedures for configuring and operating the AN-80i using CLI over a Telnet Connection. All commands are case-sensitive. Use the following general format:

command <Enter>

Online help is available for all commands, and the Tab key can be used for auto-complete functions. The following table lists all AN-80i commands available from root mode (default mode when you login).

Table 9: CLI - Command Summary

PTP	PMP	Command	Description
√	√	**arp**	Add static ARP definitions to the AN-80i ARP table.
√	√	**chgver**	Change default version of software and reboot.
√	√	**clear**	Clear commands.
√	√	**del**	Delete an ID.
	√	**enable**	Enable an ID.
√	√	**freq**	Enter frequency ranges for autoscan and DFS.
√	√	**generate**	Create DSA key for SSH locally on AN-80i.
√	√	**get**	Display the value of a statistic or parameter.
√	√	**load**	Load commands.
√	√	**logout**	End the current Telnet session.
	√	**new**	Create a new ID.
√	√	**ping**	Send a ping message from the AN-80i system.
√	√	**reboot**	Reboot the AN-80i.
√	√	**reset**	Reset the AN-80i statistics values.
√	√	**save**	Save the selected configuration settings.
√	√	**script**	Generate a configuration script.
√	√	**set**	View/modify a system parameter value.
√	√	**show**	View system compound objects (e.g., configuration).
√	√	**snmpcommunity**	View/modify the SNMP community settings.
√	√	**snmptrap**	View/modify the SNMP trap settings.
√	√	**test**	Activate edited changes to the system configuration for a test period of five minutes.
√	√	**upgrade**	Upload a software binary image to the AN-80i.
√	√	**user**	View/modify the user/password configuration.
	√	**whoami**	Display login name for this Telnet session.

Table 10: CLI - Root Mode Commands

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

6.1 Command Set

6.1.1 Arp

Use the ***arp*** command to manually (e.g., for wireless link aggregation). A maximum of two static (persistent) entries can be added to the table. Use the 'save config' command to permanently save changes to the static entries in the ARP table. Static entries loaded at boot time are recorded in the AN-80i system log.

Table 11: CLI - arp

arp <add> <del> <print>

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

Add a new static entry in the AN-80i ARP table. Use 'save config' to save these entries permanently. A maximum of two static entries can be added to the table.

Host	Host IP address. Must be same subnet as AN-80i unit.
MAC	Host MAC address (e.g., 01-02-03-04-05-06)

del **<Host>**

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

Host: Host IP address of ARP entry to be deleted

print

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

For example:

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

6.1.2 Chgver

Use the ***chgver*** command to change the software version loaded when the AN-80i is rebooted.

Table 12: CLI - chgver
Use this command to switch to alternate software version.
chgver (no options)
Switch to the binary saved in the alternate version of software. This command works silently (no operator confirmation) and the AN-80i reboots immediately.
Note: Use 'get swver' to list the active and alternate versions of software.

6.1.3 Clear

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

Table 13: CLI - clear
Enter this command to delete all contents from a data structure.
clear <arptable> <freqlist> <idtable> <log>
arptable
Delete all static entries in the ARP table (refer to arp).
freqlist
Delete all frequency ranges from list (refer to 'freq' command).
idtable
Delete all IDs from the idtable (PMP only).
log
Delete all messages from the log.

6.1.4 Del

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

Table 14: CLI - del	
Delete file information from the AN-80i non-volatile memory.	
del <file> <folder> <id>	
file <name> <mode>	
Remove a file from flash and runtime memory.	
name <filename>	
File name on server. File name must be one of the following:	
dsa_key_<mac>.pem	DSA key used for SSH.
rsa_key_<mac>.pem	RSA Key used for SSH.
ssl_cert_<mac>.pem	SSL Certificate.
ssl_key_<mac>.pem	SSL Key.
usr_wcert_<mac>.der*	User wireless certificate.
usr_wkey_<mac>.der*	User wireless key.
usr_wacert_<mac>.der*	User wireless authority certificate.
The <mac> portion is the MAC address of the board. For example: dsa_key_00-09-02-00-01-02.pem	
RSA is not used for SSH Connections in v4.00 and higher.	

Table 14: CLI - del

mode <usr | factory | fips>

Specify the type of information to display.

usr User entered files (default if type is not specified).

factory Factory default files (requires hardware jumper selection).

fips FIPS mode files. Refer to page 118 for a complete description of this feature.

id <id>

Remove a Group, Connection, or Link table entry.

id Unique number for Group, Connection, or Link.

folder <usr | factory | fips>

Remove all files from the specified table.

usr - User entered files (default).

factory - Factory use only.

fip - FIPS mode files. Refer to page 118 for a complete description of this feature.

6.1.5 Enable

Use the ***enable*** command to enable a specific ID (that was disabled). Available only with PMP.

Table 15: CLI - enable

Enable a group, connection, or link id (PMP only).

enable <id>

Enable a specific ID.

id Unique number for group, connection, or link.

6.1.6 Freq

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

Table 16: CLI - freq

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

add

Add a frequency range (up to 32 ranges).

begin - start frequency (MHz)

end - end frequency (MHz)

clearall

Delete all entries from the frequency list.

del <idx>

Delete a frequency validation range

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

print

Print the list of frequency validation ranges.

Local frequency ranges:

<index> <begin> <end>

reload

Reload the active list of frequency validation ranges.

6.1.7 Generate

Use the ***generate*** command to generate a DSA or RSA key for use with SSH.

Table 17: CLI - generate

Create keys of the specified type. The keys are saved in flash and runtime memory.

generate <sshkey>

The AN-80i will generate a key using its own encryption engine.

sshkey <dsa | rsa>

dsa Generate DSA key for SSH.

rsa Generate RSA key for SSH (not used in v4.00 and higher).

Note: RSA is not used for SSH connections in v4.00 and higher.

6.1.8 Get

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

Table 18: CLI - get (Common commands for PTP and PMP)

Display PTP parameters.

get <*parameter*>

datalink: Status of the data Link (LED).

0 - Data Link is not active (AN-80i can not send user data).

1 - Data Link is active (AN-80i is able to send user traffic).

erxpkt: Number of Ethernet packets received.

erxpktd: Number of Ethernet packets received that were discarded.

ethsts: Speed and duplex settings for the Ethernet port.

etxpkt: Number of Ethernet packets transmitted.

fipsstatus: Status of FIPS parameters (FIPS mode only). Refer to page 118 for a complete description of this feature.

mac: AN-80i MAC address.

pskey <key> Encryption key.

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

radiotype: Radio type.

rffreq: RF frequency setting.

rfstatus: Status RF transmitter.

swver: List the downloaded software versions.

sysuptime: Display the time since the last reboot.

txpower: Current Tx power setting.

Table 19: CLI - get (PTP-Specific Commands)

Display PTP parameters.

get <*parameter*>

calcdst: Calculated Link distance between units.

linkid: ID value -- unique value generated whenever wireless Link is established.

Table 19: CLI - get (PTP-Specific Commands)

radiotemp: Radio temperature.

rflink: Link ID.

rfstatus: Status RF transmitter.

rssimax: Maximum RSSI.

rssimean: Mean RSSI.

rssimin: Minimum RSSI.

sinadr: Ration of signal to interference + noise.

txstatus: State of the wireless interface (FIPS mode only.). Radio is disabled on failure of any security check (hardware, firmware, software).

- **Off** - Wireless security has disabled the transmitter.
- **On** - Wireless security has enabled the transmitter.

ubrate: Current UBR value.

wrxpkt: Number of wireless packets received.

wrxpktd: Number of wireless packets received that were discarded.

wrxpktr: Number of wireless packets that were retransmitted.

wsstatus: Status of the wireless security.

- **0** - Wireless security is disabled.
- **1** - Wireless security is enabled.

wtxpkt: Number of wireless packets transmitted.

wtxpktd: Number of wireless packets transmitted that were discarded.

wtxpktr: Number of wireless packets that were retransmitted.

Table 20: CLI - get (PMP-Specific Commands)

Display PMP parameters.

get <parameter>

activeids: Number of active IDs.

activelinks: Number of the active Links.

dldpkt: Number of downLink discarded packets.

dlrpkt: Number of downLink Rx packets counter.

dltpkt: DownLink Tx packets counter.

idenable: ID status.

lactive: Link active status.

ldlblk: DownLink total blocks counter.

ldlbr: DownLink burst rate.

ldldblk: DownLink discarded blocks counter.

ldllfr: DownLink lost frames counter.

ldlrblk: DownLink retransmitted blocks counter.

ldlrssi: DownLink RSSI.

ldlsnr: DownLink SINADR.

llostc: Link lost Connection counter.

Table 20: CLI - get (PMP-Specific Commands)
lrcon: Number of Link registered Connections.
lscode: Link status code.
lulblk: UpLink total blocks counter.
lulbr: UpLink burst rate.
luldblk: UpLink discarded blocks counter.
lullfr: UpLink lost frames counter.
lulrblk: UpLink retransmitted blocks counter.
lulrssi: UpLink RSSI.
lulsnr: UpLink SINADR.
luptime: Link up-time.
regconn: Number of configured Connections.
regstations: Number of configured stations.
sysstarttime: Time when the system started.
uldpkt: UpLink discarded packets counter.
ulrpkt: UpLink Rx packets counter.
ultpkt: UpLink Tx packets counter.
werxpkt: Wireless Eth Rx packets counter.
werxpktdis: Wireless Eth Rx discarded packets counter.
werxpkterr: Wireless Eth Rx packets with errors counter.
wetxpkt: Wireless Eth Tx packets counter.
wetxpktdis: Wireless Eth Tx discarded packets counter.
wetxpkterr: Wireless Eth Tx packets with errors counter.

6.1.9 Load

Use the ***load*** command to load information to the AN-80i.

Table 21: CLI - load	
Load stored information from non volatile ram or a remote server.	
load <file> <idtable> <script>	
file <server IP> <filename> <usr | factory | fips> <tftp | sftp> <user> <password>	
Load a key or certificate file from FTP server. The file will be saved in flash RAM area. A reboot is required to activate changes to security data.	
The filename must be one of the following:	
dsa_key_<mac>.pem	DSA key used for SSH.
rsa_key_<mac>.pem*	RSA Key used for SSH.
ssl_cert_<mac>.pem	SSL Certificate.
ssl_key_<mac>.pem	SSL Key.
usr_wcert_<mac>.der**	User wireless certificate.
usr_wkey_<mac>.der*	User wireless key.
usr_wacert_<mac>.der*	User wireless authority certificate.
The <mac> portion is the MAC address of the board.	

Table 21: CLI - load

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

* RSA is not used for SSH Connections in v4.00 and higher.

** Not used in v3.00 software release.

Specify where to store the security information.

usr User entered files (default if type is not specified).

factory Default files.

fips FIPS mode files.

For example:

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

idtable (no parameters)

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

script <server IP> <filename>

Use this command to load the AN-80i configuration information from a file (created using script command) located on a remote TFTP server. The file must be located in the TFTP default directory. The 'save config' command must be used to save the loaded configuration in non volatile memory. A reboot may be required to activate the loaded configuration settings.

For example:

load script 192.168.25.10 AN80i-Unit035-091121.cfg

Note: Beginning with v13.00:

i) All Links, Groups, and Connections must be within the prescribed ranges. Refer to Table 78: Spec. - Provisioning Table ID Ranges on page 149.

ii) The 'load script ...' command rejects all ID references greater than 511.

6.1.10 Logout

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

Table 22: CLI - logout

End the current Telnet session.

logout

Terminate the current Telnet session (no parameters).

6.1.11 New

Use the ***new*** command (PMP only) to create a new Link, Group, or Connection.

Table 23: CLI - new

Create a new link, group, or connector (PMP only).

new <conn> <group> <link>

conn <id>

Create a new connection ID.

id - Specify a unique ID for this connection:

group <id>

Create a new group ID.

id - Specify a unique ID for this group:

link <id>

Create a new link ID.

Table 23: CLI - new
id - Specify a unique ID for this link:

6.1.12 Ping

Use the ***ping*** command to initiate an ICMP ping command from the AN-80i.

Table 24: CLI - ping
Send an ICMP ping command. This can be used to confirm network access to FTP/TFTP servers, syslog servers, etc. **ping <IP address> <Number of Packets>** **IP address** IP address of target. **Number of Packets** Number of ICMP packets to send (1 to 16).

6.1.13 Reboot

Use the ***reboot*** command to reboot the AN-80i software.

Table 25: CLI - reboot
Command the AN-80i to reboot. Entering 0 (zero) cancels reboot in-progress. **reboot <seconds>** **seconds** Number of seconds to wait before rebooting.

6.1.14 Reset

Use the ***reset*** command to zero the AN-80i statistics or ID table.

Table 26: CLI - reset
Reset AN-80i values. **reset <stats>** Enter ID of specific Connection, Group, or Link to be reset. **stats <id>** Reset statistics for a Connections, Groups, and Links. **id** - Specify an ID to reset statistics only for that Connection, Group, or Link. Default is to reset all statistics (PMP only).

6.1.15 Save

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

```
save [option] <Enter>
```

Table 27: CLI - save
Copy parameters to non-volatile memory. Does not affect security settings. **save <config> <defaultconfig> <idtable> <snmp>** **config** Save Ethernet, wireless, and user configuration settings. **defaultconfig** Overwrite parameters with the factory default settings. The following settings are not affected: system name, location, details and contact, frequency list, SNMP configuration,

Table 27: CLI - save

Idtable (PMP only).

idtable

Save current idtable settings (PMP only).

snmp

Save current SNMP settings.

6.1.16 Script

Use the ***script*** command to save a file containing a string of Commands that can be used to restore the current (active) configuration of the AN-80i. Saved configuration files can be viewed, copied, and/or modified using a text editor.

The file will be saved in the TFTP default directory. The filename may be any name and extension valid for the TFTP server platform. It is recommended use a filename that uniquely identifies the AN-80i unit and the current date (e.g., Red80-AD0023-080723.cfg). See 'load' command.

Table 28: CLI - script

Create and save a script file containing all configuration settings.

script <server> <name>

server - TFTP server IP address

name - Script file name

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

6.1.17 Set

Use the ***set*** command to view and/or change a parameter.

Table 29: CLI - set (Common for PTP and PMP)

View and change general parameter settings.

set <parameter>

activekey <1 | 2> <key>

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

key - Optionally enter a new key value.

adaptmod <off | on>

Enable or disable the adaptive modulation function.

off - Disable

on - Enable

antgain <gain>

Set the antenna gain (used for DFS).

<gain> Enter gain in dBm.

autoscan <off | on>

Table 29: CLI - set (Common for PTP and PMP)

Enable or disable the Autoscan function.

off - Disable

on - Enable

When enabled, the PTP Subscriber (system mode) AN-80i automatically scans available channels to locate the current operating frequency of the PTP Sector Controller system. Executing a set command this field on a PTP Sector Controller will generate an error message.

buzzer <off | on>

Enable or disable the audible alignment buzzer.

off - Disable

on - Enable

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

chwidth <bandwidth>

Enter the channel bandwidth (enabled by options key).

bandwidth Enter bandwidth in MHz (e.g., 40).

dfsaction <none | txoff | chgfreq>

Select the mode of operation for DFS.

None (0): The DFS function is disabled.

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

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

encmode <0 - 4>

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

0 - Disable

1 - 64-bit (Redline)

2 - AES 128

3 - AES 192

4 - AES 256

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

Enter a value for the combined Ethernet speed and duplex.

auto - Auto-negotiate

10hd - 10Base-T Half Duplex

10fd - 10Base-T Full Duplex

100hd - 100Base-T Half Duplex

100fd - 100Base-T Full Duplex

fipsmode <off | on>

Enable or disable FIPS mode operation. In FIPS mode, only FIPS approved algorithms are used for SSH, HTTPS and wireless security. Refer to page 118 for a complete description of this feature. In FIPS mode, only FIPS approved algorithms are used for SSH, HTTPS and wireless security.

off - Disable FIPS mode.

Table 29: CLI - set (Common for PTP and PMP)

on - Enable FIPS mode.

gateway <ip>

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

gmt <value>

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

http <off | on>

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

off - Disable

on - Enable

https <off | on>

Enable or disable the HTTPS function.

off - Disable

on - Enable

ipaddr <ip> <mask>

Enter the IP address and subnet mask of the AN-80i. Confirmation is required.

Example:

set ipaddr ip 192.168.100.10 mask 255.255.255.0

lkname <text>

Enter the name of the remote unit (maximum 15 characters).

maxtxpower <-10 - 25>

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

mgmtag <off | on>

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

off - Do not use VLAN to identify management traffic.

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

mgmvid <1 - 4095>

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

vlan_id - Management VLAN ID.

netmask <mask>

AN-80i IP netmask in standard format.

For example: set netmask 255.255.255.0

optionskey <key> <1 | 2>

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

peermac <MAC>

MAC address of the communicating AN-80i. Required for wireless encryption. Use form: aa:bb:cc:dd:ee:ff

radio <off | on>

Enable or disable the radio transmitter.

off - Disable

Table 29: CLI - set (Common for PTP and PMP)

on - Enable

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

Configure the RADIUS server (allowed in FIPS mode).

