ALEOS Configuration

User Guide

20080616
Rev 2.0 C

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless AirLink AirLink device are used in a normal manner with a well-constructed network, the Sierra Wireless AirLink AirLink device should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless AirLink AirLink device, or for failure of the Sierra Wireless AirLink AirLink device to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless AirLink AirLink device in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless AirLink AirLink device **MUST BE POWERED OFF**. The Sierra Wireless AirLink AirLink device can transmit signals that could interfere with this equipment.

Do not operate the Sierra Wireless AirLink AirLink device in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless AirLink AirLink device **MUST BE POWERED OFF**. When operating, the Sierra Wireless AirLink AirLink device can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless AirLink AirLink device may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless AirLink AirLink device while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product includes technology licensed from QUALCOMM® 3G.

Manufactured or sold by Sierra Wireless Inc. or its licensees under one or more patents licensed from InterDigital Group.

Copyright

Trademarks

AirCard® and Watcher® are registered trademarks of Sierra Wireless. Sierra Wireless™, AirPrime™, AirLink™, AirVantage™ and the Sierra Wireless logo are trademarks of Sierra Wireless.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh and Mac OS X are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Support Desk:	Phone:	1-877-231-1144
	Hours:	5:00 AM to 5:00 PM Pacific Time, Monday to Friday, except US Holidays
	E-mail:	support@sierrawireless.com
Sales Desk:	Phone:	1-510-624-4200 1-604-232-1488
	Hours:	8:00 AM to 5:00 PM Pacific Time
	E-mail:	MobileandM2Msales@sierrawireless.com
Post:	Sierra Wireless America 39677 Eureka Drive Newark, CA USA 94560 Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4	
Fax:	1-510-624-4299 1-604-231-1109	
Web:	www.sierrawireless.com	

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases:

www.sierrawireless.com

Revision History

Revision number	Release date	Changes
1.x	2009	ALEOS 4.0 documentation draft created.
2.x	2010	User Guide rebranded to current standards. ALEOS 4.0.7 release udates incorporated in this guide.

Contents

1: Introduction

1

Overview

ACEmanager™ is the free utility used to manage and configure the AirLink AirLink Device. It is a web application integrated in the ALEOS firmware. ACEmanager™ provides comprehensive configuration and control functionality to all AirLink gateways and routers.

Key benefits of ACEmanager includes:

- Login and configure device parameters
- Adjust network settings
- Change security settings
- Update events reporting

Since ACEmanager can be accessed remotely as well as local, the many features of ALEOS can be configured from any location.

A template can be created, after a single devices is configured and installed, to program other gateways and routers with the same parameter values. This enables quick, accurate deployment of large pools of devices.

Other key features include:

- Remote device configuration and control
- Update firmware
- Included with every AirLink gateway and router
- Secure login

About Documentation

Each chapter in the ALEOS User Guide is a section (a tab in the User Interface) of ACEmanager.

Chapters in this user guide explain:

- Parameter description in ACEmanager
- Relevant configuration details
- User scenarios for cetain sections in the guide

The following table is a snapshot of the chapters and the product they correspond to.

No.	Chapter Name	Description
1	**Introduction**	Relevant to all products
2	**Configuring your AirLink device**	Relevant to all products
2	**View Status**	Relevant to all products
3	**WAN/Cellular Configuration**	Relevant to all products
4	**LAN/WiFi Configuration**	Relevant to all products
5	**VPN Configuration**	Relevant to all products
6	**Security Configuration**	Relevant to all products
7	**GPS Configuration**	Only for PinPoint and MP line devices
8	**Serial Configuration**	Only for products which have a serial port
9	**Report Configuration**	Only for Raven line products
10	**Services Configuration**	Relevant to all products, except Low Power which is only PinPoint and MP lines
11	**I/O Configuration**	Different sections for different product lines have been captured for display of examples.
12	**Admin**	Relevant to all products
13	**Events Reporting Configuration**	Relevant to all products

This *User Guide* is provided as a PDF (Portable Document Format) file on the installation CD or from the Sierra Wireless support website.

Tools and Reference Documents

Command	Description
AirLink Device User Guide	This is the hardware document that describes how to: • Install the AirLink device hardware. • Connect the radio antennas. • Connect a notebook computer and other input/output (I/O) devices. • Install the software. • Interpret the LEDs on the AirLink device and the indicators.
ACEview User Guide	This document explains the use of this utility tools which is used monitor the connection state of a Sierra Wireless AirLink device and GPS or power status as applicable for MP and PinPoint line devices.
ACEnet User Guide	This document explains the use of ACEnet services for remote management of Sierra Wireless AirLink devices.

2: Configuring your AirLink device

After powering on the AirLink Device and ensuring that you have an IP-based connection set up (Ethernet, USB/net, DUN, etc). You can log on to ACEmanager by entering http://192.168.13.31:9191 in your browser or enter other IP addresses depending on the interface you select (As shown in the table below).

Interface	AirLink device	Connected Device
Ethernet Private default	192.168.13.31*	192.168.13.100
USB/NET	192.168.14.31	192.168.14.100
DUN	192.168.15.31	192.168.15.100
Wi-Fi*	192.168.17.31	192.168.17.100

*can be changed via ACEmanager

The default login credentials are:

- Login: user
- Password: 12345

To prevent others from changing the AirLink Device settings, you can change the ACEmanager password (please refer to the Admin chapter).

Figure 2-1: ACEmanager: Main Log In screen

Main Menu Tabs

The main menu, across the top of the display, for ACEmanager is as follows:

- Upload: Loads configured information, in the form of a template, to the device.

- Download: Saves and copies checked configuration to create a template. If none of the fields are checked, all fields are selected and saved automatically.
- Reboot: Reboots the device.
- Refresh All: Refreshes all the pages.

Configuring

To configure your AirLink device, you have two options. You can use the browser based ACEmanager, as detailed in this guide, or you can use a terminal emulator application such as HyperTerminal, PuTTY, or many others to enter AT commands for many of the configuration options.

Operation Modes

The AirLink device plays the part of a HOST when a computer or another device is connected directly to its port and routes data to/from the connected device to the cellular network.

Tip: *If you need to have multiple Ethernet connections, you can connect the AirLink device to a router, switch or hub for additional ports. T*

As the host, the AirLink device can use different communication modes:

Basic Host Modes

- **AT**: The AirLink device accepts and responds to standard AT commands.
- **PassThru**: Direct connection to internal hardware (OEM Module) of the AirLink device.
- **Telnet**: The AirLink device auto-answers TCP connections to allow terminal emulation using either a local connection or remotely using the cellular connection.

Tip: *By default, the AirLink device is in AT Mode and allows AT Commands to be entered via terminal connection (through the local port connection) or remotely (through the cellular network). PassThru Mode can only be exited by resetting the AirLink device. All serial modes are entered by use of a startup mode command.*

Serial Modes

- **PPP Mode**: The AirLink device uses PPP to communicate with a device or computer connected to the serial or USB port.
- **SLIP Mode**: The AirLink device uses SLIP to communicate with a device or computer connected to the serial or USB port.
- **UDP** and **UDP PAD**: Any data received on the serial port is assembled into UDP packets and sent to the session's associated IP address and Port (described later). Any responses received from the associated IP address

and port destined for the Device Port are unwrapped and sent out the serial port.

- **TCP** and **TCP PAD**: Any data received on the serial port is packaged into TCP messages and sent to the associated connection's IP address and Port (described later). Any data received from the TCP peer is unwrapped and sent out the serial port.

Data Communication

- **Public and Private Modes**: The method used by the AirLink device to pass an IP address to a connected device.
- **Keepalive**: How the AirLink device maintains its connection to the cellular network.

AT Mode

Using a terminal connection, AT commands can be used to configure the device, command it to do something, or query a setting. ACEmanager is a graphical user interface for most AT Commands and includes other parameters without AT counterparts..

- AT commands must always be terminated by **<CR>** (ASCII character 0x0D), a carriage return (pressing enter on the keyboard). Some may also include a new line or line feed **<LF>**.
- If **E=1** (Echo On), the AT command (including the terminating <carriage return) will be displayed (output) before any responses.
- Two settings affect the format of AT command output: **V** (Verbose) and **Q** (Quiet).
- If **Q=1** (Quiet On), no result codes are output whatsoever, so there is no response generated by a (non query) command.
- If **Q=0** (Quiet Off), result codes are output. The format of this output is then affected by the Verbose setting.

  If Quiet mode is off, the result code is affected as follows:

  For **V=1** (Verbose mode), the textual result code is surrounded by a carriage return and new line. Any AT query response is also surrounded by a carriage return and new line.

  For **V=0** (Terse mode), a numeric result code is output with a single trailing carriage return (no new line is output), while any AT query response is followed by a carriage return and new line (there is no preceding output).
- For example, possible output to the AT command “AT” with carriage return (assuming quiet mode is not on) is:

  carriage return - if V=0

  carriage return and new line OK another carriage return and new line - if V=1

Note: AT commands work for the port on which they are executed. For example, if the user types ATE1 and then AT&W using a USB/serial port connection, it will set the USB/serial port to Echo On but not the telnet connection or the RS232 serial port.

PassThru Mode

In PassThru mode, the AirLink device does not behave normally, all port communication is passed directly between the internal hardware and the computer connected directly to the device. This mode can be used to configure hardware-specific settings. For example, provisioning, troubleshooting, communicating with legacy equipment, etc.

Caution: *ALEOS is disabled in PassThru Mode. You cannot use most ALEOS specific commands while the device is in PassThru Mode. While in PassThru mode, you also cannot use ACEmanager or the USB port.*

Telnet Mode

In ACEmanager you can configure Telnet operation.

If you need to change the port for Telnet (for example, you have the default port blocked on your firewall), the option is on the **Services-Telne**t tab. The default telnet port is *2332*. You can also change the Telnet timeout, if the connection is idle, default *2* minutes. This is the internal telnet on the modem to pass AT commands and not TCP pad.

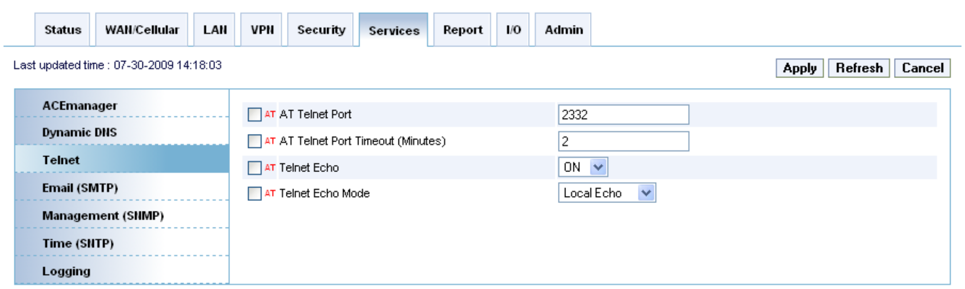


Figure 2-2: ACEmanager : Services- Telnet

Applying Templates

If you have a device configuration that works well for your needs, using ACEmanager, you can save that device's configuration as a template and then apply it to other Sierra Wireless AirLink devices.

1. Creating the Template with ACEmanager

a. Configure your AirLink device in ACEmanager.

b. Click on Apply (upper right hand) so that the conifguration settings write to the device.

c. Click on Download (menu tab) to save the template. A confirmation dialog box comes.

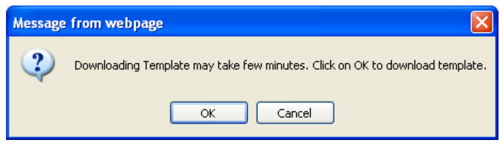


Figure 2-3: ACEmanager: Downlod template message

d. Click on Ok.

e. Click on Save button, once the File Download box displays.

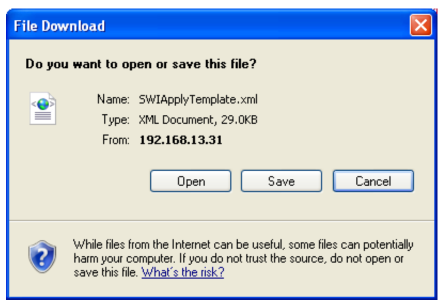


Figure 2-4: ACEmanager: File Download box

Note: Some of the configuration settings are specific to individual devices. You do not want to have those settings in your saved template otherwise the devices you configure with the template could cease to work with the cellular or local network.

f. Type in a file name that is descriptive of the template (so you can find it easily later) and save it to a location on your computer. Not all browsers will allow you to change the name of the file while downloading. As long as you do not change the extension, .xml, you can change the name and location of the file after it has downloaded.