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

ip <1 | 2> <IP address>

IP address of RADIUS server.

1 - Primary RADIUS server.

2 - Secondary RADIUS server.

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

set radius ip 1 192.168.100.50

set radius ip 2 192.168.100.51

mode <1 | 2> <off | on>

Mode of RADIUS server.

off - Disable RADIUS server.

on - Enable RADIUS server.

port <1 | 2> < 1-9999 >

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

retries <1 | 2> < 1-999 >

Maximum number for attempts to contact target RADIUS server.

secret <1 | 2> < text >

Password for RADIUS server. Must conform to security policy.

timeout<1 | 2> < 1- 90 >

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

rffreq < 3.5 - 40>

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

snmp < off | on>

SNMP enable setting.

off - Disable the SNMP agent.

on - Enable the SNMP agent.

snmptraplink < off | on>

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

off - Disable the SNMP trap message.

on - Enable the SNMP trap message.

snmptraps < off | on>

Enable or disable sending all SNMP traps.

off - Disable all SNMP trap messages.

on - Enable all SNMP trap messages.

sntp < off | on>

SNTP enable setting.

off - Disable SNTP protocol support.

on - Enable SNTP protocol support.

sntpip <ip>

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

Table 29: CLI - set (Common for PTP and PMP)

sntppoll <1 - 24>

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

ssh <off | on>

Enable or disable the SSH function.

off - Disable

on - Enable

syscontact <text>

Enter additional descriptive details about this AN-80i. Enter up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

sysdescr <text>

Details about this AN-80i. Enter up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

sysloc <location>

Enter descriptive details about the location of this AN-80i location**.** Enter up to thirty (30) alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_).

syslog <off | on>

Syslog enable setting.

off - Disable syslog server protocol support.

on - Enable syslog server protocol support.

syslogip <ip>

Enter the syslog server IP address. Valid only if syslog is enabled.

sysmode <**ptpmaster | ptpslave>**

Select operation as PMP sector controller or subscriber (availability controlled by options key).

ptpsmaster - The sector controller (base station) begins transmitting automatically; sending poll messages to locate the remote subscribers (ptpslave).

ptpslave - Subscriber waits passively, monitoring the selected channel(s) until polled by the ptpmaster (base station).

sysname <text>

Enter the name for this AN-80i. Use any combination of up to 20 letters and numbers.

telnet <off | on>

Enable or disable the Telnet port. If the Telnet port is disabled, it will not be possible to use the CLI interface.

off - Disable

on - Enable

Changes to this field are effective only following reboot.

telnetport <1 - 65535>

Telnet port address

port - Limits for the telnet port are 22..79 and 81..65534 (default is 23).

Changes to this field are effective only following reboot.

usrauthmode <local> <radius>

Set the user authentication mode. Specify local services, the RADIUS server, or both in combination.

Table 29: CLI - set (Common for PTP and PMP)

local - use local authentication.

radius - Use the RADIUS server.

x509auth <off | on>

Enable or disable authentication.

off - Allow network connections without authentication.

on - Require authentication using X.509 certificates.

Table 30: CLI - set (PTP-Specific Commands)

View and change PMP-specific parameters.

set <parameter>

atpc <off | on>

Enable or disable the ATPC function. Both units monitor Rx signal and automatically adjust the Tx level of the transmitting system to optimize system performance. The ATPC feature must be enabled on both ends of the link.

off - Disable

on - Enable

This mode can be changed only if allowed by the options key. If the options key does not allow changes: 1) value is specified by the options key, 2) executing a set command for this field will generate an error message.

dataserver

Factory test only -- do not modify this parameter.

dst <distance>

Enter the actual length of the path that the wave travels in order to establish the link. Used only if dstmod is set to 'manual'.

distance Units (mi/km) are defined by dstmu setting.

dstmode <auto | manual>

Select the mode for setting the distance of the wireless link.

auto: Distance is calculated automatically by the AN-80i.

manual: Operator enters link distance.

dstmu <mile | km>

Select the measurement unit for the link length (dstmode).

mile - dstmode units are miles

km - dstmode units are kilometers

efw <off | on>

Enable or disable the Ethernet Follows Wireless function.

off - Disable

on - Enable

When Ethernet Follows Wireless is enabled the Ethernet port status is controlled to reflect the status of the wireless interface. When the AN-80i detects that the wireless interface has failed (or is manually disabled), the local Ethernet port is immediately disabled. The Ethernet port is enabled when the AN-80i registers on the wireless link.

efwtimeout <1-9999>

Enter the period (in seconds) the Ethernet port will remain disabled following loss of connectivity on the wireless interface. Following this interval, the Ethernet port

Table 30: CLI - set (PTP-Specific Commands)

will be automatically re-enabled to allow management of the AN-80i.

flowctrl <off | on>

Enable or disable the flow control function. The Flow control feature enables the AN-80i to request other Ethernet devices to pause transmission during busy periods.

off - Disable

on - Enable

mrate <1 - 54>

Maximum uncoded burst rate (Mbps). Maximum value is set by the options key. Entry values are dependent on the channel bandwidth (chwidth). See Table 5: PTP & PMP - Modulation/Coding for UBR.

pllm <off | on>

Enable or disable prioritized low latency mode;

off - Disable

on - Enable

ratedif <levels>

Enter the number of modulation levels to step down during re-transmission of errored wireless packets.

levels - Set from 0 to 7 (recommended value = 2).

snmpversion < v2 | v3 >

Select the supported version of SNMP. Note that in all current software versions this selection is exclusive (e.g., selecting v3 excludes support of v2).

v2 - enable SNMP v2c support. This mode supports only v2c).

v3 - Enable SNMP v3 support. This mode supports only v3).

sysmode <ptpmaster | ptpslave>

ptpmaster - This unit begins transmitting automatically; sends poll messages to the remote unit and negotiates the wireless link.

ptpslave - This unit waits passively, monitoring the selected channel(s) until polled by the ptpmaster, and participates in negotiating the wireless link.

Table 31: CLI - set (PMP-Specific Commands)

View and change PMP-specific parameters.

set <parameter>

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

If set to a non-zero value, the subscriber is allowed to connect only to this base station with this MAC address (may use '-' or ':' for separators).

bsporten <id> <off | on>

Enable and disable sector controller Ethernet port.

id - ID of port

off - Disabled

on - Enabled

congid <id> <gid>

Group associated with this Connection.

id - Connection ID number.

gid - Group ID number.

Table 31: CLI - set (PMP-Specific Commands)

conlid <id> <lid>

Link associated with this Connection.

id - Connection ID number.

lid - Link ID number.

conpri <id> <0 - 7>

Connection default priority.

id - Connection reference ID number.

convid <id> <1 - 4095>

Set or show a Connection's VLAN ID

id - Connections reference ID number.

conviden <id> <off | on>

Enable or disable VLAN connections.

id - Connection ID number.

on - VLAN is enabled.

off - VLAN is disabled.

dlminrate <id> <1 - 54>

Link minimum downlink uncoded burst rate (Mbps). Entry values are dependent on the channel bandwidth (chwidth). See Table 5: PTP & PMP - Modulation/Coding for UBR.

id = Link ID number.

dlpir <id> <50 - 50000>

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

id - Connection ID number.

dlqos <id> <1 - 53>

Connection downlink QoS setting (from AN-80i PMP configuration tool).

id - Connection ID number.

dlrate <id> <6 - 54>

Link maximum downlink uncoded burst rate.

id = Link ID number.

fastreg <off | on>

Fast registration mode.

grppir <id> <50 - 50000>

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

id - Group ID number.

grppri <id> <0 - 7>

Group default priority.

id - Group reference ID number.

grpqos <id> <6 - 53>

Group QoS (Mbps). Applies to uplink and downlink.

id - Group reference ID number.

grprate <id> <6 - 54>

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

Table 31: CLI - set (PMP-Specific Commands)

id - Group reference ID number.

grppri <id> <pri>

Group default priority.

id - Group reference ID number.

pri - Group 802.1p priority setting.

grpvid <id> <vid>

Group VLAN ID.

id - [id number]

vid - VLAN ID

grpviden <id> <off | on>

Group VLAN enable.

id - [id number]

off - Disabled

on -Enabled

idname <id> <name>

View or modify the name associated with an ID.

id - ID for Link, Connection, or Group.

name - Name (maximum 15 text characters).

maxdst <distance>

Maximum distance to a subscriber.

value - Distance (Km) to farthest subscriber.

regper <4 - 100>

The number of frames between registrations.

sstoss <id> <off | on>

Status of packet routing between SSs.

id - Link ID number.

off - Disable routing broadcast packets from SS to SS.

on - Enable routing broadcast packets from SS to SS.

sysmode <pmpsc | pmpss>

pmpsc - The sector controller (base station) begins transmitting automatically; sending poll messages to locate the remote subscribers (pmpss).

pmpss - Subscribers wait passively, monitoring the selected channel(s) until polled by the pmpsc (sector controller).

ulminrate <id> <6 - 54>

Link minimum downlink uncoded burst rate.

id = Link ID number.

ulpir <id> <50 - 50000>

Connection uplink peak information rate (PIR) (Kbps).

id - Connection ID number.

ulqos <id> <6 - 53>

Connection uplink QoS setting.

id - Connection ID number.

ulrate <id> <1-54>

Table 31: CLI - set (PMP-Specific Commands)

Link maximum uplink uncoded burst rate.

id = Link ID number.

6.1.18 Show

Use the ***show*** command to display system statistics.

show <Enter>   Change to 'show' mode.

show [field] <Enter> Display values for the selected parameter.

Table 32: CLI - show (Common PTP and PMP Commands)

Display PTP system parameters and statistics.

show <config> <files> <log> <snmp> <stats>

config

List system configuration information.

files <run | usr>

List the key and certificate files.

run - Display keys currently in use.

usr - Display the user keys and certificates (default).

log: list the system log

snmp

List the SNMP configuration.

stats

Display available statistics.

Table 33: CLI - show (PMP-Specific Commands)

Display PMP system parameters and statistics.

show <conns> <groups> <idtable> <links>

conns <id>

List information for all or specified Connection. Default is to display all Connections.

id ID number of specific link or group to show related connections.

```
192.168.25.2(show)# conns 4
      96          Data A     Conn
      97         Voice A     Conn
```

groups

List information for all Groups.

```
192.168.25.2(show)# groups
      64            Voice     Group
      65             Data     Group
```

idtable

List information for all system IDs.

```
192.168.25.2(show)# idtable
      ID            Name     Type        Status
-----------------------------------------------------
       4           Sub A     Link        Enabled
       5           Sub B     Link        Enabled
      10           Sub C     Link        Enabled
      15           Sub D     Link        Enabled
      64           Voice     Group       Enabled
      65            Data     Group       Enabled
      96          Data A     Conn        Enabled
      97         Voice A     Conn        Enabled
```

Table 33: CLI - show (PMP-Specific Commands)

```
                     98           Data B     Conn        Enabled
                     99          Voice B     Conn        Enabled
                    100           Data C     Conn        Enabled
                    101          Voice C     Conn        Enabled
```

links

Display information for all Links.

```
         192.168.25.2(show)# links
                      4             Sub A     Link      Down
                      5             Sub B     Link      Down
                     10             Sub C     Link      Down
                     15             Sub D     Link      Down
```

6.1.19 Snmpcommunity

Use the ***snmpcommunity*** command to configure SNMP community permissions.

Table 34: CLI - snmpcommunity

Configure SNMP community permissions.

snmpcommunity <add> <clearall> <default> <del> <print>

add <name> <rights>

Add a new SNMP community to the SNMP community table. The index value is assigned automatically. Up to eight community entries can be entered.

name

Enter the SNMP community name.

rights

Specify the rights for this community string. Where.

0: Deny read and write permission (enter zero).
r: Grant read access permission only.
w: Grant write access permission only.
rw: Grant read and write access permission.

clearall (no parameters)

Delete all SNMP parameters.

default <idx>

Set all SNMP parameters to factory default settings.

idx Specify single entry to be set to default (use 'print' command to display ids).

del <idx>

Delete the specified community entry.

idx Specify single entry to be deleted (use 'print' command to display ids).

print

List all SNMP communities and associated permissions.

6.1.20 Snmptrap

Use the ***snmptrap*** command to configure the SNMP trap message reporting.

Table 35: CLI - snmptrap

Configure SNMP community trap settings.

snmptrap <add> <change> <clearall> <del> <print>

add <ipaddr> <port> <identity>

Table 35: CLI - snmptrap

Create a new SNMP trap. The index value is assigned automatically. Up to eight settings may be entered.

ipaddr	Enter destination IP address
port	Enter destination port address.
identity	v2: Enter associated SNMP community string.
	v3: Enter account username for authorization.

change <idx> [-p <port>] [-i <ip_add>] [-c <community>] [-u username]

Modify the specified SNMP setting.

idx	Index of the SNMP trap (use 'print' command to display ids).
-i <ip_add>]	Enter destination IP address.
-p <port>]	Enter destination port address.
-c <community>	Enter associated SNMP community string (SNMP V1 or V2).
-u <username>	Enter account username for authorization (SNMP V3 only).

clearall

Delete all SNMP parameters.

del <idx>

Delete the specified SNMP trap.

idx	Index of the SNMP trap to be deleted (use 'print' command to display ids).

Linkupdown

Trap indicates when the wireless Link is lost and recovered.

Off -

On -

print

List all SNMP trap settings.

6.1.21 Test

Use the ***test*** command to load the current edited (but not permanently saved) configuration settings. The AN-80i will operate with these settings for a period of five minutes. During the 'test' period, you may click the Save button at any time to save this configuration permanently (also terminating the five minute timer). If the Save button is not selected, the previous saved settings are reloaded.

Table 36: CLI - test

Load the current edited configuration settings (for five minutes).

test <config>

Test AN-80i configuration settings

config - Load and test configuration settings

6.1.22 Upgrade

Use the ***upgrade*** command to upload a new software binary file to the AN-80i.

Table 37: CLI - upgrade

Configure SNMP community permissions.

upgrade <ip addr> <file name> <user name> <password>

ip addr	IP address of the FTP/TFTP server.
file name	Name of the binary file to be uploaded.
user name	FTP account name (FTP server only).
password	FTP account password (FTP server only).

TFTP: You must specify the TFTP server address and the full name of the binary file (including .bin extension). The software binary file must be located in the default directory of the TFTP server.

FTP: You must specify the FTP server address, account user name, account password, and the full name of the binary file (including .bin extension). The software binary file must be located in the default directory for the specified user account.

6.1.23 User

Use the ***user*** command to manage user accounts, passwords, and user Groups. When in user mode, only the <chgpasswd> field is available, since the user can change only their own password. The other commands are available only for members of the administrator Group.

Table 38: CLI - user

Manage the user accounts.

user <add> <attr> <chgpasswd> <del> <print>

add <username> <usertype>

Administrators can use this command to add new user accounts. Usernames may be 1 to 19 alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_), Passwords may be 8 to 15 alpha-numeric characters including a-z, A-Z, 0-9, dash (-), and underscore (_). The operator must confirm their own password and a password for the new account.

The AN-80i supports administrator and user accounts. See 0:

Factory Default Settings on page 116 for the factory default login values. See Table 7**:** PTP & PMP - User Access on page 68 for permissions associated with each group.

username	Enter name of new administrator or user account.
usertype	Specify the type of account being created.
user	User account.
admin	Administrator account.

For example,

```
192.168.25.2(user)# add user2 user
Enter your password: ********
The new user password (8 to 15 characters)
Enter the new user password: ********
Confirm the new user password: ********
```

attr <username> < none | MD5 | SHA > < none | DES | AES >

Table 38: CLI - user
Designate an authentication method and privacy method to be used for SNMP v3 requests. An authentication method must be selected to enable usage of the privacy method. Only combination SHA authentication + AES privacy is valid in FIPS mode. **username** - Account to setup for SNMP v3 authorization. **chgpasswd <user name>** Administrators can change the password of any account. Users can change only their own password. Users are prompted to enter new password information. **username** Account to be modified. **del <username>** Delete a user account. **username** Account to be deleted. **print** Display a list of user accounts.

6.1.24 Whoami

Use the ***whoami*** command to display the username of the current Telnet session. This command is not available when logged in as administrator.

Table 39: CLI - whoami
Display username for this Telnet session. **whoami**

Chapter 7

7 Diagnostics and Troubleshooting

This section provides basic diagnostic and troubleshooting procedures to help solve problems that may occur with the system. If the system is not operating correctly after applying the suggestions in this section, please contact your local Redline representative. Include the model name and serial number of the system in your communications.

7.1 Long Reset (Recover from Lost IP or Password)

If the operator can not access the AN-80i management interface (forgotten IP, username, and/or password), a long reset operation must be performed to provide access the unit. The long reset provides an opportunity to login to the AN-80i using the default IP, usernames and passwords. The long reset procedure requires local access to the AN-80i PoE adapter to power-cycle the AN-80i, and a PC with an Ethernet cable and a Telnet client or Web browser.