The template will now download.

You can use a template you created yourself, using the steps above, or a template provided by your AirLink representative or someone in your company who has set up a device template. The template you wish to apply must be saved to your hard drive.

a. Load the template.

1. Connect to the device you want to configure using ACEmanager.
2. Click on the *Upload* button on the toolbar.

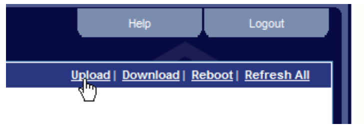


Figure 2-5: ACEmanager : Load

3. Browse and Select the template you have saved (you may need to change folders if you saved it to a different location).

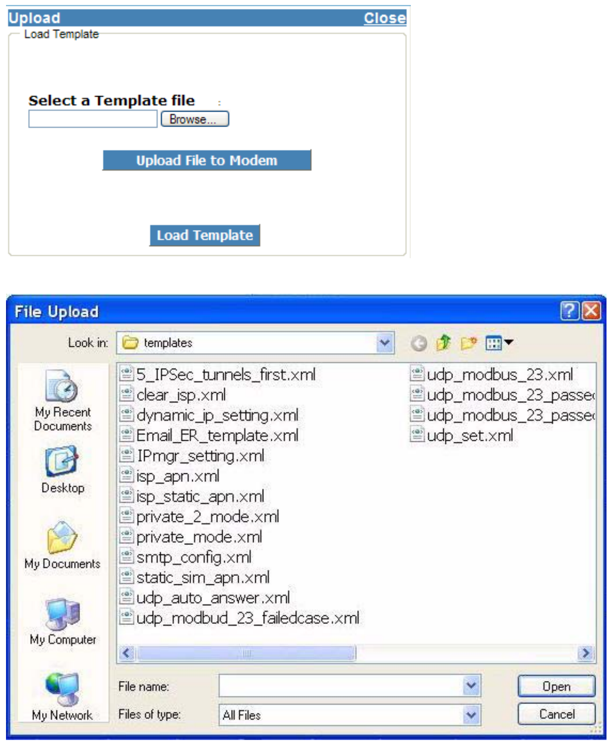


Figure 2-6: ACEmanager: select and load template

4. Click on Upload File to device.
5. Click on Load Template.

Tip: *After you load the template, it's best to go back over the ACEmanager tabs to make sure all the settings are what you require.*

6. Click the *Apply* button on the toolbar to write the configuration to the device.

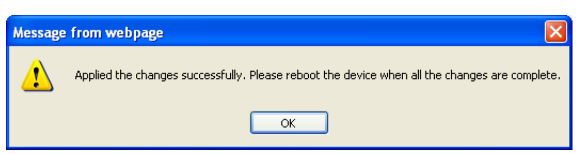


Figure 2-7: ACEmanager: Apply changes dialog box

7. Click on OK.
8. Click on the Reboot tab to reset the device.

Caution: *Many of the configuration settings will not take effect until the device has been reset.*

Tip: *You can use common settings on one device to configure those same settings on another device even of a different type. For example, you can use the serial settings of a device (such as PinPoint X or Raven X) to configure the serial settings of a AirLink device. Settings not applicable to the device on which you are loading the template, will be discarded, such as GPS settings for a Raven X which does not have GPS features.*

3: View Status

3

- Home
- WAN/Cellular
- LAN/WiFi
- VPN
- Security
- Services
- GPS
- Serial
- Applications
- About

The Status tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

Note: Categories not applicable to a device line will not appear as selectable. For example, Status>GPS will only be available for devices with the GPS feature set.

All of the fields in the “Status” group have read-only parameters and provide information about the AirLink Device. Depending on the individual settings and the onboard cellular module of the AirLink Device, the actual status pages may look different than the screenshots listed here. The individual status sections give an accurate view of the current running configuration of the AirLink Device. Refer to the following sections for information about the individual configuration options.

Home

The home section of the status tab is the first page displayed when you log in to ACEmanger. It shows basic information about the cellular network connection and important information about the device you would most likely want to see first.

Tip: *Refer to the "WAN / Cellular" section of this guide for information about configuring the cellular device.*

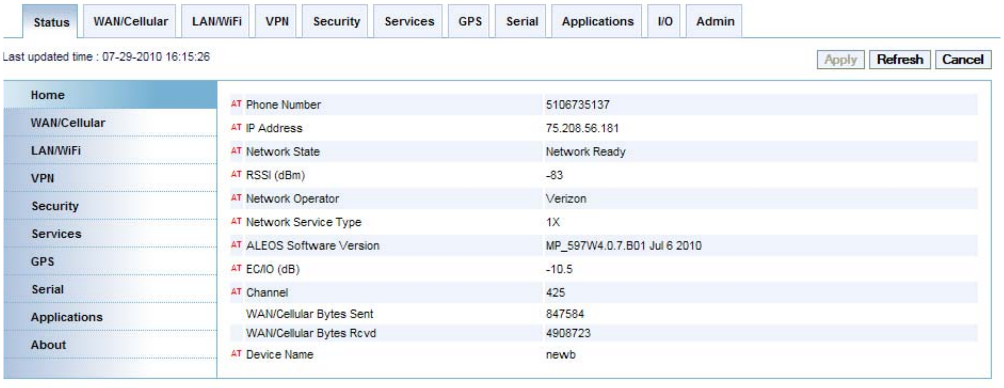


Figure 3-1: ACEmanager: Status - Home

Phone Number	The phone number (programmed into the device) is part of carrier account.
IP Address	The current IP address of the device reported by the internal module, generally obtained from your carrier. This is the address you can contact the AirLink device from the Internet if you have a mobile terminated or Internet accessible account.
Network State	Not Connected or Connected. Current state of the cellular radio.
RSSI	The current RSSI (Receive Signal Strength Indicator) of the AirLink device as a negative dBm value. Signal strength of the cellular signal. The lower the number, the better the signal strength. The exact numbers vary between cellular carriers. However, -40dBm to -70dBm usually means the AirLink Device is in an excellent coverage area.
Network Operator	Indicates the network the device is currently on.
Network Service Type	The type of service being used by the device, for example EV-DO Rev A or HSPA.
ALEOS Software Version	Software version of the ALEOS build currently installed in the device.
Channel	The current active CDMA/GSM channel number.
WAN/Cellular Bytes Sent	Number of bytes sent to the network since system startup.
WAN/Cellular Bytes Rcvd	Number of bytes received from the network since system startup.
Device Name	Name of the device.

WAN/Cellular

WAN/cellular status indicates specific information about the cellular connection including IP address and how much data has been used. Some of the information on this page is repeated on the home page for quick reference.

Figure 3-2: ACEmanager: Status - WAN/Cellular

Command	Description
Cellular IP Address	Cellular WAN IP Address.
Ethernet IP Address	Ethernet IP Address. This is present in WAN failover mode only.
Keepalive IP Address	The IP address that WAN keepalive uses to test cellular connectivity.
Keepalive Ping Time	The amount of time between keepalive pings in seconds.
DNS Server 1	First DNS IP addresses of cellular or Ethernet network.
DNS Server 2	Second DNS IP addresses of cellular or Ethernet.
Error Rate	The network bit error rate.
Bytes Sent	Number of bytes sent to the cellular network, since the system startup.
Bytes Received	Number of bytes received from the network, since system startup.
Packets Sent	Number of packets sent to the network , since system startup.
Packets Received	Number of packets received from the network, since system startup.

LAN/WiFi

This is the status of the local network. It lists information about the network and connected clients. If the device has WiFi, this section will also include WiFi status information.

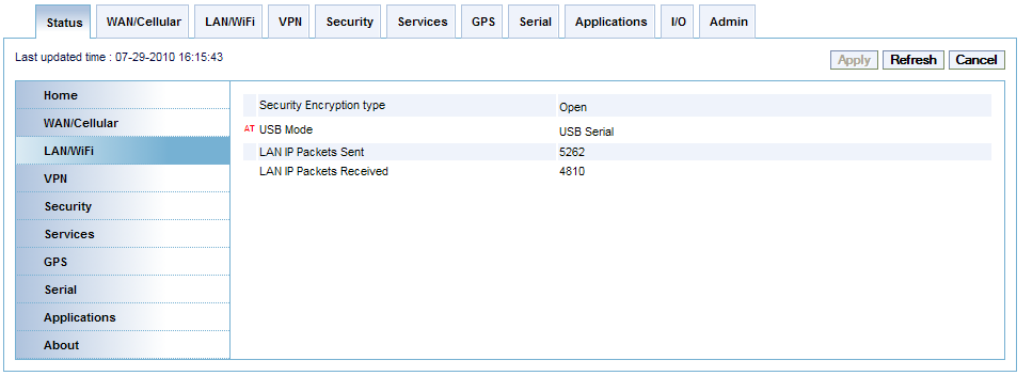


Figure 3-3: ACEmanager: Status - LAN/WiFi

Command	Description
USB Mode	Indicates which virtual mode of the USB port is set.
LAN IP Packets Sent	Number of IP packets sent to the host interface since the system startup.
LAN IP Packets Received	Number of IP packets received from the host interface since the system startup.

VPN

The VPN section gives an overview of the VPN settings and indicates whether a VPN connection has been made.

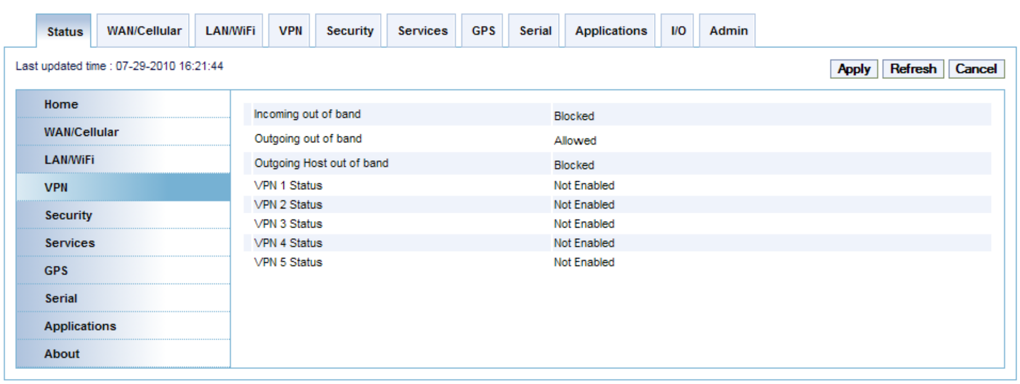


Figure 3-4: ACEmanager: Status - VPN

Command	Description
Incoming out of band	Incoming out of band.
Outgoing out of band	Outgoing ALEOS out of band.
Outgoing Host out of band	Outgoing Host out of band.
VPN 1 to 5	Disabled, Enabled, Connected. The status of the IPSec VPN client or GRE client.

Security

The security section provides an overview of the security settings on the AirLink Device.

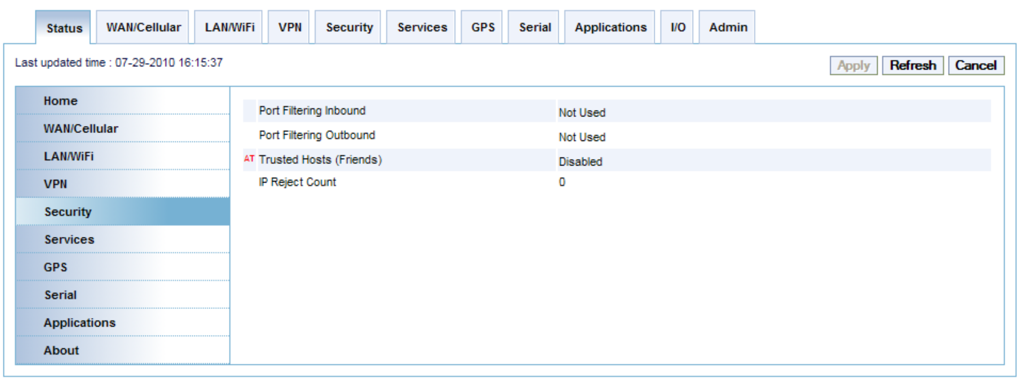


Figure 3-5: ACEmanager: Status - Security

Command	Description
Port Filtering Inbound	Enabled or disabled. Show status of inbound port filtering.
Port Filtering Outbound	Enabled or disabled. Show status of outbound port filtering.
Trusted Hosts	Disabled or Enabled. Accepts packets from only specific IPs.
IP Reject Count	Rejected IP Data.

Services

This section shows status of AirLink services, including the ACEmanager access level.

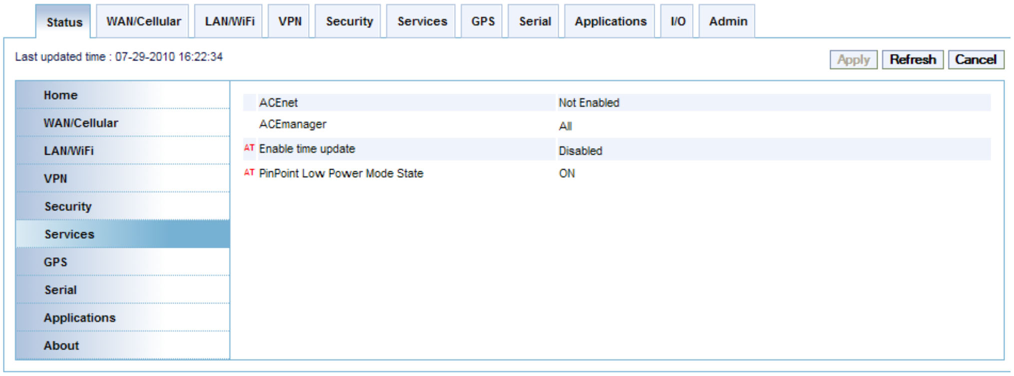


Figure 3-6: ACEmanager: Status - Services

Command	Description
ACEmanager	ACEmanager access mode.
Enable time update	Daily SNTP updates of the system time.

GPS

Note: The GPS tab that displays in ACEmanager, is applicable to PinPoint line and MP line devices.

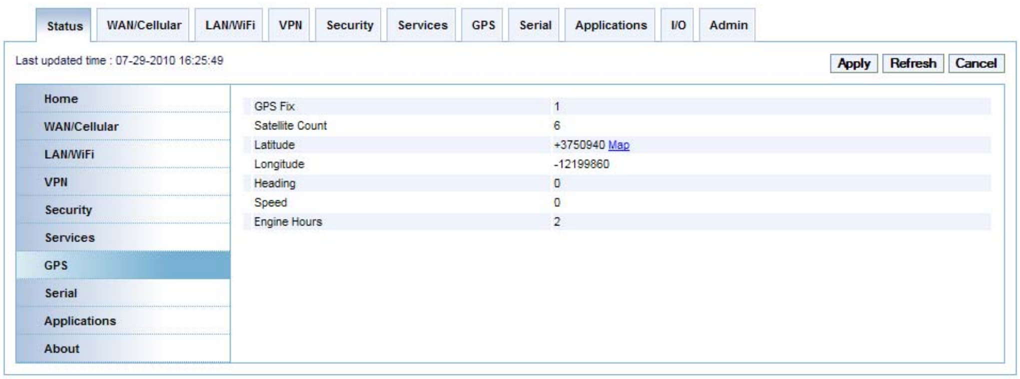
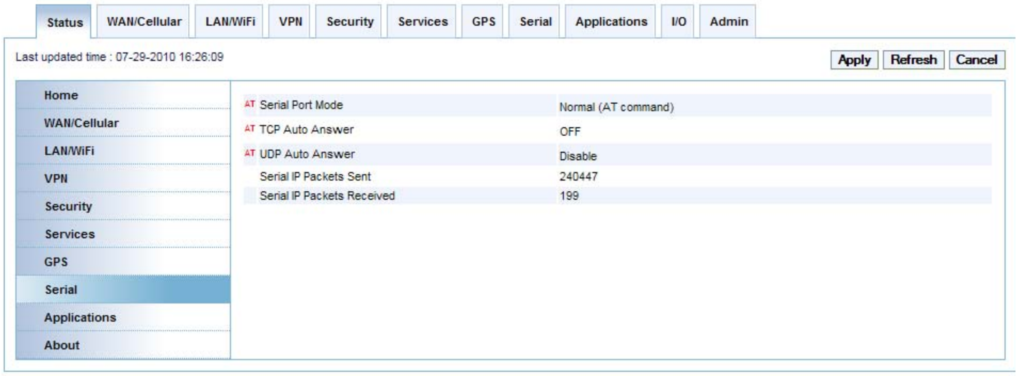


Figure 3-7: ACEmanager: Status - GPS

Command	Description
GPS Fix	0 = No Fix, 1 = GPS Fix, 2 = WAAS
Satellite Count	Shows how many satellites the GPS receiver can detect.
Latitude	Latitude of the GPS receiver.
Longitude	Longitude of the GPS receiver.
Heading	The direction in which the AirLink device is moving. No configuration is needed for Heading or Speed, they are calculated automatically.
Speed	TAIP data - Vertical Speed
Engine Hours	Measure of how many hours the engine is on.

Serial



Note: The Serial tab that displays in ACEmanager, is applicable to all Sierra Wireless AirLink devices except Raven XE.

Figure 3-8: ACEmanager: Status - Serial

Command	Description
Serial Port Mode	Default power-up mode for the serial port: When the AirLink device is power-cycled, the serial port enters the mode specified by this command after 5 seconds. On startup, typing ATMD0 within 5 seconds changes the mode to normal (AT command) mode.
TCP Auto Answer	This register determines how the AirLink device responds to an incoming TCP connection request. The AirLink device remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the device must be set for a successful TCP connection. The AirLink device will send a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgement of the connection request and the TCP session is established. • Off (Default) • On • Use Telnet server mode on TCP connections With a Telnet connection, overrides the client's default echo, allowing the server on the host port to perform the echo. CRLF sequences from the telnet client will also be edited to simply pass CRs to the server on the host port.
UDP Auto Answer	Enables UDP auto answer (half-open) mode. Normal mode Enable UDP auto answer mode.
Serial IP Packets Sent	Number of bytes sent over serial port to host.
Serial IP Packets Received	Number of bytes received over serial port from host.

Applications

The Application section of the Status group provides information on status of Garmin device.

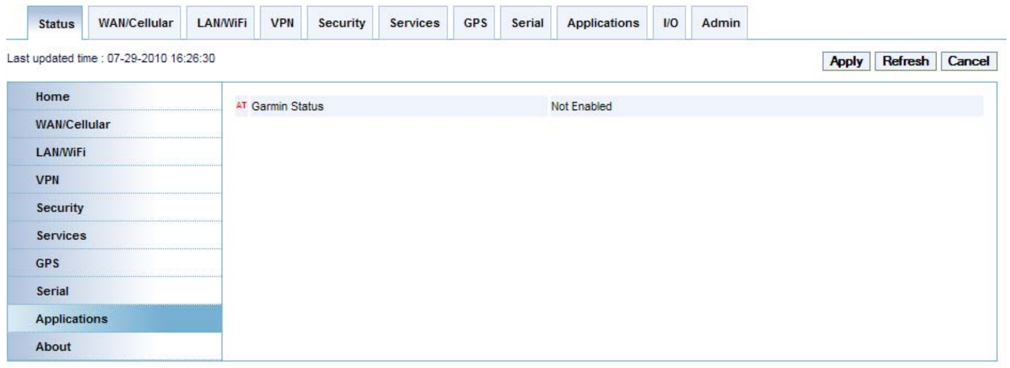


Figure 3-9: ACEmanager: Status- Applications

About

The About section of the Status group provides basic information about the cellular device.

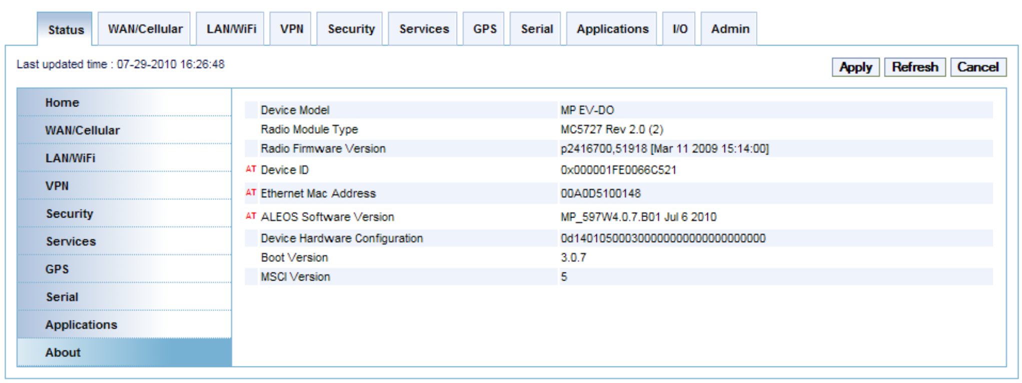


Figure 3-10: ACEmanager: Status - About

Command	Description
device name	Name of the AirLink device (up to 20 characters long) to use when performing IP address change notifications to IP Manager. On AirLink devices with WiFi, this is not the SSID.
Radio Module Type	MC 5727. The model number of the internal cellular radio module.
Radio Firmware Version	Firmware version in the radio module.
Device ID	The 64-bit device ID the device uses to identify itself to the cellular network.

Command	Description
Ethernet Mac Address	The MAC address of the Ethernet port.
ALEOS Software Version	Displays version of ALEOS software running on the AirLink Device.
device Hardware Configuration	Indication of the internally configured hardware.
Boot Version	The version of boot code installed in the device.
MSCI Version	Version of MSCI

4: WAN/Cellular Configuration

The WAN/Cellular tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

The WAN/Cellular section allows changes to the cellular connection and main operating mode of the AirLink Device.

Note: The Network Credential and Advanced settings will appear differently and is dependent on cellular carrier settings.

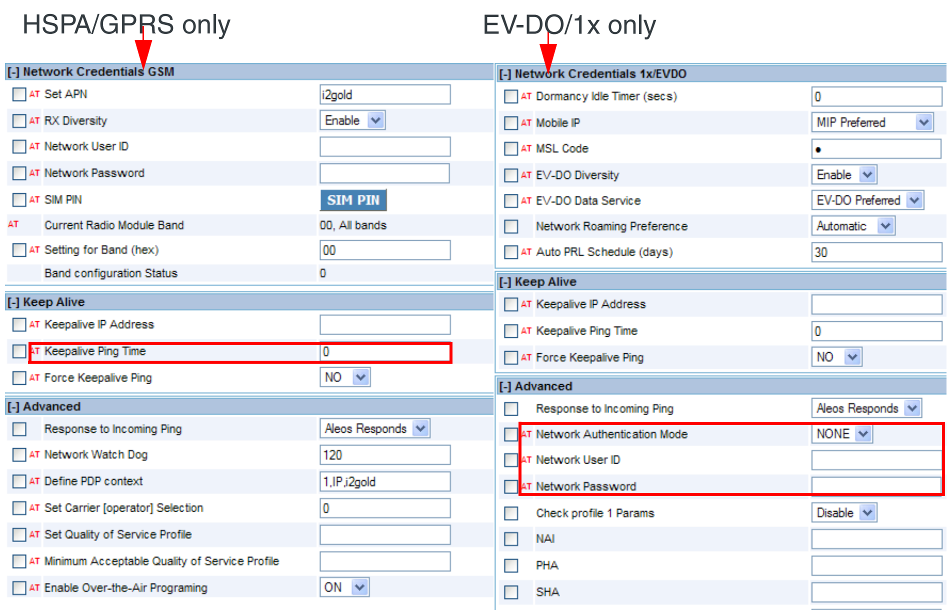


Figure 4-1: ACEmanager: WAN/Cellular - EV-DO /1X

<table>
<tr><th>Carrier type</th><th>Command</th><th>Description</th></tr>
<tr><td>EV-DO/1X</td><td>Dormancy Idle Timer (secs)</td><td>Inactivity timer, in seconds. Typical network settings cause a link to go dormant after 10 to 20 seconds of inactivity, no packets transmitted or received. This time can be shortened to release the physical RF link sooner when the application only transmits short bursts.
• n=0 : Allows the cellular network to determine the inactivity timer.
• n= seconds (maximum 20 seconds)</td></tr>
<tr><td>EV-DO/1X</td><td>Mobile IP</td><td>Mobile IP (MIP) Preferences. On a Mobile IP network, a device connects to the network using PPP. During the negotiation process the AirLink device is NOT required to present a username and password to authenticate because the authentication parameters are stored in the device itself.
• n=0 : Disabled, SIP only
• n=1 : MIP preferred
• n=2 : MIP only
Note: Your account with your cellular carrier may not support Mobile IP.</td></tr>
<tr><td>EV-DO/1X</td><td>MSL Code</td><td>The NAMLCK is the device's 6-digit OTSL (One Time Subsidy Lock), MSL (Master Subsidy Lock), or SPC (Service Provisioning Code). Your cellular carrier will provide the unlock code.
• nnnnnn=6 digit unlock code
Note: If the number is accepted by the device, the OK result code is returned. If the number is rejected, the ERROR result is returned. If three successive Errors are returned, the device must be reset by Sierra Wireless AirLink Solutions to allow any further attempts. The device permits 99 failures of this command during its lifetime. After that, the device becomes permanently disabled.</td></tr>
<tr><td>EV-DO</td><td>EV-DO Diversity</td><td>EV-DO Diversity allows two antennas to provide more consistent connection.
• Disabled
• Allow
If you are not using a diversity antenna, *EVDODIVERSITY should be disabled.</td></tr>
<tr><td>EV-DO</td><td>EV-DO Data Service</td><td>Change the allowable Network type.
• EV-DO preferred but can “fall back” on CDMA/1x
• EV-DO only, fall back disabled
• CDMA/1x only, EV-DO disabled
*PROVISION=MSL,MDN/MIN[,SID][,NID]
It is recommended to use the Setup Wizard for your carrier to provision the device. Provision the device with the lock code and phone number. Cannot be configured in ACEmanager.
• MSL=master lockcode
• MDN/MIN=phone number
• SID=system ID
• NID=network ID</td></tr>
</table>