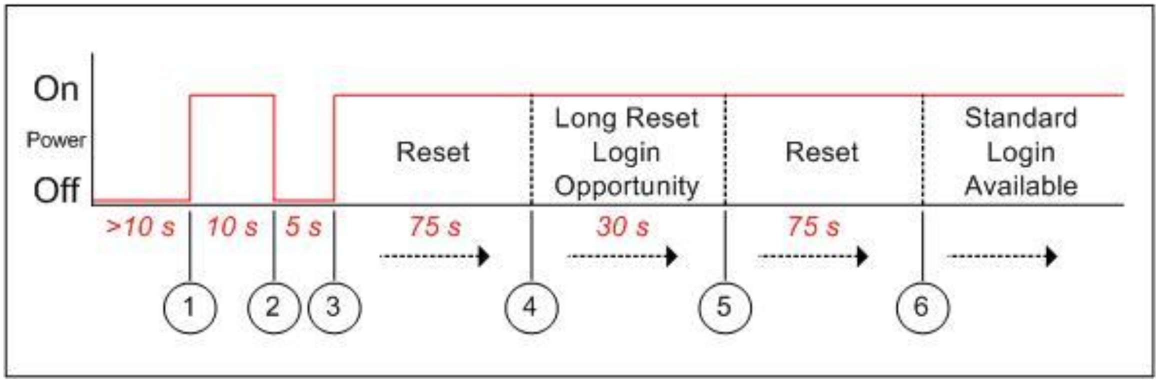


Fig. 51: Diag. - Recovering Lost IP Address

7.1.1 Performing a Long Reset Using Telnet

Use the following steps to gain access to the AN-80i management interface.

1. Power-off the AN-80i PoE adapter and remove the local network Ethernet cable. Use an Ethernet jumper cable to connect the PC directly to the PoE adapter DATA (INPUT) Ethernet port. Prepare the PC for Telnet access by opening a command prompt window on the PC and typing the following command (do not press the Enter key until step 6):

   ```
   telnet 192.168.25.2
   ```

   Note: If using a web browser, type the URL **http://192.168.25.2** in the address field.
2. Restore power to the AN-80i PoE adapter and wait 10 seconds.
3. Power-off the AN-80i PoE adapter for 5 seconds.
4. Restore power to the AN-80i PoE adapter and wait about 75 seconds, then press the ENTER key on the PC to start the Telnet session. When the login prompt appears, you have approximately 30 seconds to login using the default username (admin) and password (admin).
5. Logging in to the unit immediately resets the admin and user accounts to factory default values and deletes all other user accounts. All standard configuration commands are now available.

6. Reboot the unit to exit from long reset mode.

Notes:

7. If a login prompt does not appear in step 4, re-enter the Telnet command during the 30 second interval until the command prompt appears. If this is not successful, repeat steps 1 to 4 using an initial wait time of 70 to 90 seconds).
8. When the operator performs a login (Telnet or Web browser) during a long reset session, the usernames and passwords for the administrator and user are automatically reset to default values. All other user accounts are deleted.
9. If the operator does not login during step 5, the AN-80i will reboot automatically and be fully operational (with no changes) within two minutes.

Refer to page 118 for a complete description of this feature.

7.1.2 Restore Default Passwords Only

Use this procedure if the unit IP address is known and it is desired only to restore the default usernames and passwords. All other configuration settings are preserved.

Telnet

1. Perform a long reset and use Telnet to login to the AN-80i using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).
2. Enter the command **reboot** to restart the unit. Do not enter any other commands.
3. Login to the AN-80i using the user-configured IP address and the default administrator username (admin) and password (admin).

Web

1. Perform a long reset and use a Web browser to login to the AN-80i using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).
2. Click **Configure System** to display the **System Configuration** screen.
3. Click on the **Reboot** buttons at the bottom of the screen to reboot the AN-80i.
4. Login to the AN-80i using the user-configured IP address and the default administrator username and password (admin/admin).

7.1.3 Restore Factory Configuration

Use the following steps to restore the AN-80i to the factory configuration

Telnet

1. Perform a long reset and use Telnet to login to the AN-80i using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).
2. Enter the command **save defaultconfig**. The AN-80i will automatically reboot.
3. Wait for the reboot to complete (10 seconds) and login to the AN-80i using the default IP address (192.168.25.2) and the default administrator username (admin) and password (admin).

Web

1. Perform a long reset and use a Web browser to login to the AN-80i using the default IP address (192.168.25.2), and the default administrator username (admin) and password (admin).
2. Click **Configure System** to display the **System Configuration** screen.
3. Click on the **Def Cfg** button at the bottom of the screen to reload the factory settings and automatically reboot the AN-80i.

4. Wait for the reboot to complete (10 seconds) and login to the AN-80i using the default IP address (192.168.25.2) and the default administrator username (admin) and password (admin).

7.2 Testing and Saving System Parameters

The AN-80i is a highly configurable communications device. All user settings are saved in non-volatile RAM. The system configuration and SNMP settings are saved separately.

7.2.1 CLI Interface

Use the 'test' command to have the AN-80i load the edited settings. The AN-80i will operate with these settings for a period of five minutes. During the test period, you may click the Save button at any time to save this configuration permanently. Otherwise, after five minutes, the AN-80i will reboot and load the previously saved settings.

Note: Factory defaults can only be restored using the Commands.

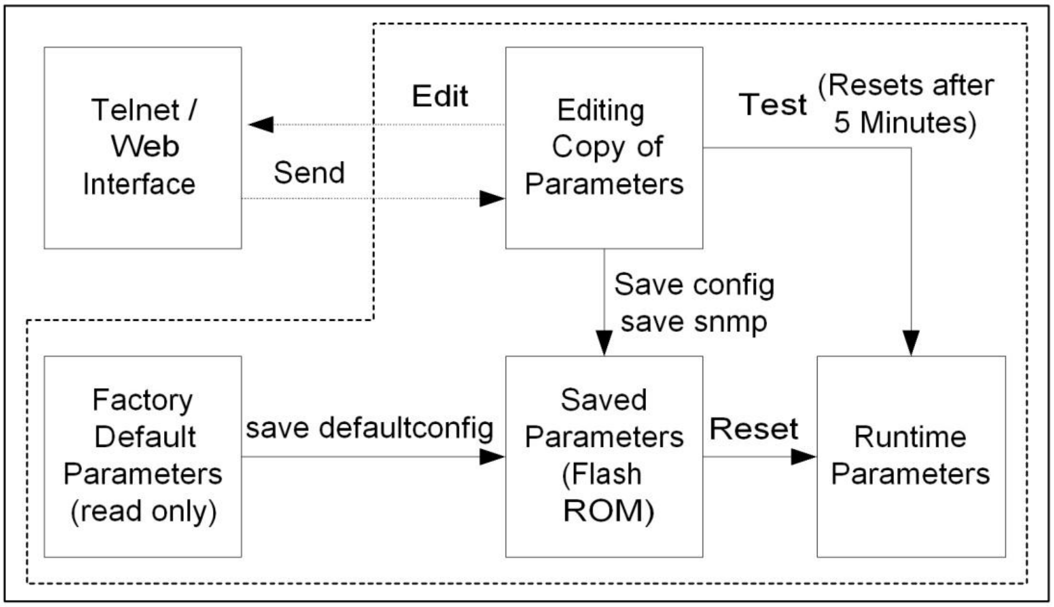


Fig. 52: Diag: - Saving Parameters in NVRAM

7.2.2 Web Interface

The Test button is located on the System Configuration page. Click to have the AN-80i load the current settings displayed in the configuration screen. The AN-80i will operate with these settings for a period of five minutes. During the test period you may click the Save button at any time to save this configuration permanently (also terminating the five minute timer). After five minutes, if the Save function button has not been applied, the AN-80i will reboot and load the previously saved settings.

Attempt to login to the AN-80i using a Web browser. Microsoft Internet Explorer is recommended. If the AN-80i does not respond by displaying the login dialog box, check that the correct IP address is being used. The value 192.168.25.2 is the factory default value and may have been changed during installation.

Test is to verify the IP address is reachable from the computer. Use the ping command to test the Connection between the AN-80i and host computer.

```
>ping 192.168.25.2
```

If the ping test is successful, the host computer was able to send and receive packets to/from the AN-80i. The problem may be with the Internet browser or related settings on the host computer. Reboot the host computer to try to resolve the problem.

If the ping is unsuccessful, there may be problems using that IP address; the IP address may be incorrect, or there may be a duplicate address. For correct operation the host computer and the AN-80i must be on the same subnet. For example, if the AN-80i is using the factory default settings, the host computer could be set for an IP of *192.168.25.3 and a subnet mask of 255.255.255.0.*

If the correct IP address of the AN-80i cannot be determined, it is recommended to perform the IP recovery procedure. See section 7.1: Long Reset (Recover from Lost IP or Password on page 105.

The following table lists some common troubleshooting tips for the web interface.

Table 40: Diag. - Web Interface Diagnostics

Symptom	Possible Problem	Solution
General Information screen is not displayed	Incorrect IP address and/or Subnet Mask.	Perform a ping test from the host computer command line. If the ping test is unsuccessful, then the problem is with the IP address. Perform a long reset to apply the default address (192.168.25.2) and Subnet Mask (255.255.255.0)
	Problems with host computer, or AN-80i.	If the ping is successful, reset the AN-80i, and/or reset the host computer.
	Host PC ARP table is incorrectly configured	Run 'arp -d' whenever the AN-80i is swapped. Check that the subnet mask for the host PC matches the subnet mask of the AN-80i. Check that the host PC address is 192.168.25.n, where 'n' is not equal to 0,2, or 255.

7.3 Dashboard LEDs

The following LED indicators are displayed on the AN-80i web interface page (there are no LED indicators on the AN-80i hardware).

7.3.1 Ethernet LEDs

Ethernet Link LED

The Link LED lights solid green when there is an Ethernet connection and no traffic, and blinks when traffic is detected. If the LED is off, it may indicate one of the problems listed in the following table:

Table 41: Diag. - PTP Ethernet Link/Act LED Diagnostics

Symptom	Possible Problem	Solution
No Ethernet Link	Poor cable connection to equipment.	Carefully check all cable connections.
	Wrong type of cable to Ethernet equipment.	If the Ethernet is connected to a router, a straight-through cable is required. If the Ethernet is connected to a switch, a crossover cable is required.
	System processor malfunction.	Apply short reset or long reset.
	The connected Ethernet equipment may be malfunctioning.	Repair or replace faulty equipment.

Ethernet 100 LED

The Ethernet 100 LED lights solid green when the Ethernet port is operating at 100 Mb/s and is off when operating at 10 Mb/s. If the LED is off, it may indicate one of the problems listed in the following table:

Table 42: Diag. - PTP Ethernet 100 LED Diagnostics

Symptom	Possible Problem	Solution
Ethernet 10 Mbps	Unit is manually set for 10Base-T operation and connected device is operating at 100Base-T or auto-negotiate.	It is strongly recommended to disable auto-negotiation (if enabled) and manually configure all devices to matching speed and duplex. If manual settings are not available, both devices must be set to auto-negotiate.
	The connected Ethernet device is operating at 10Base-T.	This is normal when unit is connected to a computer or server operating at 10Base-T.

Ethernet FD LED

The FD LED lights solid green when the Ethernet connection is operating in full duplex mode and blinks when collisions are detected on the Ethernet port. If the LED is blinking, it may indicate one of the conditions listed in the following table:

Table 43: Diag. - PTP Ethernet Link/Collision LED Diagnostics

Symptom	Possible Problem	Solution
Link Collision (*FD* LED blinks)	Collisions are normal for half duplex links.	No problem.
	Incompatible Ethernet port speed.	It is strongly recommended to disable auto-negotiation (if enabled) and manually configure all devices to matching speed and duplex. If manual settings are not available, both devices must be set to auto-negotiate.

7.3.2 PTP Wireless LEDs

Wireless Data Link LED

The PTP wireless Data LED lights solid green when data can be transmitted across the wireless interface (LED is valid only when the Link LED is lit). If the LED is off, it may indicate one of the problems listed in the following table:

Table 44: Diag. - PTP Wireless Data LED Diagnostics

Symptom	Possible Problem	Solution
No wireless data link	Link not established (Wireless Link LED is off).	A wireless link must be established before data can be exchanged.
	Security settings do not match.	Enter identical encryption field settings on master and slave units.

Wireless Link LED

The PTP wireless Link LED lights solid green when the wireless link is established. If the LED is off, it may indicate one of the problems listed in the following table:

Table 45: Diag. - PTP Wireless Link LED Diagnostics

Symptom	Possible Problem	Solution
No wireless link	Link name does not match.	Enter identical Link Name field settings on master and slave units (may be blank).
	Remote system is malfunctioning or is not powered-on.	Verify operation of remote system.
	The propagation path is blocked.	Clear path or re-locate unit.
	The transceiver is malfunctioning.	Repair/replace unit.
	Antenna is not aligned with the remote system.	Re-align the antenna.

Wireless Signal LED

The PTP wireless signal LED lights when a wireless link is established. Signal indications are different based on the Adaptive Modulation setting:

Table 46: Diag. - PTP Wireless Signal LED Indication

Adaptive Modulation	Description	
Enabled	The LED lights solid green when the wireless link is operating at the rate equal to the Uncoded Burst Rate setting, and blinks when operating at a lower rate.	
Disabled	The LED lights solid green when the wireless link is established.	
LED is off (Weak RF Link)	Obstructions in the propagation path causing signal degradation.	Try to remove obstacles or re-locate antenna.
	Antenna moved, due to high winds.	Re-align the antenna.

7.3.3 PMP Wireless LEDs

Wireless Link LED

The PMP wireless Link LED lights solid green under the following conditions:

Sector Controller:	When a wireless link is established to one or more subscribers.
Subscriber:	When a wireless link is established to the sector controller.

Table 47: Diag. - Wireless Link LED Diagnostics

Symptom	Possible Problem	Solution
No wireless link	Remote system is malfunctioning or powered-off.	Verify operation of remote system (sector controller or subscriber).
	The propagation path is blocked.	Clear path or re-locate unit.
	The transceiver is malfunctioning.	Repair/replace unit.
	Antenna is not aligned.	Re-align the subscriber antenna.

Wireless Signal LED

The PMP wireless Signal LED has the same function as the wireless Link LED.

7.4 Status Codes

7.4.1 PTP Status Codes

The PTP status code is displayed in a series of decimal characters representing the status of six different alarm conditions. The value '1' indicates the associated condition is active. All unused bits are set to zero. To determine the status, the decimal number must be converted to binary notation.

Table 48: Diag. - PTP Status Codes

Error Type	Error # Decimal*	Error # Binary	Description
Tx Power	1	1	Power output is less than 10 dBm. This message may appear before the RF link is established.
RF High Temp. Warning	2	10	The transceiver internal temperature rose above 185 degrees F / 85 C. The transceiver will shut down for 30 seconds to allow cooling.
RF PLL Lock Error	16	1 0000	The PLL (Phase Locked Loop) section within the AN-80i experienced an error. Reset the AN-80i.
PHY lock error	32	10 0000	The PLL (Phase Locked Loop) section within the AN-80i experienced an error. Reset the AN-80i.
80 MHz PLL lock error	64	100 0000	The PLL (Phase Locked Loop) section within the AN-80i experienced an error. Reset the AN-80i.
Firmware Configuration Error	128	1000 0000	Error detected in the AN-80i configuration file.

*Displayed decimal value if this is the only active error condition.

It is recommended to use a scientific calculator that supports binary notation (e.g., Windows on-screen calculator). Set the mode for decimal and enter the status code. Change the mode to binary and match active bits (1) to the table entries.

Example, if 'RF High Temp. Warning' (2) and ' PHY lock error' (1 0000) were active, the status code value would be 34 (binary 100010) (leading zeros are not displayed).

7.4.2 PMP Status Codes

The PMP status code is displayed in a series of hexadecimal characters representing the status of different alarm conditions. The value '1' indicates the associated condition is active. All unused bits are set to zero.

To determine the status, the hexadecimal number must be converted to binary notation. It is recommended to use a scientific calculator that supports binary notation (e.g., Windows on-screen calculator). Set the mode for Hex and enter the status code. Change the mode to binary and match active bits (1) to the PMP Status Codes table.

For example, if 'Radio Over Temperature' bit 1 and 'PLL Error' bit 4 were active, the status code value could be Hex '12' (binary 1 0010).

Table 49: Diag. - PMP Status Code Bits

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	9	8	7	6	5	4	3	2	1	0

Table 50: Diag. - PMP Status Codes	
Bit	**Description**
1	Radio over-temperature
4, 5, 6	PLL Errors
8	Firmware Error
16	No Ethernet packets received by the wireless MAC
17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28	MAC Internal Errors

7.4.3 FIPS Status Codes

The PMP status code is displayed in a series of hexadecimal characters representing the status of different alarm conditions. The value '1' indicates the associated condition is active. All unused bits are set to zero.