Carrier type	Command	Description
EV-DO/1X	**Network Roaming Preference**	Automatially allows home and roaming network preference.
EV-DO/1X	**Auto PRL Schedule (days)**	Indicates PRL update schedule. 0 = Disable. *Not all carriers support this feature.*
EV-DO/1X	**Check profile 1 Params**	Enables checking and updating the Profile 1 Parameters. *Not all carriers support this feature.*
EV-DO/1X	**NAI**	Sets the Network Access ID. *Not all carriers support this feature.*
EV-DO/1X	**PHA**	Sets the IP address of the primary home agent. *Not all carriers support this feature.*
EV-DO/1X	**SHA**	Sets the IP address of the secondary home agent. *Not all carriers support this feature.*
EV-DO/1X	**MHSS**	Sets the home agent shared secret key. *Not all carriers support this feature.*
EV-DO/1X	**MASS**	Sets the AAA shared secret key. *Not all carriers support this feature.*
HSPA/ GPRS	**Set APN**	Easy entry of the APN. If left blank, the device will attempt to use the default subscriber value as defined by the account. • apn=access point name
HSPA/ GPRS	**Rx Diversity**	This is the diversity setting, It is Disabled by default.
HSPA/ GPRS	**Network User ID**	Network User ID The login that is used to login to the cellular network, when required. • uid=user id (up to 64 bytes)
HSPA/ GPRS	**Network Password**	Network Password. The password that is used to login to the cellular network, when required. pw=password (30 characters maximum).
HSPA/ GPRS	**SIM PIN**	Enter the SIM PIN.
HSPA/ GPRS	**Current radio module band**	Band reported by the radio module.
HSPA/ GPRS	**Setting for Band**	Desired band to set by ALEOS in the radio module. To change the value, Apply the change and Refresh to see the status of the configuration below. Allows you to select GSM bands - All, 3G only, 2 G only, 3G all and 2G all.
HSPA/ GPRS	**Band Configuration Status**	Indicator of a pending change for the Setting for Band. 0 = never set, 1= will be set on reboot, 2= set in radio module, 3= This value created an error response.
		Keep Alive

Carrier type	Command	Description
All	Keepalive IP Address	The IP address that the AirLink Device will ping to determine if there is internet connectivity and make sure this IP address is accessible. Set the IP address or valid internet domain name for the AirLink device to ping to keep itself alive (online). *IPPING must to be set to a value other than 0 to enable pinging. • d.d.d.d=IP address • name=domain name *IPPINGADDR sets the IP address you want to use for the connection test. If *IPPINGADDR is left blank or is set to an invalid IP address (example, an IP which is unreachable or one which is not a valid IP address), device performance will be adversely affected.
	Keepalive Ping Time	The amount of time between pings when the device is idle. Set the period to ping (if no valid packets have been received) a specified address (*IPPINGADDR) to keep the device alive (online). • Disable pinging (default) • 5-255 minutes 15 minutes is the minimum interval which can be set for Keepalive. If you set *IPPING for a value between 0 and 15, the minimum value of 15 will be set. *IPPING sets the interval, in minutes, you want Keepalive to test the network connection. To disable Keepalive, set *IPPING to 0 (default setting). 15 to 60 minutes is the minimum time which can be set for Keepalive. If you set *IPPING for a value less than the minimum, the minimum value will be set.
	Force Keepalive ping	If the ping should occur even if the device is not idle.
		Advanced
All	Network Watch Dog	Network connection watchdog: The number of minutes to wait for a network connection. If no connection is established within the set number of minutes, the device resets. • n=0 : Disabled. • n=minutes : Default = 120 min.
EV-DO/1X	Network Authentica-tion Mode	Specifies the authentication method to be used in the network PPP session. • PAP and CHAP are two options.
EV-DO/1x	Network User ID	Network User ID The login that is used to login to the cellular network, when required. • uid=user id (up to 64 bytes)
EV-DO/1x	Network Password	Network Password. The password that is used to login to the cellular network, when required. pw=password (30 characters maximum).
HSPA/ GPRS	Define PDP context	Easy entry of the APN. If left blank, the device will attempt to use the default subscriber value as defined by the account. • apn=access point name 1 and “IP”, are required and not variable. Quotes need to be placed around the APN. **Tip:** *When *NETAPN has been configured, +CGDONT will be pre-populated in ACEmanager .*

Carrier type	Command	Description
HSPA/ GPRS	Set carrier Operator selection	Manually specify an operator. Refer also to *NETOP. • mode=0 : Automatic - any affiliated carrier [default]. • mode=1 : Manual - use only the operator <oper> specified. • mode=4 : Manual/Automatic - if manual selection fails, goes to automatic mode. • format=0 : Alphanumeric ("name") (G3x10 must use this format). • format=2 : Numeric oper=”name”
HSPA/ GPRS	Set Quality of service profile	Set Quality of Service Profile. Change should be at carrier's request. Normally not required to be changed.
HSPA/ GPRS	Minimum Acceptable Quality of Service Profile	Minimum Acceptable Quality of Service Profile. Change should be at carrier's request. Normally not required to be changed.
All	Enable Over-the-Air Programming	Enables/disables over-the-air firmware upgrading of the AirLink device. When Sierra Wireless releases a new version of ALEOS, you can upgrade your remote devices with Over-the-Air Programming (OPRG) enabled. • Disables • Enables

SIM PIN

The SIM PIN feature in ACEmanager allows users to change the SIMP Pin number as per their requriements or keep it the same. The three options offered in the pop up box once you click on SIM PIN are:

- Don’t change - This is selected by default and implies that you do not want to change the SIM Pin number.
- Enable - Choose this option of you want to enable the SIM Pin (change) feature.
- Disable - Choose this option if you want to disable the SIM Pin feature.

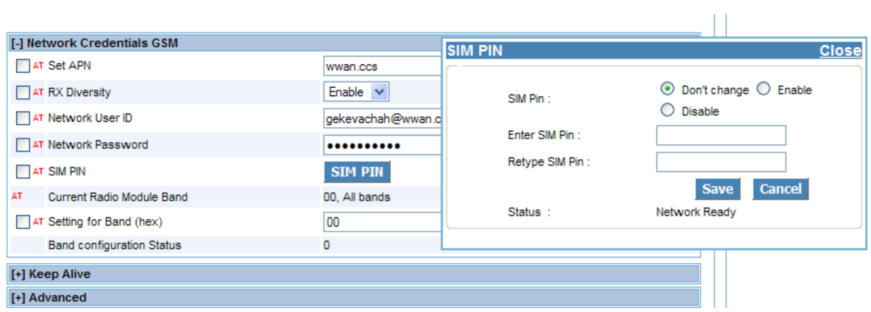


Figure 4-2: ACEmanager: WAN/Cellular - SIM PIN

To change the SIM PIN number,

1. Enter the SIM Pin number and retype it.

2. Click on Save.

Keepalive

Keepalive is used to test the connection to the cellular network by pinging an IP address after a specified period of inactivity. Keepalive is only recommended for users who have a remote terminated device that infrequently communicates to the network or if you have experienced issues over time where the device can no longer be reached remotely.

When Keepalive pings the IP address, an acknowledgement indicates there is an active connection to the network. If the AirLink device does not receive a response from the IP address, it will make additional attempts according to a backoff algorithm before determining the Internet connection is not functioning properly. If it determines the connection is not functioning, the device will then attempt to reconnect to the carrier to reestablish IP connectivity.

Data usage using Keepalive

Keepalive is an optional feature. If you frequently pass data with your device, you most likely do not need to have Keepalive enabled. When using Keepalive, be aware that a ping moves approximately 66 bytes of data over the network and is billable by the carrier. The following *IPPING settings will incur approximate monthly data usage in addition to any other data usage:

*IPPING	Estimated Usage
15 minutes	400k / month
30 minutes	200k / month
60 minutes	100k / month
120 minutes	50k / month

5: LAN/WiFi Configuration

5

The LAN tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

The primary purpose of the AirLink device is to route data from one or more devices connected to one or more of the ports to the cellular network and, ultimately, under most circumstances, to the Internet.

Public and Private Mode

To support some legacy installations, the AirLink device has the ability to act as a one-to-one gateway giving the cellular network granted IP address directly, to a connected device. This is Public mode.

Since the one-to-one gateway configuration will not allow the flexibility of a LAN environment where several devices can connect to the AirLink device, Private Mode provides a NAT environment with an optional DHCP server.

Tip: *When using Public mode, Sierra Wireless recommends connecting the device directly to the computer or other end device. Using a hub or switch may prevent the AirLink device from updating the IP address of the end device when an IP address is received from the cellular network.*

In ACEmanager, the Host Public mode and DHCP settings are part of the **LAN tab.** The DHCP addresses for USB/net are on LAN > USB page, the DHCP addresses for the serial PPP are on the PPPoE page, and the DHCP addresses for the WiFi, as applicable, are on the WiFi page.

Addressing

This section governs Ethernet port connections and the Public/Private mode of all ports. Changing settings in this area requires a reboot of the AirLink device after applying any changes.

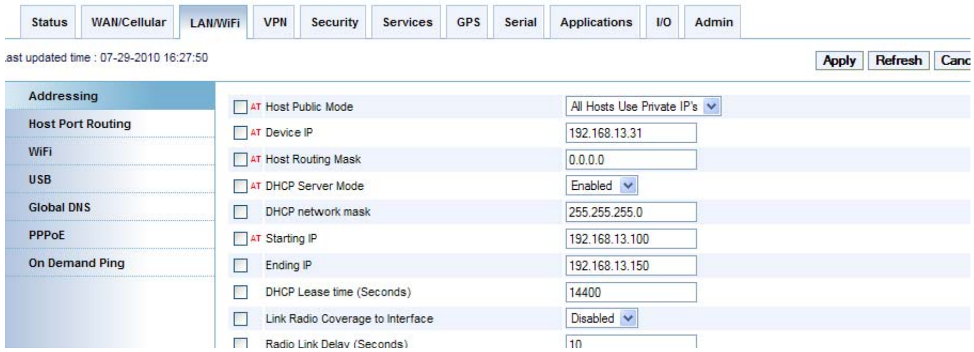


Figure 5-1: ACEmanager: LAN/WiFi - Addressing

Command	Description
Host Public Mode	Sets the Host Interface that uses the Public IP address grated by the cellular network or if all should use private IP addresses. All host interfaces which are not using the public IP address will use private IP addresses. 0 = Ethernet Uses Public IP ; 1 = All Hosts Use Private IP's - This is the default. 2 = USB Uses Public IP 3 = RS232 Uses Public IP *Note: The connected computer receives DHCP address from ALEOS and it also has default router set up to device IP.*
Device IP	The Ethernet IP address of the AirLink Device. By default this is set to 192.168.13.31.
Subnet mask	The subnet mask indicates the range of host IP addresses which can be reached directly. Changing this will limit or expand the number of clients that can connect to the AirLink Device. The default is 255.255.255.0 and means that 254 clients can connect to the AirLink Device. Using 192.168.13. as the first three octets of their IP address if the device IP is 192.168.13.31.
Server Mode	Enabled or Disabled. By default, the Ethernet DHCP server is enabled. Disabling the DHCP server will require all connected clients to have static IP addressing.
DHCP Network Mask	The Netmask given to any Ethernet DHCP client.
Starting IP	Ethernet DHCP pool starting IP address. *Note: If you have only one computer or device connected directly to the Ethernet port, this is the IP address it will be assigned.*
Ending IP	The ending IP for the Ethernet Interface.
DHCP Lease time (seconds)	Configurable DHCP lease time.
Link Radio Coverage to Interface	This will disable the specified port when there is no cellular coverage. 1 = Ethernet; 2 = USB
Radio Link Delay (Seconds)	The delay in seconds before the radio link goes down.