Table 51: Diag. - FIPS Status Codes	
0x0001	Power up self test for random number generator failed
0x0002	Power up self test for 3DES failed
0x0004	Power up self test for AES (communication channel) failed
0x0008	Power up self test for SHA failed
0x0010	Power up self test for HMAC failed
0x0020	Power up self test for DSA failed
0x0040	Power up self test for RSA failed.
0x0080	Power up self test for AES (data channel) failed
0x0100	Continuous self test for random number generator failed

7.4.4 System Log Messages

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

Table 52: Diag. - System Log Messages

Event ID	Event Description
1001	System Configuration Load: OK
1002	System Configuration Save: OK
1003	EEPROM Directory Load: OK
1004	EEPROM Directory Save: OK
1005	User Configuration Load: OK
1006	User Configuration Save: OK
1007	Network Configuration Load: OK
1008	Network Configuration Save: OK
1009	Network Configuration: OK
1010	Version Ctrl Data Load: OK
1011	Version Ctrl Data Save: OK
1012	System Description Load: OK
1013	System Description Save: OK
1014	Options Key Load: OK
1015	Options Key Save: OK
1016	Options Key Properties Load: OK
1017	Options Key Properties Save: OK
1018	Options Key Activated: OK
1019	Data server started: OK
1021	Upgrade: OK
1023	Firmware configuration: OK
1026	Factory Data Save: OK
1029	HTTP(User Mgm): Chg User Attributes: OK
1030	SNMP Configuration Load: OK
1031	SNMP Configuration Save: OK
1032	SNTP: Time received: OK
1033	DFS: Event Detected
1033	MAC Initialization: OK
1034	DFS: Event Detected
1035	ID deleted: OK
1036	Restart freq scan (RSSI)
1037	Restart freq scan (TimeOut)
1038	Reg Req (step 1)
1039	Reg Req (step 2
1040	Reg Req (step 2)
1041	Restart freq scan (!act links)
1042	ID tables saved: OK
1043	ID defined: OK
1044	ID tables not changed: OK
1045	ID modified: OK
1046	RF frequency validation: OK
2001	System Configuration Load: Error
2002	System Configuration Save: Error
2003	EEPROM Directory Load: Error
2004	EEPROM Directory Save: Error
2005	User Configuration Load: Error
2006	User Configuration Save: Error
2007	Network Configuration Load: Error
2008	Network Configuration Save: Error

Table 52: Diag. - System Log Messages	
Event ID	**Event Description**
2009	Network Configuration: Error
2010	Version Ctrl Data Load: Error
2011	Version Ctrl Data Save: Error
2012	System Description Load: Error
2013	System Description Save: Error
2014	Options Key Load: Error
2015	Options Key Save: Error
2016	Options Key Properties Load: Error
2017	Options Key Properties Save: Error
2018	Options Key Activated: Error
2019	No Options Key
2020	Fail to start the data server
2021	Data server
2022	Data server
2023	Upgrade client start: Error
2024	Upgrade in progress
2025	Upgrade: FAIL
2026	Upgrade: Error
2028	Factory Data Corrupted (use fallback values)
2028	TFTP: Error
2029	Firmware configuration: Error
2031	Factory Data Save: Error
2034	HTTP(User Mgm): Invalid password
2035	HTTP(User Mgm): Invalid User
2036	HTTP(User Mgm): Chg User Attributes: Error
2037	SNMP Configuration Load: Error
2038	SNMP Configuration Save: Error
2039	Invalid Options Key
2039	SNTP: Time received: Error
2040	MAC Initialization: Error
2041	MAC Busy
2042	ID database corrupted
2043	Invalid ID
2044	Max. ID number reached
2045	Int Procs programming: Error
2046	Int Procs start: Error
2047	ID action not possible
2048	ID validation: Error
2049	HW validation: Error
2050	FTP: Error
2051	WS: Timeout (WS_SEND_SESSION_REQ)
2063	SSH RSA KEY missing, using default key
2064	SSH DSA KEY missing, using default key
2065	SSL Certificate missing, using default one
2066	SSL KEY missing, using default one
2070	Pre Shared Key Error
2071	Authentication Packet Validation Error
2072	Encryption Key Validation Error
2073	Signature Validation Error
2074	Certificate Validation Error
2075	RNG self test Error
2076	DSA pair wise test failed
2077	RNG self test failed

Table 52: Diag. - System Log Messages	
Event ID	**Event Description**
2078	TDES self test failed
2079	AES self test failed
2080	SHA self test failed
2081	HMAC self test failed
2082	RSA self test failed
2083	DES self test failed
2084	MAC AES self test failed
2086	Upgrade image validation: Error
2087	Upgrade Error: image save
2088	SSH RSA KEY missing, using generated key
2089	SSH DSA KEY missing, using generated key
2090	Test not executed when FIPS mode changed
2091	The options key expires in less than 6 days
2092	SSL Certificate missing, HTTPS disabled
2093	Wireless Security Certificates missing
2094	Firmware validation: Error (%s)
2095	Image validation: Error
2099	Unknown Message

7.5 Factory Default Settings

Table 53: Diag. - Factory Default Settings

CLI Parameter	Web Field	Key Control	PTP [1]	Def Cfg Button Setting
activekey	Active Key			No change
adaptmod	Adaptive			Off
antgain	Antenna Gain			30
atpc	ATPC		PTP	Off
autoscan	Autoscan			Off
buzzer	Buzzer			Off
chwidth	Channel Width			Based on Key: Key = No change No Key = 10 MHz
dfsaction	DFS Action	Y		Based on Key: Req. = chgfreq Not Req = none No Key = none
dst	Link Length		PTP	0
dstmu	Link Length Measurement		PTP	Auto
efw	Ethernet Follows Wireless		PTP	Off
efwtimeout	Ethernet Follows Wireless Timeout		PTP	0
encmode	Encryption Type	Y		None
ethmode	Ethernet Mode			Auto
fipsmode	FIPS Mode	Y		0 (none)
flowctrl	Flow Ctrl		PTP	Off
freq	Frequency List			Cleared
gateway	Default Gateway Address			192.168.25.1
gmt	Time Offset			+0.00
http	HTTP Enable			On
https	HTTPS Enable			On
ipaddr	IP Address			192.168.25.2
lkname	Link Name		PTP	Blank
maxdst	Max. Distance			0 [3]
maxtxpower	Maximum Tx Power			14 dBm
mgmtag	Mgmt Tag Enable			Off
mgmvid	Mgmt VID			0
mrate	Uncoded Burst Rate	Y	PTP	Based on Key: Key = No Key = 3 Mbps
netmask	IP Subnet Mask			255.255.255.0
optionskey	Options Key			Unchanged
peermac	Peer MAC		PTP	00:00:00:00:00:00:00
pllm	Low Latency Mode		PTP	Off

Table 53: Diag. - Factory Default Settings				
CLI Parameter	**Web Field**	**Key Control**	**PTP** [1]	**Def Cfg Button Setting**
pllm	Prioritized Low Latency		PTP	Off
radio	Radio Enable			On
radius	RADIUS			Blank
ratedif	Modulation Reduction Level		PTP	2
regper	Registration Period			16 [3]
rffreq	RF Freq. (MHz)			Based on options key.
snmp	SNMP			Unchanged
snmpcommunity	SNMP Community Strings			"Public". read "Private" read/write
snmptraplink	SNMP Traps			Off
snmptraplist	SNMP Trap List			Cleared
snmptraps	SNMP Trap Links			Off
snmpversion	SNMP Version			V2 (if enabled) [2]
sntp	SNTP Enable			Off
sntpip	SNTP IP Address			192.168.25.1
sntppoll	Polling Interval			24
ssh	SSH			On
syscontact	System Contact			Blank
sysdescr	System Details			Blank
sysloc	System Location			Blank
syslog	Sys Log Enable			Off
syslogip	Sys Log IP			192.168.25.1
sysmode	System Mode			Based on Key: No Key = PTP only Key = unchanged
sysname	System Name			AN-80i
telnet	Telnet Enable			On
telnetport	Telnet Port			23
txpower	Tx Power			14 dBm
user	User Account			admin/admin[4]: user/user
userauthmode	User Authentication			Local
x509auth	X.509 Authentication Enable			Off

1. PTP mode only; 2. SNMP v2 only in PMP mode; 3. PMP only; 4. All user created accounts are deleted.

Chapter 8

8 Security

8.1 Overview

The Redline AN-80i provides a high level of security and reliability. Security sensitive institutions including banks, military, government groups, and large corporations have tested and approved the AN-80i as meeting their strict requirements for network operations.

There are two primary modes of operation for the AN-80i:

Standard Security: Wireless authentication using X.509 certificates, AES 128-bit wireless encryption, and Redline proprietary wireless encryption are standard features on the AN-80i system. AES 256 bit encryption is optional and must be purchased separately and enabled by loading an AES-enabled options key.

FIPS Mode: FIPS mode is optional and must be purchased separately and enabled by loading a FIPS-enabled options key.The FIPS option meets the requirements of FIPS140-2 Level 2 and those of federal government and military customers. The AN-80i FIPS implementation has passed full function validation tests by an NIST accredited lab[1]. Security features include extensive built-in self-tests for hardware, onboard firmware, and downloaded software, and a t amper-proof enclosure to ensure system integrity. AES 256-bit wireless encryption is included with the FIPS option.

8.1.1 Authentication

The AN-80i supports the use of X.509 certificates for authentication.

- Challenge-response mechanism during the link establishment
- FIPS mode requires X.509 certificates and keys

8.1.2 Data Security

The AN-80i includes security mechanisms that provide sender authentication and security and integrity for data sent over the wireless interface. These features include:

- Wireless speed encryption/decryption for data traffic
- Messages encrypted and validated using AES in CCM (Counter with Cipher Block Chaining-Message Authentication Code)
- FIPS approved key derivation with separate keys for data traffic and key transport
    - Diffie-Hellman for key establishment
    - AES Wrap algorithm for key transport
    - Keys changed at random intervals
- FIPS mode allows only FIPS approved algorithms to be selected

AES (Advanced Encryption Standard) option is an encryption standard employed worldwide. The AES cryptographic cipher uses a block length of 128 bits and key lengths of 128, 192 or 256 bits. As used in the United States, AES is a Federal Information Processing Standard (FIPS), specifically, FIPS Publication 197, that

[1] FIPS 140-2 certification is expected n June 2010. Currently in „Finalization' stage of Module in Process for official documentation review by CMVP/NIST.

specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive information. The AES block cipher has been ratified as a standard by National Institute of Standards and Technology of the United States (NIST).

The AN-80i also supports a Redline engineered proprietary encryption scheme based on private-key proprietary algorithms. The proprietary encryption system supported in the AN-80i PTP uses a 64 -bit private-key stream cipher that is changed every wireless data block. Keys are generated using the proprietary algorithm that can generate up to 2^48 distinct independent sequences of keys.

8.1.3 Management Security

The AN-80i includes security mechanisms for device management.

- TLS 1.0 for HTTPS for secure Web access
- SSH v2 for secure command line operation
- SNMP v3 with AES support
- Digitally-signed software upgrade files
- FIPS mode allows only FIPS-approved cryptographic algorithms

8.1.4 Physical Security

The Redline AN-80i is enclosed in a weatherproof aluminum alloy case. The module's enclosure is sealed using tamper-evident labels, which prevent the case covers from being removed without signs of tampering.

The security of the AN-80i system is further increased by the following factors:

- Stream cipher cannot be reverse-engineered -- even by destroying the equipment
- Key generation algorithm cannot be reverse-engineered -- even by destroying the equipment
- MAC address of a system cannot be changed without damaging the equipment
- Two communicating AN-80i systems detecting they have the same MAC address will immediately shut down

Important Security Guidelines:

1. Store encryption keys and certificate information in a secure location.
2. Always use secure transfer (e.g., SSH or SSL) when working with encryption keys and certificates.
3. It is recommended to use the AN-80i local Ethernet port to transfer encryption keys and certificates, or sftp if loading certificates or keys across an open network.

8.2 Standard Security Mode

This section describes using the AN-80i security features in standard (non-FIPS) mode.

Important: When operating in standard security (non FIPS) mode, the wireless authentication, SSH, and HTTPS algorithms use only certificate and key files loaded in the user (usr) table.

8.2.1 Wireless Authentication

Wireless authentication is a standard feature on all AN-80i systems.

Out-of-Box Operation

Wireless authentication is not supported out of box. Each AN-80i system to use wireless authentication must meet the following requirements:

1. The operator must generate and load X.509 certificate and key files
2. The wireless certificate and key files must be loaded into the user (usr) table. The files can only be loaded using the CLI interface (Telnet or SSH).

Load Wireless X.509 Certificate and Key Files

Use the following steps to setup wireless authentication:

1. Use a commercially available tool to create the required X.509 certificates and keys. The filenames used must comply with the following requirements:

usr_wacert_<mac>.der	X.509 authority certificate
usr_wcert_<mac>.der	X.509 certificate
usr_wkey_<mac>.der	Private key

2. Copy the certificate and key files to the default directory of a TFTP server.
3. Use the Command 'load' to copy the certificate and key files from the TFTP server to the AN-80i.
4. Use the command 'show files usr' to verify the files have been successfully loaded.
5. Reboot the AN-80i to activate changes to the key files.

Enable Authentication

The wireless X.509 certificate and key files must be loaded into the usr table and the AN-80i rebooted to activate the new keys before wireless authentication can be enabled.

Use one of the following methods to enable authentication:

CLI: set x509auth on

Web: Configuration screen -> Wireless Security Configuration:

X.509 Authentication Enable ☑

Note: Save the configuration to activate changes.

Example

Load certificate files and key from the TFTP server at 192.168.25.10 to the AN-80i having MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.10 usr_wacert_00-09-02-01-C1-9A.der usr tftp
192.168.25.2# load file 192.168.25.10 usr_wcert_00-09-02-01-C1-9A.der usr tftp
192.168.25.2# load file 192.168.25.10 usr_wkey_00-09-02-01-C1-9A.der usr tftp
192.168.25.2# show files usr
    dsa_key.pem     size=672     md5=fa9bd7a1f465fd7e9fed30150b0608c4
    usr_wkey.der    size=1194    md5=1c5c5ddd0f08604a3b48cf41a8570557
    usr_wacert.der  size=1144    md5=ff0ce6923fc67a02d1e7bc6fa4856f94
    usr_wcert.der   size=999     md5=82b115af9dba510e5af8ce558e964265
192.168.25.2# reboot
```

```
...
192.168.25.2# set x509auth on
192.168.25.2# save config
```

8.2.2 Redline 64-bit Encryption (PTP Only)

Redline proprietary 64-bit wireless encryption is a standard on all AN-80i PTP systems.

Out-of-Box Operation

The AN-80i provides out-of-box wireless encryption using the Redline proprietary encryption scheme based on private-key proprietary algorithms. This encryption method is also compatible with AN-50e equipment. Identical encryption settings must be used on both communicating wireless systems.

Enabling Redline 64-bit Encryption

Use the following steps to enable 64-bit encryption on the AN-80i:

1. Enter the MAC address of the remote AN-80i (or AN-50e) unit.

   Web: Configuration screen -> Ethernet Configuration: Peer MAC

2. Choose the same 64-bit encryption setting on both systems (80i/80i or 80i/50e). A data link can be established only between systems with identical security settings.

   Web: Configuration screen -> Wireless Security Configuration: Encryption Type

3. Save the configuration to activate changes.

Example

Enable 64-bit encryption. Remote AN-80i has MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# set peermac 00 09 02 01 C1 9A
192.168.25.2# set encmode 1
192.168.25.2# save config
```

8.2.3 AES Encryption

AES 128 bit wireless encryption is a standard feature on all AN-80i systems. AES 256-bit wireless encryption is an optional feature that may be purchased separately.

Out of Box Operation

AES encryption is not supported out of box. Each AN-80i system to use AES encryption must meet the following requirements:

1. AN-80i software with FIPS support is loaded and operational .
2. AES 128-bit:
   An options key enabled for AES 128-bit operation must be obtained, loaded on the AN-80i, and be the currently active options key. The AES 128-bit feature is a standard (no charge) for AN-80i systems.
3. AES 256-bit:
   An options key enabled for AES 256-bit operation must be purchased, loaded on the AN-80i, and be the currently active options key. AES 256-bit operation is a chargeable upgrade for systems.

Enabling AES

Use the following steps to setup and enable AES encryption:

1. Obtain an AES-enabled upgrade options key for all communicating AN-80i systems.
2. Copy each new options key to the AN-80i with the matching MAC address.

   Refer to section 5.4: Product Options Screen on page 77 .
3. Select the new key in the Active Options Key field and click Activate to immediately enable the AES feature.

4. Choose the same AES encryption setting on both AN-80i systems. A data link can be established only between systems with identical security settings.

   Web: Configuration screen -> Wireless Security Configuration: Encryption Type

   (None, 64-Bit, AES 128, AES 192, AES 256)

5. Save the configuration to active changes.

8.2.4 SSH for Secure CLI

SSH is a standard feature on all AN-80i systems. SSH provides secure access when using the command line interface (CLI) to manage AN-80i equipment. When SSH is required, TELNET (unsecured access) should be disabled. Use an SSH client (e.g., OpenSSH, Putty, etc) to access an AN-80i using SSH.

It is recommended that system operators generate a unique certificate and private-public keys, and load these on the AN-80i before using the HTTPS feature in a production environment.

Out-of-Box Operation

The AN-80i provides out-of-box use of the SSH interface. If no user-generated DSA key has been loaded on the AN-80i, a temporary key is generated automatically.

> Each reboot, a new self-generated key (ssh_key<mac>.pem) is loaded into the user table. The self-generating key feature is disabled when the user loads a key in the user (usr) table or creates a key using the CLI 'generate' command.

Note: When using the self-generated key, a warning message may be displayed, based on the SSH client security settings (e.g., *'Warning: Potential Security Breach. The servers host key does not match ...'*). The operator has full access to the secure CLI interface.

Enable SSH

SSH is disabled by (factory) default. Use the CLI or Web interface to enable SSH:

Web interface: Configuration screen -> Ethernet: SSH Enable ☑

Command: set ssh on

Loading an SSH Key File

Use the following steps to load user-generated X.509 certificate and key files:

1. Use a commercially available tool to create the required key file. The DSA key file must conform to the following:
   - Maximum key size is 2048 bits
   - Key filename must be in the following format:

     dsa_key_<mac>.pem
2. Copy the key file to the default directory on a TFTP server.
3. Use the CLI 'load' command to load the SSH DSA key into the user (usr) table. It is recommended to use the local Ethernet port when transferring encryption keys and certificates to the AN-80i.
4. Reboot the AN-80i to activate changes to the key files.
5. Login to the AN-80i and verify the files have been successfully loaded.

Example

Use TFTP server at IP address 192.168.25.10 to load an SSH key file for the AN-80i with MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.10 dsa_key_00-09-02-01-C1-9A.pem usr tftp
192.168.25.2# show files usr
```

```
    dsa_key.pem     size=672       md5=fa9bd7a1f465fd7e9fed30150b0608c4
192.168.25.2#
192.168.25.2# reboot
```

SSH Key Generate Utility

Use the Command 'generate sshkey dsa' to create a DSA key and save this file in the user (usr) table. This key file will be persistent through reboots. After executing the generate command, the AN-80i must be rebooted to activate the new key.

Example: Generate a new DSA key file.

```
192.168.25.2# generate sshkey dsa
192.168.25.2# reboot
```

8.2.5 HTTPS (SSL) for Secure Web

HTTPS (SSL) is a standard feature on all An-80i systems. HTTPS uses authentication and encryption to provide secure access over an unsecured network. When HTTPS is required, HTTP (unsecured access) should be disabled.

Out-of-Box Operation

The AN-80i provides out-of-box HTTPS (SSL) using an embedded X.509 certificate. The embedded certificate is identical for all shipped AN-80i equipment and is intended only to for initial system configuration. Use of the embedded certificate does not provide a secure solution.

When using the embedded certificate, warning messages may be displayed based on browser security settings (e.g., '*The security certificate presented was not issued by a trusted certificate authority. The security certificate presented was issued for a different website address.*) The operator has full access to the secure Web interface.

It is recommended that system operators generate a unique certificate and private-public keys, and load these on the AN-80i before using the HTTPS feature in a production environment.

Enable HTTPS/SSL

HTTPS is disabled by (factory) default. Use the Web interface or CLI to enable HTTPS:

Web interface: Configuration screen -> Ethernet: HTTPS Enable ☑

Command: set https on

Save the configuration to active changes.

To access the AN-80i using HTTPS, the URL entered in the Web browser must specify 'https' or directly reference port 443.

Example: To access the AN-80i when HTTPS is enabled (default IP shown):

```
https://192.168.25.2/        (Web browser automatically redirects to port 443)
http://192.168.25.2:443/     (Operator specifies port 443)
```

Loading HTTPS (SSL) Certificate and Key Files

Use the following steps to load user-generated X.509 certificate and key files:

1. Use a commercially available tool to create the required certificate and key files.

   The X.509 certificate file must conform to the following:

   - Maximum file size is 1400 bytes
   - Subject must match the access method (e.g., IP or name)
   - Filename must be formatted as follows:

     ssl_cert_<mac>.pem

   The SSL (RSA) key file must conform to the following:

- Maximum 2048 bits.
- Filename must be formatted as follows:

  ssl_key_<mac>.pem

2. Copy the key files to the default directory on a TFTP server.
3. Use the CLI 'load' command to load the RSA key and certificate. It is recommended to use the local Ethernet port when transferring encryption keys and certificates to the AN-80i.
4. Use the command 'show files usr' to verify the files have been successfully loaded.
5. Reboot the AN-80i to activate changes to the key files. HTTPS will be available when the system reboot is completed.

Example

Load HTTPS (SSL) key and certificate files from the TFTP server at 192.168.25.1 to the AN-80i having MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.1 ssl_cert_00-09-02-01-C1-9A.pem usr tftp
192.168.25.2# load file 192.168.25.1 ssl_key_00-09-02-01-C1-9A.pem usr tftp
192.168.25.2# show files usr
    dsa_key.pem      size=672       md5=fa9bd7a1f465fd7e9fed30150b0608c4
    usr_ssl_key.der   size=1194      md5=1c5c5ddd0f08604a3b48cf41a8570557
    usr_ssl_cert.der   size=1144      md5=ff0ce6923fc67a02d1e7bc6fa4856f94
192.168.25.2# reboot
```

8.3 FIPS - High-Security Model

FIPS operation is an optional feature for AN-80i systems.

The FIPS option provides very high security for physical, data, and management when using the AN-80i equipment. FIPS supports the strongest standards based encryption for information secrecy and integrity against eavesdropping. Built-in security mechanisms protect against denial-of-service, replay attacks, and the strongest standards-based authentication algorithm to prevent man-in-the-middle attacks.

When FIPS mode is active, the AN-80i provides secure system access and management with user authentication over SSH and/or HTTPS using FIPS approved/validated algorithms. The system also provides authentication for network connections and X.509 certification based authentication over the wireless interface and hardware-based AES encryption.

If SNMP v3 is enabled, authentication is performed using SHA and AES privacy, and a user ID/password policy is enforced.

Important: When operating in FIPS mode, the wireless authentication, SSH, and HTTPS algorithms use only certificate and key files loaded in the FIPS (fips) table.

8.3.1 FIPS Mode Setup

FIPS Mode Out-of-Box Operation

FIPS mode is not supported out of box. Each AN-80i system to be used in FIPS mode must meet the following requirements:

1. AN-80i software with FIPS support is loaded and operational.
2. An options key enabled for FIPS operation must be purchased, loaded on the AN-80i, and be the currently active options key.

Notes:

1. SSH access is mandatory for loading FIPS certificates and keys, and is available out-of-box. See SSH description later in this section.
2. HTTPS is not required for FIPS setup and is not out-of-box compatible with FIPS mode. See HTTPS description later in this section.
3. SNMP is not required for FIPS setup and does not include all the functions necessary to enable and configure FIPS mode operation.

Setting Up FIPS Mode Operation

1. Adjust User Account Settings

All user accounts (admin and user type) must conform to the FIPS security policy requiring a minimum of eight characters for all usernames and passwords. The operator must create new compatible 'admin'; and 'user' type accounts as required and then delete all non-compatible accounts. There must always be at least one 'admin' type account.

Example: Sample username/password combinations.

admin / admin:	*Not acceptable*
administrator / admin:	*Not acceptable*
administrator / admin678:	*Acceptable*

2. Restrict management access to SSH (and optionally SNMP v3).

HTTP:	Off
HTTPS:	Off

SNMP:	Off (or v3)
Telnet:	Off
SSH:	On

3. Enable FIPS Bypass Mode

FIPS mode can be enabled after all user accounts have been made compliant to the FIPS security policy, and management access has been restricted to SSH.

Web: Configuration screen -> Wireless Security Configuration:

FIPS Mode Enable ☑

CLI: set fipsmode on

Save the configuration to activate changes. If all conditions for FIPS mode are satisfied, the AN-80i will reboot and enter FIPS mode.

Using SSH to Troubleshoot FIPS Mode

If FIPS mode does not become active, use the Command 'get fipsstatus' to show a report of the FIPS components. The following example indicates that the user accounts do not comply with the FIPS security policy.

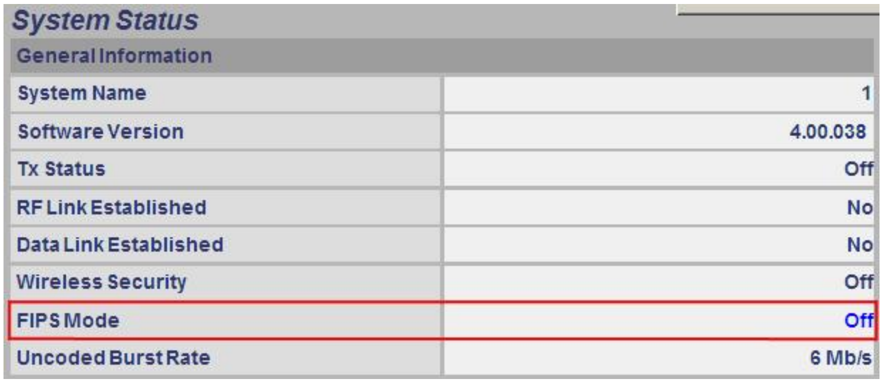
Example

Check the status of FIPS mode components.

```
192.168.25.2# get fipsstatus
FIPS Status              : OFF
FIPS Components:
FIPS Mode                : OFF
   Self Test             : PASS
   Users Validation      : FAIL
   HTTP                  : OFF    (OFF)
   SNMP                  : V3     (OFF or V3)
   Telnet                : OFF    (OFF)
   HTTPS                 : OFF
   SSH                   : ON
```

Using HTTP to Troubleshoot FIPS Mode

If the AN-80i does not enable FIPS mode as requested, re-enable HTTP, login to the Web GUI and click **System Status** in the main menu. Locate **FIPS Mode** and then click on the status **'Off'** link to display the FIPS Status screen. The following screens display

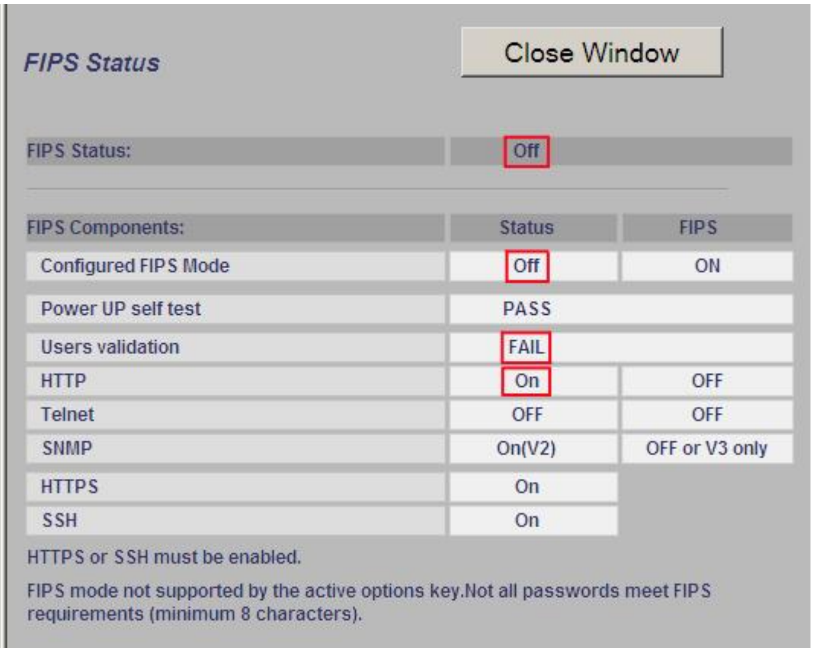


System Status

General Information	
System Name	1
Software Version	4.00.038
Tx Status	Off
RF Link Established	No
Data Link Established	No
Wireless Security	Off
FIPS Mode	Off
Uncoded Burst Rate	6 Mb/s

Fig. 53: Security - System Status - FIPS Status Off

The FIPS Status screen provides a summary of the all FIPS related operations, policies, and parameter settings. The following example screen indicates that the user accounts do not comply with the FIPS security policy (and HTTPS is enabled).



FIPS Status:	Off	
FIPS Components:	**Status**	**FIPS**
Configured FIPS Mode	Off	ON
Power UP self test	PASS	
Users validation	FAIL	
HTTP	On	OFF
Telnet	OFF	OFF
SNMP	On(V2)	OFF or V3 only
HTTPS	On	
SSH	On	

HTTPS or SSH must be enabled.

FIPS mode not supported by the active options key.Not all passwords meet FIPS requirements (minimum 8 characters).

Fig. 54: Security - FIPS Status Popup - Invalid Account Setup

8.3.2 FIPS: Wireless Authentication

The FIPS mode option includes wireless authentication using X.509 certificates, and AES encryption.

Out-of-Box Operation

Wireless authentication in FIPS mode is not supported out of box. Each AN-80i system to be setup with wireless authentication must meet the following requirements:

1. AN-80i software with FIPS support is loaded and operational.
2. FIPS bypass mode must be active (see FIPS Mode Out-of-Box Operation).
3. The user must create X.509 certificate and key files for wireless authentication and load these in the FIPS (fips) table (requires reboot). The fips table is accessible only by using SSH when FIPS mode is active.

Load FIPS Wireless Certificate and Key Files

Use the following steps to setup wireless authentication:

1. Use a commercially available tool to create the required X.509 certificates and keys. The filenames must be formatted as follows:

usr_wacert_<mac>.der	X.509 authority certificate
usr_wcert_<mac>.der	X.509 certificate
usr_wkey_<mac>.der	Private key

2. Copy the certificate and key files to the default directory on a TFTP server.
3. Use the CLI 'load' command to copy the X.509 certificate and key files to the AN-80i.
4. Use the command 'show files fips' to verify the files have been successfully loaded.
5. Reboot the AN-80i to activate changes to the key files.
6. Enable wireless authentication.

Example

Use the TFTP server at IP address 192.168.25.1 to load certificate and key files generated for the AN-80i with MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.1 usr_wacert_00-09-02-01-C1-9A.der fips tftp
192.168.25.2# load file 192.168.25.1 usr_wcert_00-09-02-01-C1-9A.der fips tftp
192.168.25.2# load file 192.168.25.1 usr_wkey_00-09-02-01-C1-9A.der fips tftp
192.168.25.2# show files fips
    dsa_key.pem      size=672       md5=fa9bd7a1f465fd7e9fed30150b0608c4
    usr_ssl_key.der   size=1194      md5=1c5c5ddd0f08604a3b48cf41a8570557
    usr_ssl_cert.der   size=1144      md5=ff0ce6923fc67a02d1e7bc6fa4856f94
192.168.25.2# reboot
...
192.168.25.2# set x509auth on
```

8.3.3 FIPS: AES Encryption

AES 256 bit wireless encryption is a standard feature with the FIPS option. AES encryption is not supported on AN-50e systems.

Out-of-Box Operation

AES encryption in FIPS mode is not supported out of box. Each AN-80i system to use AES encryption in FIPS mode must meet the following requirements:

1. AN-80i software with FIPS support is loaded and operational.
2. An options key enabled for FIPS operation must be purchased, loaded on the AN-80i, and be the currently active options key.
3. FIPS mode must be active (see FIPS Mode Out-of-Box Operation).
4. X.509 certificate and key files for wireless authentication must be loaded in the fips table (see FIPS: Wireless Authentication).

Enable AES Encryption

Choose the same AES encryption setting on both AN-80i systems.

CLI: set encmode: n

(where: 0 - None, 1 - (Redline) 64-Bit, 2 - AES 128, 3 - AES 192, 4 - AES 256)

Web: Configuration screen -> Wireless Security Configuration

Encryption Type: None, (Redline) 64-Bit, AES 128, AES 192, AES 256

Important: A data link can be established only between systems with identical encryption settings.

8.3.4 FIPS: SSH for Secure CLI

SSH is a standard feature that provides secure access when using the command line interface (CLI) to manage AN-80i equipment. SSH uses public-key cryptography to authenticate users and provide secure access over an unsecured network. Use an SSH client (e.g., OpenSSH, Putty, etc) to access an AN-80i using SSH. When SSH is required, TELNET (unsecured access) should be disabled.

It is recommended that system operators use a commercially available tool to generate a unique DSA key, and to load the private key into the FIPS (fips) table before using the SSH feature in a production environment.

Out-of-Box Operation

The AN-80i provides out-of-box SSH in FIPS mode. At reboot, the AN-80i checks the FIPS (fips) table SSH DSA key (dsa_key_<mac>.pem) entry, and if this entry is empty (no key), the AN-80i automatically generates a new temporary DSA key that is used until the next reboot.

The self-generated key appears in the FIPS (fips) table, but is not permanent and a new key is generated on each reboot. This feature is disabled when a user-generated key has been loaded, or a key has been created using the CLI 'generate' command.

Enable SSH

SSH is disabled by (factory) default. Use the CLI or Web interface to enable SSH:

Command: set ssh on

Web interface: Configuration screen -> Ethernet: SSH Enable ☑

Note: When using the self-generated key, a warning message may be displayed, based on the SSH client security settings (e.g., *'Warning: Potential Security Breach. The servers host key does not match ...'*). The operator has full access to the secure CLI interface.

Loading an SSH Key File

Use the following steps to load user-generated X.509 certificate and key files:

1. Use a comm ercially available tool to create the required key file. The DSA key file must conform to the following:
   - Maximum key size is 2048 bits
   - Key filename must be in the following format:

     dsa_key_<mac>.pem
2. Copy the key file to the default directory on a TFTP server.
3. Use the CLI 'load' command to load the SSH DSA key into the FIPS (fips) table. It is recommended to use the local Ethernet port when transferring encryption keys and certificates to the AN-80i.
4. Reboot the AN-80i to activate changes to the key files.
5. Login to the AN-80i and verify the files have been successfully loaded.

Example

Use TFTP server at IP address 192.168.25.10 to load an SSH key file for the AN-80i with MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.10 dsa_key_00-09-02-01-C1-9A.pem fips tftp
192.168.25.2# show files fips
    dsa_key.pem     size=672      md5=fa9bd7a1f465fd7e9fed30150b0608c4
192.168.25.2#
192.168.25.2# reboot
```

SSH Key Generate Utility

Use the Command 'generate sshkey dsa' to create a DSA key and save this file in the FIPS (fips) table. This key file will be persistent through reboots. After executing the generate command, the AN-80i must be rebooted to activate the new key.