Tip: *If you are using Private Mode for all hosts (*HOSTPRIVMODE=1), you will need to make sure that device IP, Starting IP and Ending IP are on the same subnet defined by the DHCP network mask. If the subnet mask is 255.255.255.0, it is safe to use 192.168.x.y for each as long as the x is the same number (0 in the example screen shot above) and the y is different (1 and 2 in the example) and between 0 and 254.*

Internal DHCP Server

DHCP (Dynamic Host Configuration Protocol) has become a primary component of today's network environments. DHCP allows one server to automatically and dynamically allocate network IP addresses and other network related settings (such as subnet masks, routers, etc.) to each computer or device without the need to set up each specifically or keep track of what addresses have already been used.

In a default configuration, the AirLink device acts as a DHCP host to any device connected to its ports, providing that device with an IP address which can be used to communicate on the Internet. In Public Mode, that will be the IP address assigned by the cellular network. In Private Mode, that will be the IP addresses defined in the LAN pages.

Address assignment in Public mode

1. When the AirLink device registers on the cellular network, it is assigned an IP address from the carrier, let's say 10.1.2.0.
2. Acting as a DHCP server,with Ethernet uses Public IP, when the AirLink device receives a DHCP request from an Ethernet device connected to its ports, it hands off the assigned address to the device and sets up the default gateway address as 10.1.2.1. If the fourth octet is already a 1, it assigns 10.1.2.2 as the router address.

Note: The primary gateway, to the cellular network for any connected device, is enabled by default

3. The AirLink device also sends a /24 netmask (255.255.255.0 by default) and sets up a static route which maps 192.168.13.31 (or the address configured with *HOSTPEERIP if it is changed) to 10.1.2.1 (or 10.1.2.2 if that was what the gateway address was given as).

Tip: *When PPPoE is used with the AirLink device, DHCP is not needed. A tunnel is set up connecting a device (such as your computer or a router) with the device. The device will then simply use the MAC address of the AirLink device to send all outgoing packets.*

Host Port Routing

The "Host Network" is the equivalent of the IP route command.

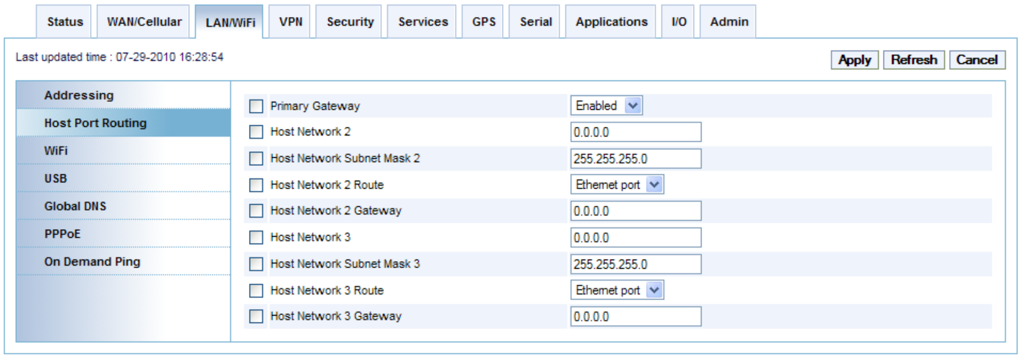


Figure 5-2: ACEmanager: LAN/WiFi - Host Port Routing

Command	Description
Primary Gateway	Your device is the Primary Gateway for the network behind a router connected to it and ALEOS responds to ARPs for all non-host ethernet subnets.
Host Network 2 and Host Network 3	Network to route to host IF. Host Network 2 and 3 are secondary networks connected to the AirLink device. For example, 192.168.10.0.
Host Network Subnet Mask 2 and Host Network Subnet Mask 3	This is the subnet for the applicable network. For example, 255.255.255.0, which would with the setting above define a secondary network of 192.168.10.0/24.
Host Network 2 Route and Host Network 3 Route	This indicates what type of router is being used for the host network. If it is a traditional router which handles ARP for addresses on it's subnet, select Ethernet. If it is a "dumb" gateway which is a conduit to a subnet but doesn't handle any ARP, select Gateway. When Gateway is selected, ALEOS will ARP for the destination address and send it to the defined Host Network Gateway address.
Host Network 2 Gateway and Host Network 3 Gateway	This is the IP address of the 'dumb' Gateway. This should be left as 0.0.0.0 if the Host Network Route is Ethernet. Many routers will respond to ARP requests for subnets behind the router. The default is Ethernet, which means the user does not have to configure the gateway IP. However some routers don't respond to ARP requests for subnets. Hence, users need to enter the gateway address.

Wi-Fi devices

On supported models, the MP has a Wi-Fi radio for wireless LAN connections.

Note: WiFi is only avaialble on MP models with W. For example, MP 890W or MP 597W.

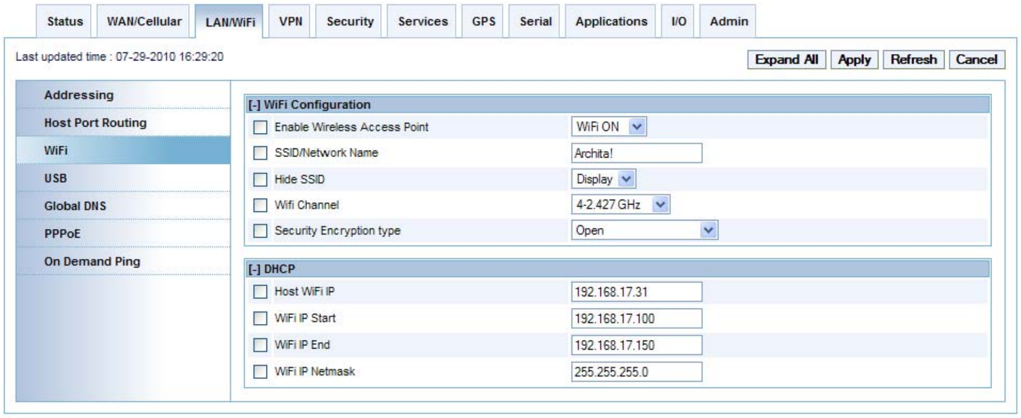


Figure 5-3: ACEmanager: LAN/WIFI

Command	Description
Enable Wireless Access Point	WI-Fi on or Wi-fi off. Allows you to disable or enable the Wi-Fi access point. If you are using the MP in an environment wheres security or safety require that you disable Wi-Fi, you can turn Wi-Fi off here. The WAN and Ethernet LAN connections will remain active.
SSID/Network Name	The default network name is 'MP'.
Hide SSID	Hide or Show. This determines whether the SSID will be broadcasted by the MP. Hiding the SSID will not prevent people from connecting to the box if the signal is open.
Wi-Fi Channel	1-11. The Wi-Fi access point on the MP can use any of 11 channels. If other Wi-Fi networks are in range and operating on nearby channels, you may be able to avoid interference by changing to a different Wi-Fi channel.
Security Encryption type	Open, WEP, WPA. The MP box supports Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access/802.11i (WPA and WPA2 Personal and Enterprise). Both protocols will restrict access to the MP box and protect data transmitted between the clients and the device. WPA provides the highest level of security if all of the LAN devices on your network support this protocol. WPA Enterprise is the follow on wireless security method to WPA that provides stronger data protection for multiple users and large managed networks. It prevents unauthorized network access by verifying network users through an authentication server.
Host WiFi IP	The WiFi IP address of the AirLink Device. By default this is set to 192.168.17.31.
WiFi IP Start	Start WiFi IP
WiFi IP End	End WiFi IP
WiFi IP Netmask	Mask for WiFi subnet

Note: The DHCP Server for Wi-Fi is seperate from the Ethernet DHCP Server. If you disable DHCP Server on LAN - Addressing, the Wi-Fi DHCP should be unaffected.

Open

Open Wi-Fi protocol is not password protected and has no additional conifguration requirements in ACEmanager.

Note: Selecting the encryption type will enable additional configuration option

Shared WEP

WEP or Wireless Encryption Protocol is the least secure, but most supported encryption method.

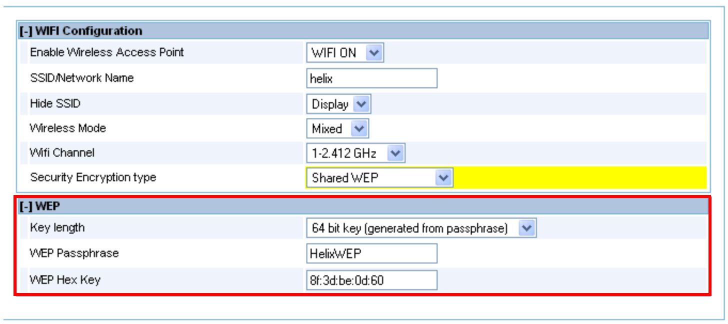


Figure 5-4: ACEmanager: WIFI - Shared WEP

Command	Description
Key Length	64 bit, 128 bit, Custom. WEP is available with shorter 64 bit keys or longer 128 bit keys. While 128 bit encryption provides a higher level of security, some computers and Wi-Fi clients only support 64 bit encryption. Use a key length that is compatible with all of the wireless clients on your network.
WEP Passphrase	The default passphrase is 'MPWEP'. You can enter your own private WEP passphrase to generate a hex (hexadecimal) key. Treat the passphrase like a password and select one that is difficult for others to guess. After you enter a new passphrase, click the Apply button to make the change effective. When logging into Wi-Fi from your computer, enter the hex key, not the passphrase. Most WEP connections only use the hexadecimal format. The passphrase is simply used as an easy way for you to create a hex key. You can configure your own hex key rather than generating one with a passphrase by selecting the 'Custom Key' option from the drop-down menu. Make sure your hex key only includes 10 or 26 valid hex digits, created through pairs of characters of 0-9 and/or a-f, with each pair separated by a colon. For example, 80:3a:c9:95:b8.

WPA/WPA2 Personal

WiFi Protected Access (WPA and WPA2), requiring a pre shared passphrase be known before being able to connect to a network. WPA/WPA2 Personal authenticates the passphrase directly in the device.

Note: WPA or WPA2 is determined by the encryption scheme selected. TKIP is WPA. AES is WPA2.

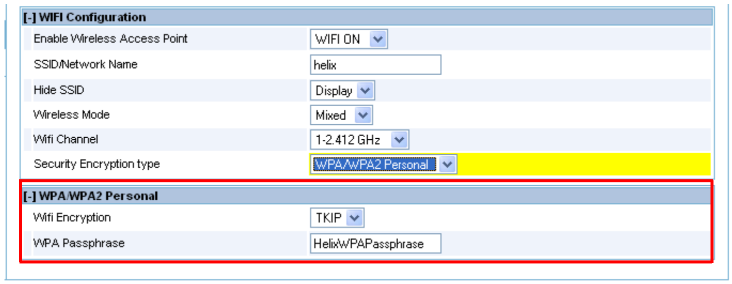


Figure 5-5: ACEmanager: WiFi - WPA/WPA2 Personal

Command	Description
WiFi Encryption	TKIP or AES. Defines what encryption scheme to use under WPA. Options are Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).
WPA Passphrase	By default this is 'DeviceWPAPassphrase'. You can change this to another phrase with alphanumeric characters and symbols when creating a passphrase.

WPA Enterprise

WPA Enterprise adds another layer of security to WPA by requiring clients authenticate with a server before being able to access the network. Clients connecting to the MP when WPA Enterprise is enabled will need to have certificates installed from the RADIUS server, allowing them access to the network before being allowed to connect.

Note: As with WPA/WPA2 Personal, WPA or WPA2 is determined by the encryption scheme selected. TKIP is WPA. AES is WPA2.