Example

Generate a new DSA key file.

```
192.168.25.2# generate sshkey dsa
192.168.25.2# reboot
```

8.3.5 FIPS: HTTPS for Secure Web

HTTPS (SSL) is a standard feature on all An-80i systems. HTTPS uses authentication and encryption to provide secure access over an unsecured network. When HTTPS is required, HTTP (unsecured access) should be disabled.

Out-of-box Operation

Out-of-box, HTTPS access does not meet the security standards for FIPS security mode (embedded certificate and key are identical for all units). Each AN-80i system to use HTTPS in FIPS mode must meet the following requirements:

1. AN-80i software with FIPS support is loaded and operational.
2. FIPS mode must be active (see FIPS Mode Out-of-Box Operation).
3. X.509 certificate and key files for HTTPS (SSL) must be loaded in the FIPS table.

It is recommended to use the local Ethernet port when transferring encryption keys and certificates to the AN-80i.

Loading HTTPS (SSL) Certificate and Key Files

Use the following steps to load user-generated X.509 certificate and key files:

1. Use a commercially available tool to create the required certificate and key files.

   The X.509 certificate file must conform to the following:

   - Maximum file size is 1400 bytes
   - Subject must match the access method (e.g., IP or name)
   - Filename must be formatted as follows:

     ssl_cert_<mac>.pem

   The SSL (RSA) key file must conform to the following:

   - Maximum 2048 bits.
   - Filename must be formatted as follows:

     ssl_key_<mac>.pem

2. Copy the key files to the default directory on a TFTP (or SFTP) server.
3. Use the CLI 'load' command to load the RSA key and certificate.
4. Use the command 'show files fips' to verify the files have been successfully loaded.
5. Reboot the AN-80i to activate changes to the key files. HTTPS will be available after the system reboot is completed.

Example

Load HTTPS (SSL) key and certificate files from the TFTP server at 192.168.25.1 to the AN-80i having MAC address 00 09 02 01 C1 9A.

```
192.168.25.2# load file 192.168.25.1 ssl_cert_00-09-02-01-C1-9A.pem fips tftp
192.168.25.2# load file 192.168.25.1 ssl_key_00-09-02-01-C1-9A.pem fips tftp
192.168.25.2# show files fips
    dsa_key.pem      size=672      md5=fa9bd7a1f465fd7e9fed30150b0608c4
    usr_ssl_key.der  size=1194     md5=1c5c5ddd0f08604a3b48cf41a8570557
    usr_ssl_cert.der size=1144     md5=ff0ce6923fc67a02d1e7bc6fa4856f94
192.168.25.2# reboot
```

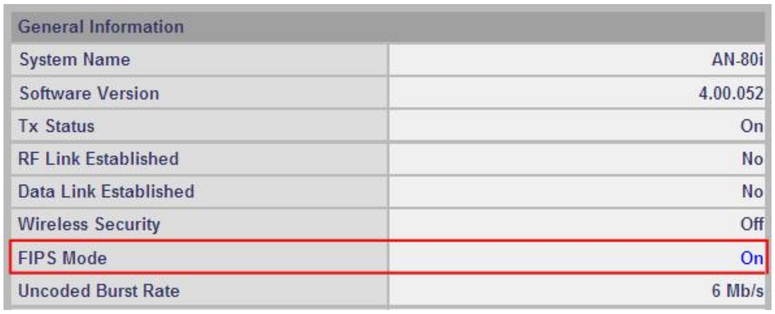
Enable HTTPS (SSL) Access

If the certificate and key files do not exist in the fips table, HTTPS is automatically disabled when the AN-80i is changed to FIPS mode.

Enter the Command 'set https on' to enable HTTPS. Use the Command 'save config' to save this setting and activate changes.

FIPS Status Summary Screen

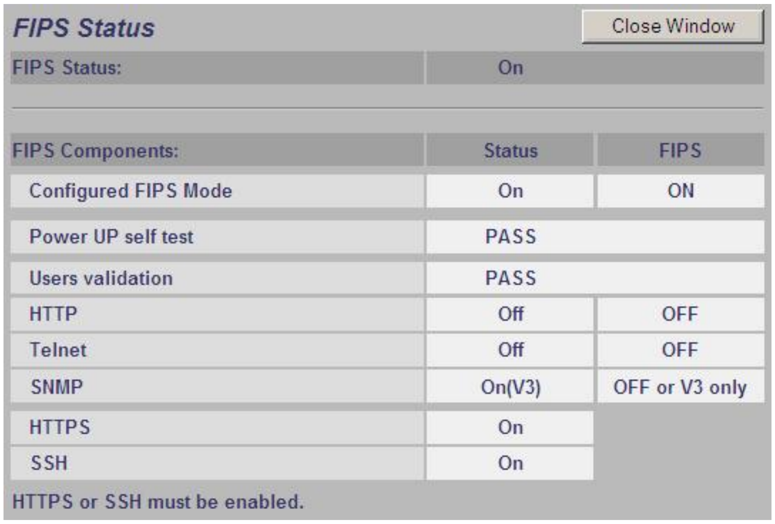
The FIPS status screen is displayed in the Web GUI by clicking System Status in the main menu, locating FIPS Mode and then clicking on the status (Off/On) link.



General Information	
System Name	AN-80i
Software Version	4.00.052
Tx Status	On
RF Link Established	No
Data Link Established	No
Wireless Security	Off
FIPS Mode	On
Uncoded Burst Rate	6 Mb/s

Fig. 55: Security - System Status - FIPS Status

The FIPS Status screen provides a summary of all FIPS related operations, policies, and parameter settings. The FIPS Mode status selection is available only in FIPS-enabled systems (see FIPS Mode Out-of-Box Operation).



FIPS Status

FIPS Status:	On	
FIPS Components:	**Status**	**FIPS**
Configured FIPS Mode	On	ON
Power UP self test	PASS	
Users validation	PASS	
HTTP	Off	OFF
Telnet	Off	OFF
SNMP	On(V3)	OFF or V3 only
HTTPS	On	
SSH	On	

HTTPS or SSH must be enabled.

Fig. 56: Security - FIPS Status - FIPS Mode Active

8.3.6 FIPS Behavior

Certificate and Key Files

When FIPS mode is active, only certificate and key files in the FIPS (fips) table are used by the AN-80i. The user (usr) table is accessible, but is not used in FIPS mode (see FIPS Mode Out-of-Box Operation). Certificate and key files can be loaded and viewed only by using SSH (see SSH for Secure CLI).

Software Upgrade

The FIPS certified software from Redline is supplied as a digitally signed software binary file (*.sbin). When the AN-80i is running a version of digitally signed software (*.sbin), the 'Upload Software' function is restricted to loading only digitally signed software binary files.

Component Integrity Check

At power-up and reboot, the AN-80i performs tests on hardware and software components to detect tampering. The AN-80i is allowed to start only if all hardware and firmware components pass the related integrity check and both the active and alternate software images pass the integrity check. If any integrity test fails, a long reset must be performed and the factory defaults must be saved to restore operation of the AN-80i.

Long Reset

If the operator can not access the AN-80i management interface (unknown IP, username, and/or password), a long reset operation must be performed to provide access using the default IP, username and password. The long reset can only be invoked by an operator having physical access to the AN-80i Ethernet port and power source (e.g., PoE adapter). Wireless service is interrupted while the system is powered-off and then rebooted.

If the operator successfully logs in during the long reset opportunity, FIPS mode is disabled for the duration of the login session (Telnet and HTTP are enabled). FIPS mode operation is restored following the next reboot unless prevented by changes to the configuration. If the operator fails to login during the long reset opportunity, the AN-80i reboots automatically and FIPS mode will be active.

The FIPS mode setting is disabled in the running configuration during a long reset. The FIPS mode will be permanently disabled if the command 'save config' is issued during the long reset session.

Runtime Keys and Certificate Files

The following tables are used to store keys and certificates. Each table provides storage for a specific function (e.g., usr table for standard security mode operation). Key files and certificates are loaded into the runtime (run) table during each system reboot. The runtime table is populated at boot time according to the following policies:

1. For each file type, the user (usr/fips) file (if present) has the highest priority. The file is loaded from the user (usr) table or FIPS (fips) table based on the operational mode:

   Standard Mode: Load files from the user (usr) table.

   FIPS Mode: Load files from the FIPS (fips) table.
2. The factory (fact) file is loaded when there is no user file.
3. Embedded files are used for HTTPS (ssl_cert<mac>.pem and ssl_key<mac>.pem) when these files do not exist in the user/FIPS or factory tables. The embedded key and certificate are identical for all AN-80i units. The embedded certificate authority (CA) can not be displayed or changed by the user.
4. A generated file is used for SSH (dsa_key<mac>.pem) when this file does not exist in the user/fips or factory tables. The generated key is random for all AN-80i units.
5. The factory files can not be modified or deleted by the user.

Table 54: Security: Runtime (run) Keys and Certificates

dsa_key_<mac>.pem	Standard mode: Ethernet: SSH: DSA Key
ssl_cert_<mac>.pem	Standard mode: Ethernet: HTTPS: SSL X.509 Certificate
ssl_key_<mac>.pem	Standard mode: Ethernet: HTTPS: SSL Key
usr_wacert_<mac>.der	Standard mode: Wireless: Authentication: X.509 Authority
usr_wcert_<mac>.der	Standard mode: Wireless: Authentication: X.509 Unit Certificate
usr_wkey_<mac>.der	Standard mode: Wireless: Authentication: RSA Key

Table 55: Security: User (usr) Keys and Certificate Files	
dsa_key_<mac>.pem	Standard mode: Ethernet: SSH: DSA Key
ssl_cert_<mac>.pem	Standard mode: Ethernet: HTTPS: SSL X.509 Certificate
ssl_key_<mac>.pem	Standard mode: Ethernet: HTTPS: SSL Key
usr_wacert_<mac>.der	Standard mode: Wireless: Authentication: X.509 Authority
usr_wcert_<mac>.der	Standard mode: Wireless: Authentication: X.509 Unit Certificate
usr_wkey_<mac>.der	Standard mode: Wireless: Authentication: RSA Key

Table 56: Security: FIPS (fips) Key and Certificate Files	
dsa_key_<mac>.pem	FIPS mode: Ethernet: SSH: DSA Key
ssl_cert_<mac>.pem	FIPS mode: Ethernet: HTTPS: SSL X.509 Certificate
ssl_key_<mac>.pem	FIPS mode: Ethernet: HTTPS: SSL Key
usr_wacert_<mac>.der	FIPS mode: Wireless: Authentication: X.509 Authority Certificate
usr_wcert_<mac>.der	FIPS mode: Wireless: Authentication: X.509 Unit Certificate
usr_wkey_<mac>.der	FIPS mode: Wireless: Authentication: RSA Key

Table 57: Security: Factory (factory) Key and Certificate Files	
dsa_key_<mac>.pem	FIPS mode: Ethernet: SSH: DSA Key
usr_wcert_<mac>.der	FIPS mode: Wireless: Authentication: X.509 Unit Certificate
usr_wkey_<mac>.der	FIPS mode: Wireless: Authentication: RSA Key

Chapter 9

9 Appendices

9.1 AN-80i Technical Specifications

Table 58: Spec. - AN-80i Technical Specifications

T35 Radio:	
RF Band:	3.320 - 3.798 GHz (TDD) [1]
Rx Sensitivity:	-90 dBm @ 3 Mbps max.
Center Freq. Steps:	1 MHz [2]
Channel Size:	PTP: 3.5, 5, 7, 10, 14, 20, 28, 40 MHz (software selectable) [1] PMP: 3.5, 5, 7, 10, 14, 20 MHz (software selectable) [1]
T49 Radio:	
RF Band:	4.900 - 5.350 GHz (TDD) [1]
Rx Sensitivity:	-88 dBm @ 3 Mbps max.
Center Freq. Steps:	2.5 MHz [2]
Channel Size:	PTP: 5, 10, 20, 40 MHz (software selectable) [1] PMP: 5, 10, 20 MHz (software selectable) [1]
T54 Radio:	
RF Band:	5.470 - 5.725 GHz (TDD) [1]
Rx Sensitivity:	-85 dBm @ 3 Mbps max.
Center Freq. Steps:	2.5 MHz [2]
Channel Size:	PTP: 5, 10, 20, 40 MHz (software selectable) [1] PMP: 5, 10, 20 MHz (software selectable) [1]
T58 Radio:	
RF Band:	5.725 - 5.850 GHz (TDD) [1]
Rx Sensitivity:	-85 dBm @ 3 Mbps max.
Center Freq. Steps:	2.5 MHz [2]
Channel Size:	PTP: 5, 10, 20, 40 MHz (software selectable) [1] PMP: 5, 10, 20 MHz (software selectable) [1]
System Capability:	LOS, Optical-LOS, and Non-LOS
RF:	
Rx Dynamic Range:	> 50 dB
Maximum Tx Power:	25 dBm (Ave. Max.) [1,3]
Minimum Tx Power:	10 dBm Automatic Transmit Power Control (ATPC) Dynamic Frequency Selection (DFS) Automatic link distance ranging Up to 80 km (50 mi) line-of-sight @ 48 dBm EIRP [1, 6]
Data Rate:	
PTP:	Up to 90 Mbps average Ethernet rate (40 MHz channel) [4]
PMP:	Up to 48 Mbps average Ethernet rate (20 MHz channel) [4]
PoE Cable:	Up to 91.5 m (300 ft) [5]
Over The Air Encryption:	Proprietary private key encryption, AES-128 standard AES-256 [8]

Table 58: Spec. - AN-80i Technical Specifications

Node Authentication:	X.509 certificates
Network Attributes:	802.3x Ethernet flow control DHCP pass-through, transparent bridge 802.1p network traffic prioritization [6] 802.1Q VLAN classification [7]
Modulation/Coding Rates:	BPSK 1/2, BPSK 3/4, QPSK 1/2, QPSK 3/4, 16 QAM 1/2, 16 QAM 3/4, 64 QAM 2/3 and 64 QAM 3/4
MAC:	Concatenation Time Division Multiple Access (TDMA) Automatic Repeat Request (ARQ) error correction Dynamic adaptive modulation (bi-dir. burst to burst auto select) Packet fragmentation [7]
Network Services:	Transparent to 802.3 services and applications
Duplex Technique:	Dynamic TDD (time division duplex)
Wireless Transmission:	OFDM (orthogonal frequency division multiplexing)
Network Connection:	10/100 Ethernet (RJ-45)
System Configuration:	HTTP/HTTPS (Web) interface, SNMP, SSH, Telnet (CLI), TFTP
Network Management:	SNMP v2c or v3: standard and proprietary MIBs
Power Requirements:	Standard IEEE 802.3af (15.4 W Max.) PoE
Operating Temperature:	-40 C to 60 C
Dimensions/Weight:	289 mm x 190 mm x 51.5 mm (11.38 in x 7.50 in x 2.03 in)
Ingress Protection:	IP67
Weight:	2 Kg (4.4 lb) without bracket or antenna
Storage Temperature:	-50 C to 70 C
Compliance:	
Safety:	IEC, EN, and UL/CSA 60950
EMC:	EN 301 489-1, EN 301 489-17
T58 radio, 5.8 GHz:	IC RSS-210, FCC part 15, ETSI EN 302 502
T54 radio, 5.4 GHz:	IC RSS-210, FCC part 15, ETSI EN 301 893
T49 radio, 4.9 GHz:	IC RSS-111, FCC part 15/90, ETSI EN 301 893
T35 radio, 3.5 GHz:	IC RSS-192, FCC Part 15/90, ETSI EN 302 326-2
Other:	OMAN-TRA: 5.4 GHz: R/1213/09 D080214 5.8 GHz: R/1214/09 D080214

[1] Limited by regional regulations.
See Table 73: Spec. - Regional Identification Codes on page 144 for available channels.