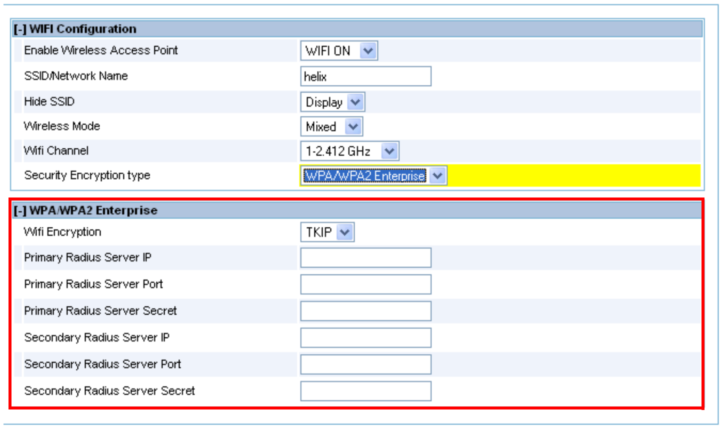


Figure 5-6: ACEmanager: WiFi - WPA/WPA 2 Enterprise

Command	Description
WiFi Encryption	TKIP or AES. Defines what encryption scheme to use under WPA. Options are Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).
Primary or Secondary Radius Server IP	This is the IP address of your enterprise RADIUS server. These servers must be accessible ALL the time or clients will not be able to connect via Wi-Fi. The secondary server is optional and used when the primary server is not available.
Secondary Radius Server Port	This is the port number of your enterprise RADIUS server. The secondary port is used when the primary is unavailable. Only used when a Secondary Radius Server is specified.
Primary or Secondary Radius Server Secret	This is the shared secret key used to secure communications with the RADIUS server. Only used when a Secondary Radius Server is specified.

USB

The AirLink device is equipped with a USB port which increases the methods by which you can send and receive data from a connected computer. The USB port can be set to work as either a virtual Ethernet port or a virtual serial port. A driver installation is required to use the USB port in either mode.

By default, the port is set to work as a virtual Ethernet port.

Note: It is recommended that you use a USB 2.0 cable with your AirLink device and connect directly to your computer for best throughput.

To change the USB port to allow virtual serial port communication in ACEmanager in the LAN > USB group, choose USB Serial as the USB Device Mode. To disable the USB port, select Disabled from the same menu.

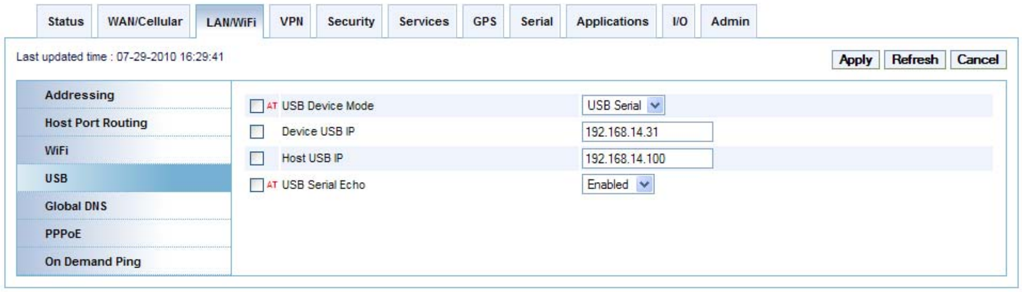


Figure 5-7: ACEmanager : LAN/WiFi - USB

Note: There is a USBnet/ USBserial driver for the Win7 64 bit USB.

Note: The change to the USB mode is immediate and generally does not require a reboot..

Command	Description
USB Device Mode	*USBDEVICE=n This parameter alters the default startup data mode for the USB port.
Device USB IP	The USB/net IP address of the AirLink Device. By default this is set to 192.168.14.31. 1 - USBNET 0 - USB Serial 2 - Disabled
Host USB IP	The IP for the computer or device connect to the USB port.
USB Serial Echo	Toggle AT command echo mode when the USB is configured for virtual serial. 0 = OFF; 1 = ON

Note: USB Serial works with Linx CDC-ACM driver.

Installing the USB drivers

Virtual Ethernet is the default setting for the USB port. If you want to install the virtual serial port, change the Device Mode to USB Serial

When you connect the AirLink device for the first time to a USB port on your computer, Windows should detect a new device and prompt you to install the driver.

Note: Windows will see each port type as a different USB device and will see every port on your computer separately. If you change the port type on the AirLink device or connect to a different USB port on your computer or hub, Windows will see it as a new device.

Figure 5-8: Found New Hardware Wizard

a. To start the install of the USB virtual Ethernet driver, select No, not this time and click Next.

b. Select Install from a list of specific location and click Next.

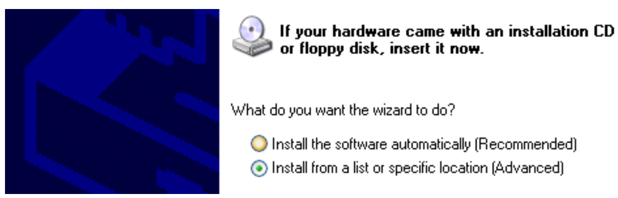


Figure 5-9: Hardware Wizard : Location options

a. Select and/or enter the location of the driver.

- If the driver is on the CD and the CD is in your drive, you can just select Search removable media.
- If you have installed ACEmanager or the Setup Wizard, the drivers have been conveniently copied to your hard drive. Enter C:\Program Files\Common Files\AirLink as the location to search.
- If you will be installing the driver from a file downloaded from the Sierra Wireless website, select Include this location in the search and type in the location where you downloaded the file.

b. Click Next.

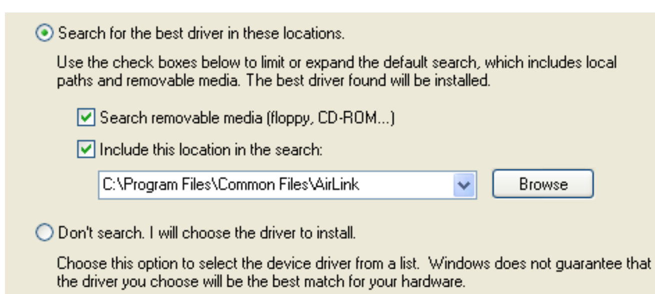


Figure 5-10: Hardware Wizard : Install location

After you select the location, the installation should begin. If you get a message asking if you want to continue the installation, click Continue Anyway.

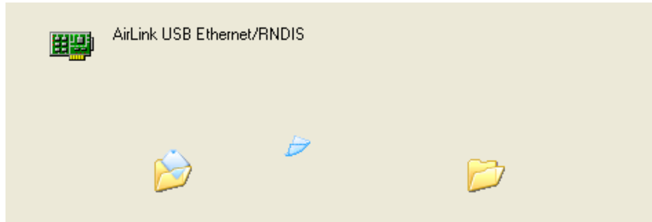


Figure 5-11: Hardware Wizard : Installing

c. Click Finish to complete the installation. The driver should be enabled without any need to reboot your computer.

Figure 5-12: Hardware Wizard : Finish

Virtual Ethernet

The USB Ethernet connection will show up in your Network Connections as a Local Area Connection.

Tip: *If you also have an Ethernet card on the computer or have installed the USB Ethernet to more than one USB port on your computer, the USB Ethernet may show up with a number.*

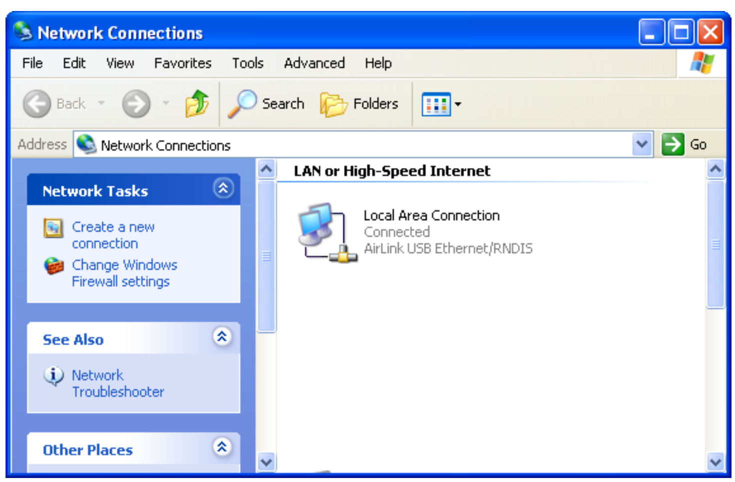


Figure 5-13: Network Connections

Note: By default, your Host IP for USB/net is 192.168.14.100.

You can also verify the installation by looking in the Device Manager.

a. Click on Start > Control Panel.

b. Double-click on the System icon.

c. Select the Hardware tab and click the Device Manager button.

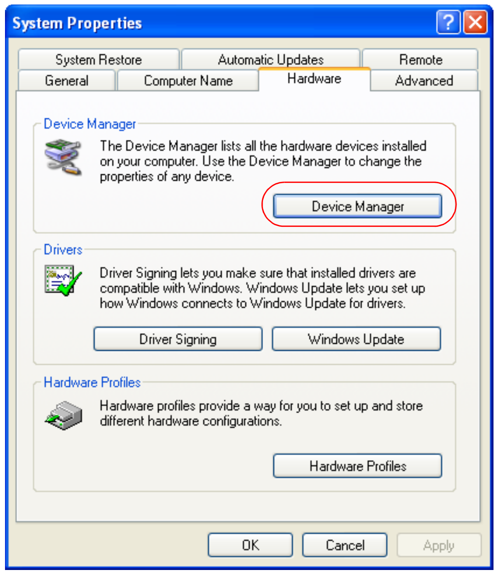


Figure 5-14: System Properties

d. Click on the + in front of *Network Adapters*.

The newly installed driver, AirLink USB Ethernet/RNDIS, should be displayed. If the driver is displayed with a # and number behind the driver name (such as, AirLink USB Ethernet/RNDIS #2), it means more than one is installed on your computer, most likely for different USB port. More than one copy of the driver should not cause any problems since only the connected port and its driver would be active.

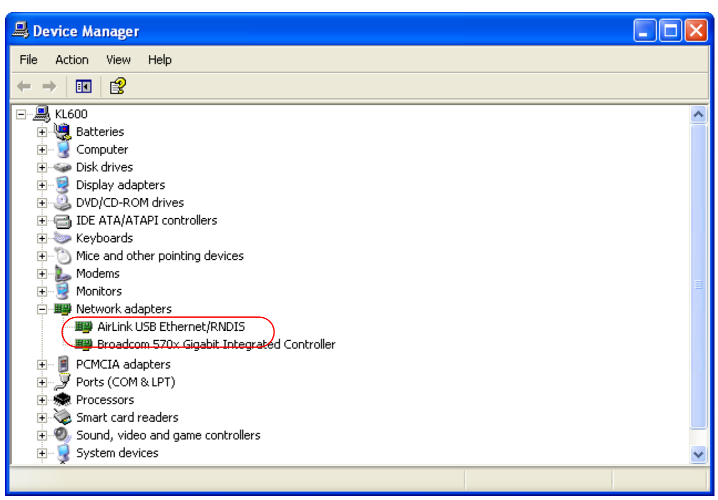


Figure 5-15: Device Manager - Ethernet

Once the driver is installed, you can use the USB port just like a standard Ethernet port.

Virtual Serial

You can verify the installation by looking in the Device Manager.

a. Click on Start > Control Panel.

b. Double-click on the System icon.

c. Select the Hardware tab and click the Device Manager button.

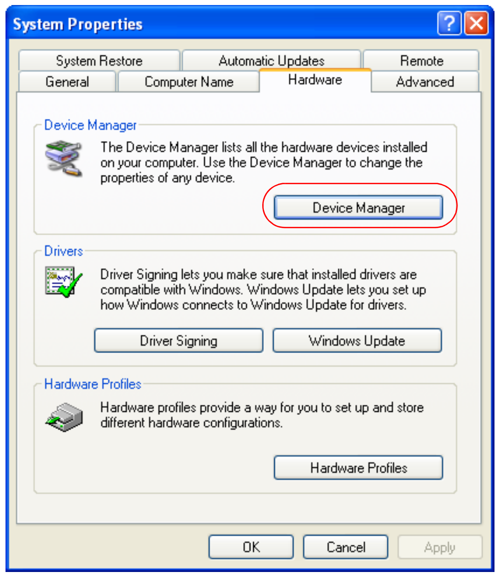


Figure 5-16: System Properties

d. Click on the + in front of *devices*.