[2] Center frequency is dependent on region.

[3] Maximum power based on radio type, modulation, and coding.

[4] Actual Ethernet data throughput is dependent on: protocols, packet size, burst rate, transmission latency, and link distance.

[5] With lightning arrestor installed.

[6] PTP Only

[7] PMP Only

[8] Purchased Option

Specifications are subject to change without notice.

9.2 Antenna & Mounting Bracket Matrix

9.2.1 3 GHz Antenna & Brackets

The following table lists antennas and mounting brackets available from Redline.

Table 59: Spec. - AN-80i 3 GHz Antenna / Mounting Bracket Matrix

Redline Order # (Part Number)	Gain (dBi)	Type	Redline Mounting Bracket
A1815MTDF (48-00077-01)	18.5	15° panel, V/H	80i-LW-MNT
A2408MTF (48-00009-00)	24	8° panel, V/H	80i-HD-MNT
A2FT2509LTP (48-00073-00)	25	9° parabolic	80i-SA-MNT
A3FT2906LTP (48-00074-00)	29	6° parabolic	80i-SA-MNT
PA14120EAS (48-00059-00)	14	120° panel, V/H	80i-HD-MNT
PA14120EASH (48-00060-00)	14	120° panel, V/H	80i-HD-MNT
PA1590EAS (48-00052-00)	15	90° panel, V/H	80i-HD-MNT
PA1590EASH (48-00053-00)	15	90° panel, V/H	80i-HD-MNT
PA1660EASH (48-00051-00)	16	60° panel, H	80i-HD-MNT
PA1760EAS (48-00050-00)	17	60° panel, V	80i-HD-MNT

9.2.2 5 GHz Antenna & Brackets

The following table lists antennas and mounting brackets available from Redline.

Table 60: Spec. - AN-80i 5 GHz Antenna / Mounting Bracket Matrix

Redline Order # (Part Number)	Gain (dBi)	Type	Freq. (GHz)					Redline Mounting Bracket
			4.90 - 5.00	5.15 - 5.35	5.25 - 5.35	5.4	5.8	
A12015EAS (48-00065-00)	15	120° panel, V	✓	✓	✓	✓	✓	80i-HD-MNT
A2209MTFW (48-00071-00)	22	9° panel, V/H	✓	✓	✓	✓	✓	80i-LW-MNT 80i-HD-MNT
A2804MTFW (48-00070-00)	28	4.5° panel, V/H	✓	✓	✓	✓	✓	80i-HD-MNT
A2906PWP (48-00063-00)	29	6° parabolic	✓	✓	✓	✓	✓	80i-SA-MNT
A3204PWP (48-00064-00)	32	4° parabolic	✓	✓	✓	✓	✓	80i-SA-MNT
A3403RWP (48-00033-00)	34.6	3.4° parabolic			✓	✓	✓	80i-SA-MNT
A36009MMO (48-00048-01)	9	360° omni		✓	✓	✓	✓	80i-SA-MNT
A6017EAS (48-00067-00)	17.5	62° panel, V	✓	✓	✓	✓	✓	80i-HD-MNT
A9016EAS (48-00066-00)	16.6	90° panel, V	✓	✓	✓	✓	✓	80i-HD-MNT

9.2.3 Legacy Products

The following products are listed for reference only. These items are discontinued and not available to order from Redline.

Table 61: **Spec. - AN-80i Legacy Antenna / Mounting Bracket Matrix**

Redline Order # (Part Number)	Gain (dBi)	Type	Freq. (GHz)						Redline Mounting Bracket
			3.3 3.6	4.90 - 5.00	5.15 - 5.35	5.25 - 5.35	5.4	5.8	
A12015MTS	15	120° panel			✓	✓	✓	✓	80i-HD-MNT
A2014ARF	20	13.8° panel	✓						80i-HD-MNT
A2209MTFD	22	9° panel			✓	✓	✓	✓	80i-LW-MNT 80i-HD-MNT
A2212AWFD	22	12° panel			✓	✓	✓	✓	80i-LW-MNT 80i-HD-MNT
A2212RWP	22	12° parabolic				✓	✓	✓	80i-SA-MNT
A2310AWF	23	10° panel			✓	✓	✓	✓	80i-HD-MNT
A2510PWP	25	10° panel	✓						80i-HD-MNT
A2804MTF	28	4.5° panel			✓	✓	✓	✓	80i-HD-MNT
A2806RWP	28	6.2° parabolic				✓	✓	✓	80i-SA-MNT
A3104RWP	31.2	4.2° parabolic				✓	✓	✓	80i-SA-MNT
A6015MTS	16	60° panel			✓	✓	✓	✓	80i-SA-MNT
A6017RWS	17	60° panel				✓	✓	✓	80i-SA-MNT
A9014MTS	14	90° panel			✓	✓	✓	✓	80i-SA-MNT
A9016RWS	16	90° panel				✓	✓	✓	80i-SA-MNT

9.3 ETSI Certified Antennas

The RF output power and selection must be professionally programmed and installed by the manufacturer or a trained professional installer.

9.3.1 5.8 GHz Radio: ETSI Certified Antennas

The following table lists ETSI certified 5.8 GHz antennas. Operation is restricted to 10 MHz and 20 MHz channel operation only.

Table 62: Spec. - ETSI Certified Antennas: 5.8 GHz Operation

Redline Order # (Part Number)	Gain (dBi)	Antenna Type	App.	Tx Power Setting (dBm)
A12015EAS (48-00065-00)	15	120°, 4.9-5.9 GHz, sector flat panel	PMP	9
A2209MTFW (48-00071-00)*	22	9°, 4.9-5.875 GHz, flat panel	PTP	-1
A36009MMO (48-00048-01)	9	360°, 5.0 - 6.0 GHz, omni directional	PMP	13
A6017EAS (48-00067-00)	17.5	62°, 4.9-5.9 GHz, sector flat panel	PMP	5
A9016EAS (48-00066-00)	16.6	90°, 4.9-5.9 GHz, sector flat panel	PMP	7

9.3.2 5.4 GHz Radio: ETSI Certified Antennas

The following table lists ETSI certified 5.4 GHz antennas.

Table 63: Spec. - ETSI Certified Antennas: 5.4 GHz Operation

Redline Order # (Part Number)	Gain (dBi)	Antenna Type	App.	Tx Power Setting (dBm)
A12015EAS (48-00065-00)	15	120°, 4.9-5.9 GHz, sector flat panel	PMP	5
A2209MTFW (48-00071-00)	22	9°, 4.9-5.875 GHz, flat panel	PTP	8
A2804MTFW (48-00070-00)	28	4.5°, 4.9-5.925 GHz, flat panel	PTP	1
A2806RWP (48-00031-00)	28	6.2°, 5.250-5.850 GHz, parabolic	PTP	1
A2906PWP (48-00063-00)	29	6°, 4.900-5.875 GHz, parabolic	PTP	10
A3104RWP (48-00032-00)	31.2	4.2°, 5.250-5.850 GHz, parabolic	PTP	-1
A3204PWP (48-00064-00)	32	4°, 4.900-5.875 GHz, parabolic	PTP	-3
A36009MMO (48-00048-01)	9	360°, 5.0 - 6.0 GHz, omni	PMP	10
A6017EAS (48-00067-00)	17.5	62°, 4.9-5.9 GHz, sector flat panel	PMP	2
A9016EAS (48-00066-00)	16.6	90°, 4.9-5.9 GHz, sector flat panel	PMP	3

9.3.3 5.15 - 5.35 GHz Radio: ETSI Antennas

The following table lists ETSI certified 5.15-5.35 GHz antennas.

Table 64: Spec. - ETSI Certified Antennas: 5.15 - 5.35 GHz Operation

Redline Order # (Part Number)	Gain (dBi)	Antenna Type	App.	Tx Power Setting (dBm)
A12015EAS (48-00065-00)	15	120°, 4.9-5.9 GHz, sector flat panel	PMP	3
A2209MTFW (48-00071-00)	22	9°, 4.9-5.875 GHz, flat panel	PTP	-4
A6017EAS (48-00067-00)	17.5	62°, 4.9-5.9 GHz, sector flat panel	PMP	0
A9016EAS (48-00066-00)	16.6	90°, 4.9-5.9 GHz, sector flat panel	PMP	2

9.3.4 3.3 - 3.8 GHz Radio: ETSI Certified Antennas

The following table lists ETSI certified 3.3 - 3.8 GHz antennas.

Table 65: Spec. - ETSI Antenna/Tx Power Setting Combinations

Redline Order # (Part Number)	Gain (dBi)	Description
A2014ARF (48-00054-00)	20	13.8°, 3.3-3.8 GHz, horizontal or vertical polarization
A2408MTF (48-00009-00)	24	8°, 3.3-3.8 GHz, horizontal or vertical polarization
A2FT2509LTP (48-00073-00)	25	9°, 3.3-3.6 GHz, parabolic
A3FT2906LTP (48-00074-00)	29	6°, 3.3-3.6 GHz, parabolic
PA14120EAS (48-00059-00)	14	120°, 3.3-3.8 GHz, vertical polarization only
PA14120EASH (48-00060-00)	14	120°, 3.3-3.8 GHz, horizontal polarization only
PA1590EAS (48-00052-00)	15	90°, 3.3-3.8 GHz, vertical polarization only
PA1590EASH (48-00053-00)	15	90°, 3.3-3.8 GHz, horizontal polarization only
PA1660EASH (48-00051-00)	16	60°, 3.3-3.8 GHz, horizontal polarization only
PA1760EAS (48-00050-00)	17	60°, 3.3-3.8 GHz, vertical polarization only

9.4 FCC & IC Certified Antennas

9.4.1 5.8 GHz Radio: FCC & IC Antennas

This device has been designed to operate with the antennas listed below, and having a maximum gain of 34.6 dBi.

Table 66: Spec. - FCC & IC Certified Antennas: 5.8 GHz PTP Operation

Redline Order # (Part Number)	Gain (dBi)	Description	App.	Ave. GUI Power Display (dBm)	Minimum Conducted Power (dBm)	Max Conducted Power (dBm)
A2209MTFW (48-00071-00)	22	9°, 4.9-5.875 GHz, flat panel	PTP	20	-12.7	26.2
A2804MTFW (48-00070-00)	28	4.5°, 4.9-5.925 GHz, flat panel	PTP	20	-12.7	26.2
A2906PWP (48-00063-00)	29	6°, 4.900-5.875 GHz, parabolic	PTP	20	-12.7	26.2
A3204PWP (48-00064-00)	32	4°, 4.900-5.875 GHz, parabolic	PTP	20	-12.7	26.2
A3403RWP (48-00033-00)	34.6	3.4°, 5.250-5.850 GHz, parabolic	PTP	20	-12.7	26.2

Table 67: Spec. - FCC & IC Certified Antennas: 5.8 GHz PMP Operation

Redline Order # (Part Number)	Gain (dBi)	Description	App.	Tx Power Setting (dBm)	Tx Peak Conducted Power (dBm)
A12015EAS (48-00065-00)	15	120°, 4.9-5.9 GHz, sector flat panel	PMP	9	19.4
A36009MMO (48-00048-01)	9	360°, 5.0 - 6.0 GHz, omni directional	PMP	13	20.3
A6017EAS (48-00067-00)	17.5	62°, 4.9-5.9 GHz, sector flat panel	PMP	5	14.9
A9016EAS (48-00066-00)	16.6	90°, 4.9-5.9 GHz, sector flat panel	PMP	7	17.2

Antennas not included in these lists or having a gain greater than 34.6 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The RF output power and selection must be professionally programmed and the equipment must be installed by the manufacturer or a trained professional installer.

9.4.2 5.4 GHz Radio: FCC & IC Antennas

This device has been designed to operate with the antennas listed below, and having a maximum gain of 22 dBi.

Table 68: Spec. - FCC & IC Certified Antennas: 5.47-5.725 GHz Operation

Redline Order # (Part Number)	Gain (dBi)	Description	Tx Power Setting (dBm)		
			10 MHz	20 MHz	40 MHz
A12015EAS (48-00065-00)	15	120°, 4.9-5.9 GHz, sector flat panel	7	7	7
A2209MTFW (48-00071-00)	22	9°, 4.9-5.875 GHz, sector, flat panel	7	7	7
A36009MMO (48-00048-01)	9	360°, 5.0 - 6.0 GHz, omni directional	7	7	7
A6017EAS (48-00067-00)	17.5	62°, 4.9-5.9 GHz, sector flat panel	7	7	7
A9016EAS (48-00066-00)	16.6	90°, 4.9-5.9 GHz, sector flat panel	7	7	7

Antennas not included in this list or having a gain greater than 22 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The RF output power and selection must be professionally programmed and the equipment must be installed by the manufacturer or a trained professional installer.

9.4.3 5.25 - 5.35 GHz Radio: FCC & IC Antennas

This device has been designed to operate with the antennas listed below, and having a maximum gain of 22 dBi.

Table 69: Spec. - FCC & IC Antennas: 5.25 - 5.35 GHz Operation

Redline Order # (Part Number)	Gain (dBi)	Description	App.	Tx Power Setting (dBm)		
				Channel Size		
				10 MHz	20 MHz	40 MHz
A12015EAS (48-00065-00)	15	120 deg., .9-5.9 GHz, sector flat panel	PMP	10	12	13
A2209MTFW (48-00071-00)	22	9°, 4.9-5.875 GHz, sector, flat panel	PTP	7	7	7
A36009MMO (48-00048-01)	9	360°, 5.0 - 6.0 GHz, omni directional	PMP	10	12	13
A6017EAS (48-00067-00)	17.5	62 deg., 4.9-5.9 GHz, sector flat panel	PMP	10	12	12
A9016EAS (48-00066-00)	16.6	90 deg., 4.9-5.9 GHz, sector flat panel	PMP	10	12	13

* FCC regulations require the DFS function be permanently enabled at the factory and can not be disabled by the installer/end-user when operating in the 5.25-5.35 GHz range.

Antennas not included in this list or having a gain greater than 22 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The RF output power and selection must be professionally programmed and the equipment must be installed by the manufacturer or a trained professional installer.

9.4.4 4.94 - 4.99 GHz Radio: FCC & IC Antennas

This device has been designed to operate with the antennas listed in the following table, and having a maximum gain of 32 dBi.

Table 70: Spec. - FCC & IC Antennas: 4.94 - 4.99 GHz Operation

Redline Order # (Part Number)	Gain (dBi)	Description	App.	Tx Power Settings (dBm)		
				Channel Size (MHz)		
				10	20	40*
A12015EAS (48-00065-00)	15	120 deg., .9-5.9 GHz, sector flat panel	PMP	18	20	N/A
A2906PWP (48-00063-00)	29	6 deg., 4.900-5.875 GHz, 2 ft parabolic	PMP	15	19	N/A
A3204PWP (48-00064-00)	32	4 deg., 4.900-5.875 GHz, 3 ft parabolic	PMP	13	16	N/A
A6017EAS (48-00067-00)	17.5	62 deg., 4.9-5.9 GHz, sector flat panel	PMP	18	20	N/A
A9016EAS (48-00066-00)	16.6	90 deg., 4.9-5.9 GHz, sector flat panel	PMP	18	20	N/A

* Industry Canada (IC) only -- FCC regulations do not allow use of 40 MHz channels.

Antennas not included in this list or having a gain greater than 32 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The RF output power and selection must be professionally programmed and installed by the manufacturer or a trained professional installer.

9.4.5 3.650-3.700 GHz Radio: FCC Antennas

The 3.650-3.700 GHz frequency range is a licensed band and operators must have a valid spectrum license to operate AN-80i equipment using this band in the USA.

Table 71: Spec. - FCC Antennas: 3.650-3.700 GHz

Redline Order # (Part Number)	Gain (dBi)	Description	Tx Power Setting for Channel (dBm)					
			3.5 MHz	5 MHz	7 MHz	10 MHz	14 MHz	20 MHz
A2014ARF (48-00054-00)	20	13.8 deg., 3.3-3.8 GHz horizontal or vertical polarization	15	17	18	20	21	23
A2408MTF (48-00009-00)	24	8 deg., 3.3-3.8 GHz horizontal or vertical polarization	11	13	14	16	17	19
A2FT2509LTP (48-00073-00)	25	9 deg., 3.3-3.8 GHz horizontal or vertical polarization	10	12	13	15	16	18
PA14120EAS (48-00059-00)	14	120 deg., 3.3-3.8 GHz vertical polarization only	20	23	24	25	25	25
PA14120EASH (48-00060-00)	14	120 deg., 3.3-3.8 GHz horizontal polarization	20	23	24	25	25	25
PA1590EAS (48-00052-00)	15	90 deg., 3.3-3.8 GHz vertical polarization only	20	22	23	25	25	25
PA1590EASH (48-00053-00)	15	90 deg., 3.3-3.8 GHz horizontal polarization	20	22	23	25	25	25
PA1660EASH (48-00051-00)	16	60 deg., 3.3-3.8 GHz horizontal polarization	19	21	22	24	25	25
PA1760EAS (48-00050-00)	17	60 deg., 3.3-3.8 GHz vertical polarization only	18	20	21	23	24	25

*Discontinued -- Not available to order from Redline.

This device has been designed to operate with the antennas listed in the following table, and having a maximum gain of 28 dBi. Antennas not included in this list or having a gain greater than 28 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The RF output power selection must be professionally programmed and the equipment must be installed by the manufacturer or a trained professional installer.

9.4.6 3.450-3.650 GHz Radio: IC Antennas

The 3.450-3.650 GHz frequency range is a licensed band and operators must have a valid spectrum license to operate AN-80i equipment using this band in the Canada.

Table 72: Spec. - IC Antennas: 3.450-3.650 GHz

Redline Order # (Part Number)	Gain (dBi)	Description
A2014ARF (48-00054-00)	20	13.8 deg., 3.3-3.8 GHz, horizontal or vertical polarization
A2408MTF (48-00009-00)	24	8 deg., 3.3-3.8 GHz, horizontal or vertical polarization
A2FT2509LTP (48-00073-00)	25	9 deg., 3.3-3.8 GHz, horizontal or vertical polarization
PA14120EAS (48-00059-00)	14	120 deg., 3.3-3.8 GHz, vertical polarization
PA14120EASH (48-00060-00)	14	120 deg., 3.3-3.8 GHz, horizontal polarization
PA1590EAS (48-00052-00)	15	90 deg., 3.3-3.8 GHz, vertical polarization
PA1590EASH (48-00053-00)	15	90 deg., 3.3-3.8 GHz, horizontal polarization
PA1660EASH (48-00051-00)	16	60 deg., 3.3-3.8 GHz, horizontal polarization
PA1760EAS (48-00050-00)	17	60 deg., 3.3-3.8 GHz, vertical polarization

This device has been designed to operate with the antennas listed in the following table, and having a maximum gain of 28 dBi. Antennas not included in this list or having a gain greater than 28 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The RF output power selection must be professionally programmed and the equipment must be installed by the manufacturer or a trained professional installer. The AN-80i supports operation using 3.5, 5, 7, 10, 14, 20, 28, and 40 MHz channels (software selectable). The following table lists IC certified antennas:

9.5 Regional Codes

The regional code is incorporated into the options key. This feature enforces compliance to regional regulatory statutes. The options keys (a string of numbers, letters, and dashes) enable AN-80i features including the maximum uncoded burst rate and frequency ranges (region codes). Options key are unique to a specific AN-80i (keyed to MAC address).

Table 73: Spec. - Regional Identification Codes

Regions	Band	Radio	DFS/CBP Required [1]	Channel Size (MHz)	Channel Step (MHz)	Start - End [2] (MHz)
Region 01						
CALA, Canada, China, Middle-East, US	US 5.8 ISM	T58	No	10	2.5	5730 - 5845
				20	2.5	5735 - 5840
				40	2.5	5745 - 5830
Region 02						
UK, Jersey, Norway	UK 5.8G	T58	Yes [3]	10	2.5	5730 - 5790 5820 - 5845
				20	2.5	5735 - 5785 5825 - 5840
Region 03						
EU	CE 5.4G	T54	Yes [4]	10	20	5500 - 5700
				20	20	5500 - 5700
				40	20	5500 - 5700
Region 04						
US	US 5.4 ICM	T54	Yes [5]	10	2.5	5475 - 5720
				20	2.5	5480 - 5715
				40	2.5	5490 - 5705
Region 05						
Canada	IC 5.4G	T54	Yes [6]	10	2.5	5475 - 5595 5655 - 5720
				20	2.5	5480 - 5590 5660 - 5715
				40	2.5	5490 - 5580 5670 - 5705
Region 06						
India	IN 5.8 G	T58	No	10	2.5	5830 - 5870
				20	2.5	5735 - 5865
				40	2.5	5845 - 5855
Region 07						
Denmark	DE 5.8 G	T58	Yes [8]	10	2.5	5750 - 5870
				20	2.5	5765 - 5865
Region 08						
US	US 4940 - 4990	T49	No	10	2.5	4945 - 4985
				20	2.5	4950 - 4980
	US 5.250 - 5.350		Yes [5]	10	2.5	5260 - 5340
				20	2.5	5265 - 5335
Region 09						
Canada	IC 4.9 G	T49	No [7]	10	2.5	4945 - 4985
				20	2.5	4950 - 4980
				40	2.5	4960 - 4970
Canada	IC 5.3 G		No [6]	10	2.5	5260 - 5340
				20	2.5	5265 - 5335
				40	2.5	5280 - 5320
Region 10						
Japan	JP 4.9 G	T49	No	10	2.5	4915 - 5055
				20	2.5	4920 - 5080

Table 73: Spec. - Regional Identification Codes

Regions	Band	Radio	DFS/CBP Required [1]	Channel Size (MHz)	Channel Step (MHz)	Start - End [2] (MHz)
Region 11						
EU	CE .2 G 5.155 - 5.245	T49	No	10	2.5	5155 - 5245
				20	2.5	5160 - 5240
				40	2.5	5170 - 5230
	CE 5.255 - 5.345		Yes [4]	10	2.5	5255 - 5345
				20	2.5	5260 - 5340
				40	2.5	5270 - 5330
Region 12						
US	US 5.260 - 5.350	T49	Yes [5]	10	2.5	5260 - 5340
				20	2.5	5265 - 5335
				40	2.5	5280 - 5320
Region 13						
Canada	IC 5.3 G	T49	No [6]	10	2.5	5260 - 5340
				20	2.5	5265 - 5335
				40	2.5	5280 - 5320
Region 14						
EU	CE 3.5 G	T35	No	3.5	1	3302 - 3798
				5	1	3303 - 3797
				7	1	3304 - 3796
				10	1	3305 - 3795
				14	1	3307 - 3793
				20	1	3310 - 3790
				28	1	3314 - 3786
				40	1	3320 - 3780
Region 15						
US	US 3.65 G	T35	Yes[9]	3.5	1	3652 - 3673
				5	1	3653 - 3672
				7	1	3654 - 3671
				10	1	3655 - 3670
				14	1	3657 - 3668
				20	1	3660 - 3665

Notes:

5. Where DFS is required by regional regulations, this function is permanently enabled at the factory and can not be disabled by the installer or end-user.
6. Center frequencies.
7. UK VNS 2107/ EN302 502
8. ETSI EN301893 v1.3.1
9. FCC Part 15
10. IC RSS-210
11. IC RSS-111
12. TKG § 55/EN302 502
13. CBP (Contention Based Protocol) as per FCC regulation CFR Part 90.1321

9.6 PMP Packet Classification

9.6.1 Classification at the Sector Controller

The AN-80i PMP deployment can be configured for use with VLAN tagged traffic, untagged traffic, or a combination these two types. Ingress packets received on the sector controller Ethernet port are classified according to the criteria in the following table. These descriptions do not include management traffic for the AN-80i sector controller or subscriber.

Table 74: Spec. - PMP Classification: Packet Received on SC Ethernet Port

VLAN tag matches a Service Group VID	
Known unicast address	Priority: Preserve original 802.1 priority. Tag: Remove outermost matching VLAN tag. Forward: To destination only. Rate: Downlink rate of member Service for this subscriber.
Unknown unicast address:	Priority: Preserve original 802.1 priority. Tag: Remove outermost matching VLAN tag. Forward: All Service Group members. Rate: Two modulation steps below the lowest rate currently in-use across all active Services
Multicast or broadcast address:	Priority: Preserve original 802.1 priority. Tag: Remove outermost matching VLAN tag. Forward: All Service Group members. Rate: Downlink rate of this Service Group.
VLAN tag *does not match any Service* Group VID -- OR -- untagged packet	
Pass through service group not defined:	Discard packet.
Pass through service group defined --- AND --- known unicast destination	Priority: Service Group default priority. Tag: Unchanged Forward: Destination only. Rate: Downlink rate of member Service for this subscriber.
Pass through service group defined --- AND --- unknown address (all types)	Priority: Service Group default priority. Tag: Unchanged Forward: All Service Group members. Rate: Two modulation steps below the lowest rate currently in-use across all active Services.
Pass through service group defined --- AND --- multicast or broadcast address	Priority: Service Group default priority. Tag: Unchanged Forward: All Service Group members. Rate: Downlink rate of this Service Group.

Table 75: **Spec. - PMP Classification: Packet Received on SC Wireless Interface**	
Service Group type: Tagged	
Known unicast address --- AND --- destination is Ethernet port	Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To sector controller Ethernet port[1].
Known unicast address --- AND --- destination is subscriber	Forward: Retransmit packet unmodified over the wireless interface to the destination subscriber. Rate: Downlink rate for member Service on this subscriber.
Multicast or broadcast	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group[2]. Rate: Downlink rate for Service Group. --- AND --- Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To sector controller Ethernet port[1].
Service Group type: Pass through	
Known unicast address --- AND --- destination is Ethernet port	Forward: Packet unmodified to the sector controller Ethernet port[1].
Known unicast address --- AND --- destination is a subscriber	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group[2]. Rate: Downlink rate for member Service on this subscriber.
Unknown unicast	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group[2]. Rate: Downlink rate is two modulation steps below the lowest rate currently in-use across all active Services. --- AND --- Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To sector controller Ethernet port[1].
Multicast or broadcast	Forward: Retransmit packet unmodified over the wireless interface to all members of this Service Group[2]. Rate: Downlink rate for Service Group. --- AND --- Forward: Packet unmodified to the sector controller Ethernet port[1].

Notes: 1 If sector controller Ethernet port is enabled, 2. If SS to SS Multicast enabled.

9.6.2 Classification at the Subscriber

The AN-80i PMP deployment can be configured for use with VLAN tagged traffic, untagged traffic, or a combination these two types. Ingress packets received on the subscriber Ethernet port are classified according to the criteria in the following table.

Table 76: Spec. - PMP Classification: Packet Received on SS Ethernet Port

VLAN tag matches a Service VID	
Known unicast	Priority: Preserve original 802.1 priority. Tag: Remove outermost matching VLAN tag. Forward: To sector controller. Rate: Uplink rate of Service matching this tag.
Unknown unicast:	Priority: Preserve original 802.1 priority. Tag: Remove outermost matching VLAN tag. Forward: To sector controller. Rate: Uplink rate of Service matching this tag.
Known multicast or broadcast:	Priority: Preserve original 802.1 priority. Tag: Remove outermost matching VLAN tag. Forward: To sector controller. Rate: Uplink rate of Service matching this tag.
VLAN tag *does not match any Service* VID -- OR -- untagged packet	
Pass through service group not defined:	Discard packet.
Pass through service group defined --- AND --- known unicast	Priority: Service Group default priority. Tag: Unchanged Forward: To sector controller. Rate: Uplink rate of (Pass through) member Service.
Pass through service group defined --- AND --- unknown unicast	Priority: Service Group default priority. Tag: Unchanged Forward: To sector controller. Rate: Uplink rate of (Pass through) member Service.
Pass through service group defined --- AND --- multicast or broadcast	Priority: Service Group default priority. Tag: Unchanged Forward: To sector controller. Rate: Uplink rate of (Pass through) member Service.

Notes: 1 If SS to SS Multicast enabled.

Table 77: Spec. - PMP Classification: Packet Received on SS Wireless Interface

Member of Service Group type: Tagged	
Any type	Priority: Use priority received with packet Tag: Add VLAN tag (outermost) for this Service (Q in Q). Forward: To subscriber Ethernet port.
Member of Service Group type: Pass through	
Any type	Forward packet unmodified to the subscriber Ethernet port ·

9.7 ID Map

Beginning with v13.xx, all IDs must comply to ranges listed in the following table. The 'load script ...' command rejects all ID references greater than 511.

Table 78: Spec. - Provisioning Table ID Ranges

Provisioning Type	Version 10.xx to 12.xx	Version 13.xx
	ID Range	ID Range
Link	4 - 1024	4 - 63
Group		64 - 95
Connection		95 - 511

Note: When the v13.xx software is run for the first time only, all existing provisioning IDs in the range 4 - 511 are automatically mapped to the new schema. All ID references greater than 511 are discarded.

9.8 Glossary Of Terms

Table 79: Spec. - Glossary

Term	Definition
Antenna Gain	The measure of antenna performance relative to a theoretical antenna called an isotropic antenna.
ARQ	Automatic Repeat Request. This is the protocol used over the air for error correction.
ATPC	Automatic Transmission Power Control. The sector controller-end system automatically adjusts the RF transmit level of both systems to optimize performance of the link.
Beamwidth	The angle of signal coverage provided by an antenna.
BFW	Broadband Fixed Wireless
Bps	Bits Per Second. Unit of measurement for the rate at which data is transmitted.
BPSK	Binary Phase Shift Keying
Channel	A communications path wide enough to permit a single RF transmission.
CIR	Committed information rate
dB	A ratio expressed in decibels.
dBi	A ratio, measured in decibels, of the effective gain of an antenna compared to an isotropic antenna.
dBm	Decibels above a milliwatt.
DFS	Dynamic Frequency Selection (DFS) can detect interference from other devices using the same frequency (especially radar) and automatically take a pre-selected action such as disable transmission or use alternative frequency.
DHCP	Dynamic Host Configuration Protocol. A DHCP server automatically issues IP addresses within a specified range to devices on a network.
Directional Antenna	An antenna that concentrates transmission power into one direction.
Encryption	For the purposes of privacy, the transformation of data into an unreadable format until reformatted with a decryption key.
Ethernet	A LAN architecture using a bus or star topology.
FD	Full Duplex. Refers to the transmission of data in two directions simultaneously.
FWA	Fixed Wireless Access
Gain	The ratio of the output amplitude of a signal to the input amplitude of a signal. Typically expressed in decibels (dB).
Gateway	A network point that acts as an entrance to another network.
GHz	Gigahertz. 1,000,000,000 Hz, or 1,000 MHz
GUI	Graphical User Interface
IP	Internet Protocol. See TCP/IP.
Isotropic	A theoretic construct of an antenna that radiates its signal 360 degrees both vertically and horizontally—a perfect sphere. Generally used as a reference.
LED	Light Emitting Diode
LOS	Line Of Sight. A clear direct path between two antennas, with no obstructions within the first Fresnel zone.
MAC	Media Access Control. A unique number assigned to a network device. Corresponds to ISO Network Model Layer 2 data link layer.
MHz	Megahertz. 1,000,000 Hz

Table 79: Spec. - Glossary

Term	Definition
Modem	MOdulator/DEModulator. A hardware device that converts digital data into analog and vice versa.
Modulation	Any of several techniques for combining user information with a transmitter carrier signal.
Multipath	The radio echoes created as a radio signal bounces off objects.
NVRAM	Non-volatile RAM. System parameters are stored in NVRAM. This data is not affected by powering off the system.
NLOS	Non Line Of Sight. Completely obstructed path between two antennas.
OFDM	Orthogonal Frequency Division Multiplexing. OFDM spreads data to be transmitted over a large number of orthogonal carriers.
OLOS	Optical Line Of Sight. A clear direct path between two antennas, with obstructions within the first Fresnel zone.
Packet	A bundle of data organized in a specific way for transmission. The three principal elements of a packet include the header, the text, and the trailer (error detection and correction bits).
PHY	Physical Layer. Provides for the transmission of data through a communications channel by defining the electrical, mechanical, and procedural specifications.
PIR	Peak Information Rate
PMP	Point to Multipoint
PTP	Point to Point
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
Receiver Sensitivity	A measurement of the weakest signal a receiver can receive and still correctly translate it into data.
RF	Radio Frequency
RSSI	Received Signal Strength Indication
Rx	Receiver
S/N	Signal to Noise Ratio
SINADR	Signal to noise and distortion ratio.
SSL	Secure Sockets Layer, a communications protocol, superseded by Transport Layer Security (TLS).
TCP/IP	Transmission Control Protocol/Internet Protocol The standard set of protocols used by the Internet for transferring information between computers, handsets, and other devices.
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for web browsing, e-mail, Internet faxing, instant messaging, and other data transfers.
Tx	Transmitter
UBR	Uncoded Burst Rate