The newly installed driver, AirLink USB Serial Port, should be displayed.

Tip: *If the driver is displayed with a # and number behind the driver name (such as, AirLink USB Serial Port #2), it means more than one is installed on your computer, most likely for different USB port. More than one copy of the driver should not cause any problems since only the connected port and its driver would be active.*

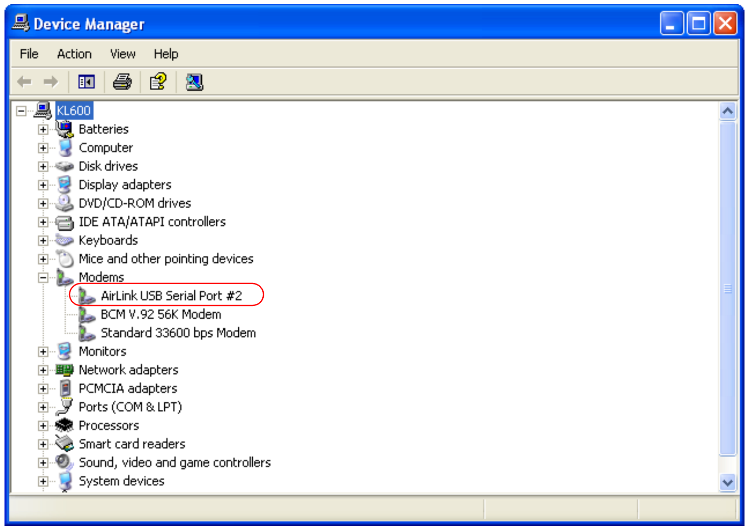


Figure 5-17: Device Manager - Serial

To connect to the device using the USB virtual serial, most applications or utilities will require you to select or enter the serial (COM) port number. The USB connection will appear as a standard serial port, so you will need to determine its number to connect to it. The driver installation will automatically assign a port or you can change it if you wish to another unused port.

a. From the Device Manager, right click on the driver name and select Properties.

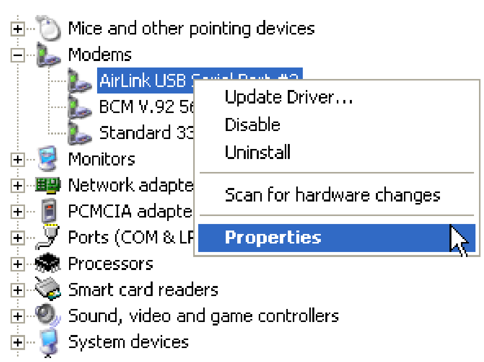


Figure 5-18: Device Manager : Driver menu

b. Select the Advanced tab and click the Advanced Port Settings button.

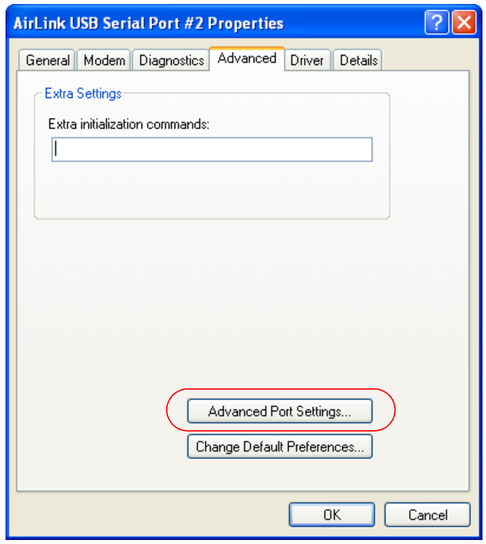


Figure 5-19: Driver Properties

c. At the bottom of the screen, the current port used will be listed. Use the drop down menu to select an available COM port number if you need to change it.

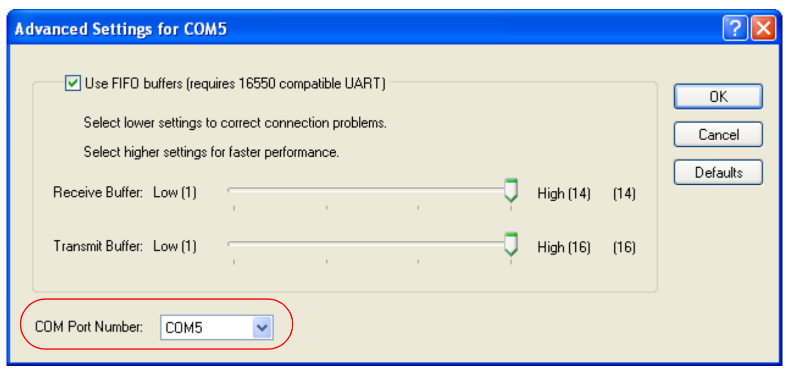


Figure 5-20: Advanced Settings

Note: The COM port number assigned by driver installation is the next port that is available. The port number might vary depending on the number of devices connected (using serial or virtual serial).

Once the driver is installed, you can use the USB port just like a standard serial port.

Global DNS

When the cellular network grants the IP address to the device, it includes the IP addresses to its DNS servers. Global DNS allows you to override the carrier's DNS settings for all connected devices. This is useful when the connected devices need to use a private network.

Note: If there are no alternate DNS defined, the default is the cellular network DNS sever.

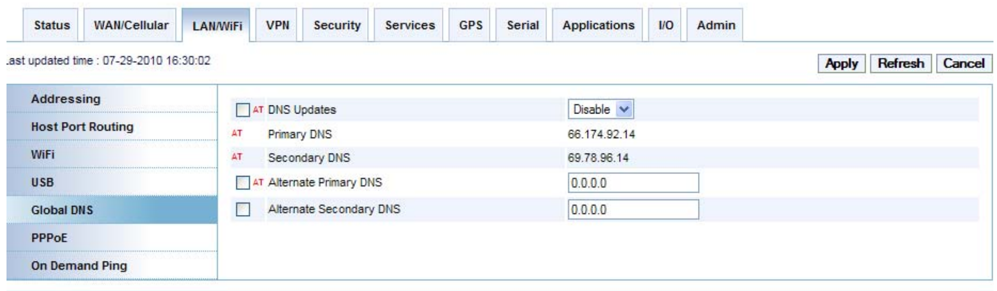


Figure 5-21: ACEmanager: LAN /WiFi- Global DNS

Command	Description
DNS Updates	Disabled or Enabled. By default this is set to Disabled.
Primary DNS	Primary carrier DNS IP Address.
Secondary DNS	Secondary carrier DNS IP Address.
Alternate Primary DNS	Alternate primary DNS address. This is optional. If the primary DNS is unavailable, this DNS address will be used.
Alternate Secondary DNS	Alternate secondary DNS address. This is optional. If the secondary DNS is unavailable, this DNS address will be used.

PPPOE

PPPoE (Point-to-Point Protocol over Ethernet) allows a point-to-point connection while using Ethernet. Just like the dial up protocol on which it is based, PPPoE uses traditional user name and password authentication to establish a direct connection between two Ethernet devices on a network (such as your AirLink device and your computer or router).

Application examples for PPPoE with your AirLink device:

- Backup connectivity solution for your network.
- Individualized Internet connection on a LAN.
- Password restricted Internet connection.

Only one computer, router, or other network device at a time can connect to the AirLink device using PPPoE.If you are using the AirLink device connected to a router as a back up Internet connection for your network, you should configure the router to use the PPPoE connection and not the individual computers.

Tip: *You may need to use Private Mode to configure the IP address of your AirLink device to be available on a LAN.*

Note: To configure a PPPoE connection on Microsoft Windows XP, 2000 or NT, you will need administrator privileges to the computer you are configuring or access granted by an administrator on the network to add/remove devices to your computer.

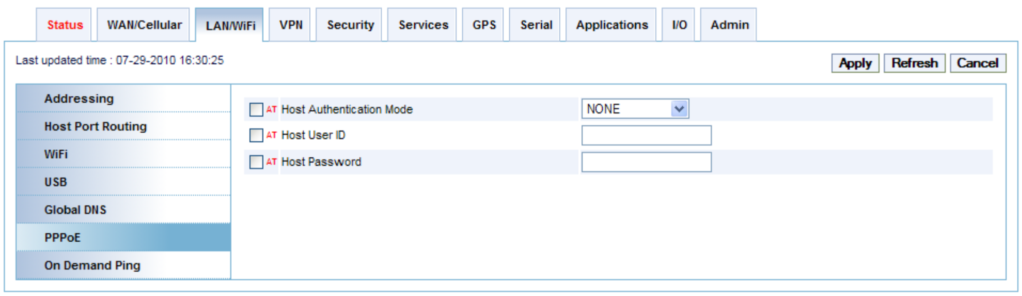


Figure 5-22: ACEmanager: LAN/WiFi- PPPoE

Command	Description
Host Authentication Mode	Host Authentication Mode: Use PAP or CHAP to request the user login and password during PPP or CHAP negotiation on the host connection. The username and password set in *HOSTUID and *HOSTPW will be used. • Disable PAP or CHAP request (Default) • PAP and CHAP • CHAP
PPP User ID	Host User ID for PAP or CHAP. • user id (up to 64 bytes)
PPP Password	Host Password for PAP or CHAP.

Configure your AirLink device to support PPPoE

- From the groups on the left, select *PPPoE* under LAN.
- Change Host Auntentication Mode to 2.
- Enter a user name for PPP User ID for the PPPoE connection.
- Enter a password (PPP password) for the PPPoE to connection.

Tip: *If you leave* PPP User ID *and* PPP password *blank, any computer or device can connect to the PinPoint device using PPPoE.*

Note: ACEmanager shows the existing values for PPP User ID *and* PPP password *encrypted and character padded.*

Optional: Configure *Device Name

a. In ACEmanager, select Dynamic DNS from the groups on the left, under Services.

b. Enter a name for device Name, such as AirLink device or the ESN.

The name you choose for device Name will not affect the connection but may need to be configured in PPPoE settings for the router, device or computer you will be connecting to your AirLink device.

6: VPN Configuration

6

The VPN tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

The AirLink Device can act as a Virtual Private Network (VPN) client, providing enterprise VPN access to any device connected to the AirLink Device even when a device has no VPN client capability on its own. The AirLink Device supports two tunneling protocols, IPsec and GRE. Both can be used at the same time.

IPSec

The IP protocol that drives the Internet is inherently insecure. Internet Protocol Security (IPSec), which is a standards-based protocol, secures communications of IP packets over public networks.

IPSec is a common network layer security control and is used to create a virtual private network (VPN).

The advantages of using IPSec or GRE feature includes:

- Data Protection: Data Content Confidentiality allows users to protect their data from any unauthorized view, because the data is encrypted (encryption algorithms are used).
- Access Control: Access Control implies a security service that prevents unauthorized use of a Security Gateway, a network behind a gateway or bandwidth on that network.
- Data Origin Authentication: Data Origin Authentication verifies the actual sender, thus eliminating the possibility of forging the actual sender's identification by a third-party.
- Data Integrity: Data Integrity Authentication allows both ends of the communication channel to confirm that the original data sent has been received as transmitted, without being tampered with in transit. This is achieved by using authentication algorithms and their outputs.

Global Settings

The AirLink Device supports Global settingss with one encrypted tunnel and one open tunnel. A sample server subnet for a Global settings would be 172.16.1.0/24. Global settings VPNs should be setup with care, as a Global settings configuration with both an enterprise VPN and access to the public Internet can inadvertently expose company resources.

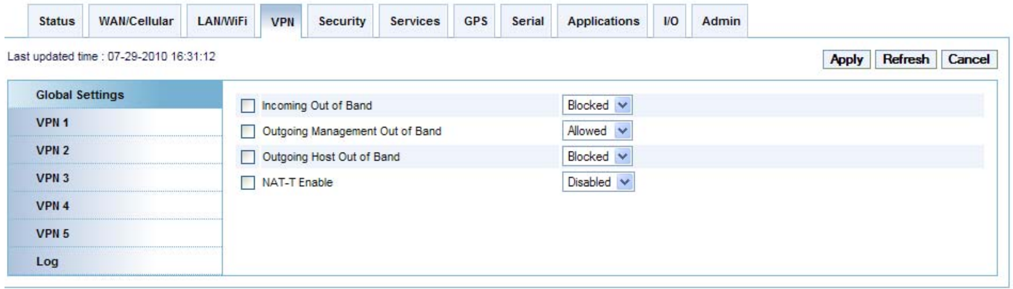


Figure 6-1: ACEmanager:VPN - Global settings

Command	Description
Incoming out of Band	Disabled or Enabled. Disables or Enables port forwarding rules.
Outgoing Management Out of Band	Outgoing ALEOS out of band can be blocked or allowed.
Outgoing Host Out of Band	Outgoing Host out of band can be blocked or allowed.
NAT-T	NAT-T Enable is disabled by default.

VPN 1 to 5

Each of the VPN tunnels 1 to 5, can be configured as IPSec, GRE or IPSec and GRE. When you select the VPN type for a tunnel, the configuration settings specific to the VPN type will become available.

The IPSec architecture model includes the Sierra Wireless AirLink gateway as a remote gateway at one end communicating, through a VPN tunnel, with a VPN gateway at the other end. The remote gateway is connected to a Remote network and the VPN is connected to the Local network. The communication of data is secure through the IPSec protocols.

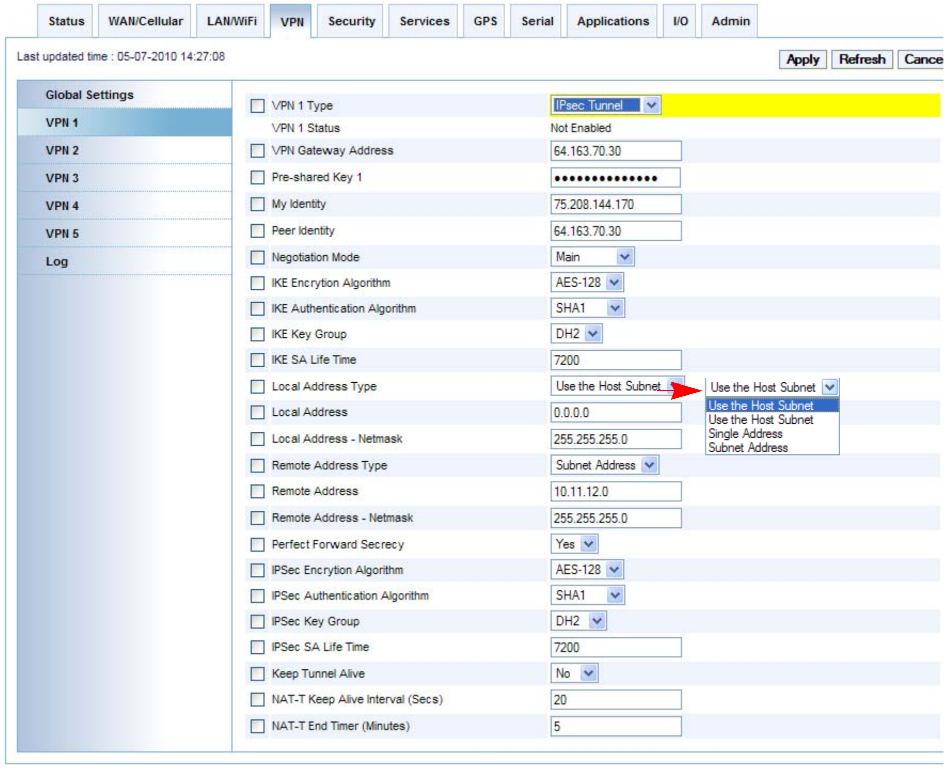


Figure 6-2: ACEmanager: VPN 1 - VPN

Command	Description
VPN # Type	Tunnel Disabled or IPsec tunnel. Use this option to enable or disable the VPN tunnel. If custom settings are used, they will be saved and the tunnel can be disabled and reenabled without needing to reenter any of the settings. The IPsec VPN employs the IKE (Internet Key Exchange) protocol to set up a Security Association (SA) between the AirLink Device and a Cisco (or Cisco compatible) enterprise VPN server. IPSec consists of two phases to setup an SA between peer VPNs. Phase 1 creates a secure channel between the AirLink Device VPN and the enterprise VPN, thereby enabling IKE exchanges. Phase 2 sets up the IPSec SA that is used to securely transmit enterprise data. For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink Device VPN and the enterprise VPN server.
VPN1 Status	Disabled, Not Connected, or Connected. This indicates the current status of the VPN connection. Use this as part of troubleshooting a VPN connection.
SNTP Server Address	The Simple Network Time Protocol Server (SNTP) ensures the clock on the AirLink Device VPN is synched to standard time. The default NTP server is pool.ntp.org. You can specify any preferred NTP server. Both the VPN server and client must use the same SNTP address.
VPN Gateway Address	The IP address of the server that this client connects to. This IP address must be open to connections from the AirLink Device Box.
Remote Subnet (IP Addr Mask)	The default configuration is 0.0.0.0/0 which will direct all traffic over the GRE tunnel.
Pre-shared Key 1	Pre-shared Key (PSK) used to initiate the VPN tunnel.

Command	Description
My Identity	If these fields are left blank, My Identity will default to the WAN IP address assigned by the carrier and Peer Identity will default to the VPN Server IP. For a fully qualified domain name (FQDN), these values should be preceded by an ‘@’character (@www.domain.com). For user-FQDN, these values should include a username (user@domain.com)
Peer Identity	Required in some configurations to identify the client or peer side of a VPN connection. This defaults to the VPN server IP address.
Negotiation Mode	Main Mode or Aggressive. To operate the onboard VPN under Aggressive mode, enable this configuration. By default the AirLink Device operates under Main Mode. Aggressive mode offers increased performance at the expense of security.
IKE Encryption Algorithm	DES, 3DES, or AES. Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) is supports 128 bit encryption.
IKE Authentication Algorithm	SHA1 or MD5. Can be configured with MD5 or SHA1. MD5 is an algorithm that produces a 128-bit digest for authentication. SHA1 is a more secure algorithm that produces a 160-bit digest.
IPSec Encryption Algorithm	DES, 3DES, or AES. Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports 128 bit encryption.
IPSec Authentication Algorithm	SHA1 or MD5. Can be configured with MD5 or SHA1. MD5 is an algorithm that produces a 128-bit digest for authentication. SHA1 is a more secure algorithm that produces a 160-bit digest.
IKE SA Life Time	180 to 86400. Determines how long the VPN tunnel is active in seconds. The default value is 28,800 seconds, or 8 hours.
Local Address Type	The network information of the device.
Local Address	Device’s subnet address.
Local Address - Netmask	24 bits netmask.
Remote Address Type	The network information of the IPSec server behind the IPSec gateway.
Remote Address	The IP address of the device behind the gateway.
Remote Address - Netmask	24 bits netmask.
Perfect Forward Secrecy	Yes or No. Provides additional security through a DH shared secret value. When this feature is enabled, one key cannot be derived from another. This ensures previous and subsequent encryption keys are secure even if one key is compromised.
IPSec Key Group	DH1, DH2, or DH5. Determines how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keysd uring the phase 1 authentication. AirLink Device supports three prime key lengths,including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits).
IPSec SA Life Time	180 to 86400. Determines how long the VPN tunnel is active in seconds. The default value is 28,800 seconds, or 8 hours.
Keep Tunnel Alive	This implies that the tunnel needs to be established automatically and if it the tunnel is pulled down, it needs to be restablished automatically.

Command	Description
NAT-T Keep Alive Interval	Length of time between NAT-T keep alive packets. The default is set to 20 seconds. Users who have devices behind the carrier firewall, and who need to use IPSec, NAT-T feature is useful in such scenarios. As the carrier is performing NAT on the IP traffic, the key exchange required for IPSec cannot be performed, preventing operation of IPSec behind the firewall. With the addition of the NAT-T (NAT Traversal) protocol, IPSec tunnels can be established between devices across the firewall.
NAT-T End Timer	If the tunnel is idle for one whole SA-Life time then the tunnel will not rekey itself. After this period, the carrier waits for that givem time and then takes away the port and IP associated with this device.

GRE

The AirLink Device can act as a Generic Routing Encapsulation (GRE) endpoint, providing a means to encapsulate a wide variety of network layer packets inside IP tunneling packets. With this featureyou can reconfigure IP architectures without worrying about connectivity. GRE creates a point-to-point link between routers on an IP network.

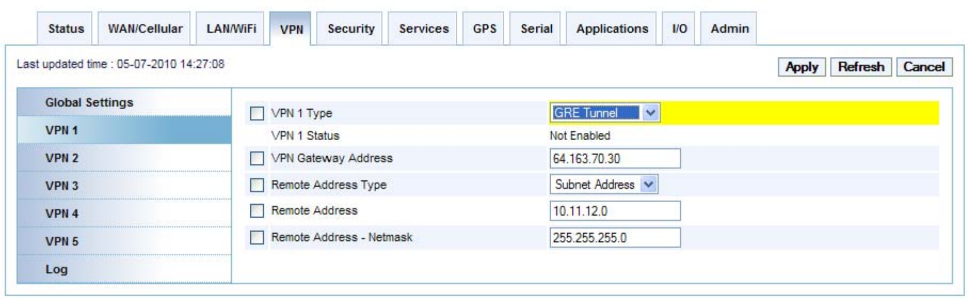


Figure 6-3: ACEmanager: VPN - VPN1- GRE Tunnel

Log

The VPN log can be used for troubleshooting purposes when setting up the IPsec and/or GRE configuration. The Log page will allow you to establish the tunnel connection and monitor the results directly. To change the intervals at which the log is displayed, you can change the settings in Auto Refresh.

Following are few main action tabs on the log page:

- Connect - indicates connecting to the tunnel.
- Refresh - is the option to refresh the page manually.
- Clear - clicking on Clear will clear out the tunnels.
- Apply Policy - will establish tunnel specification.

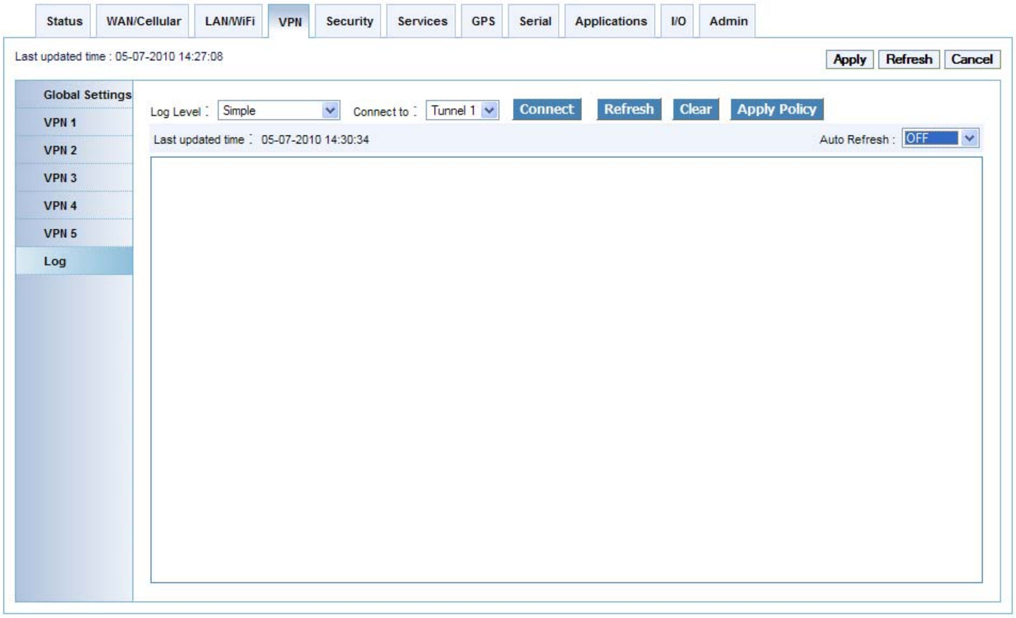


Figure 6-4: ACEmanager: VPN - Log

7: Security Configuration

7

The Security tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

The security tab covers firewall type functions, how data is routed or restricted from one side of the Device to the other, from computers or devices connected to the Device (LAN) and from computers or devices contacting it from a remote source (WAN). These features are set as “rules”.

Tip: *For additional security, it is recommended you change the default password for ACEmanager. Refer to the Admin chapter.*

Solicited vs Unsolicited

How the device responds to data being routed from one network connection to the other depends on the origin of the data.

- If a computer on the LAN initiates a contact to a WAN location (such as a LAN connected computer accessing an Internet web site), the response to that contact would be solicited.
- If, however, a remote computer initiates the contact (such as a computer on the Internet accessing a camera connected to the device), the connection is considered unsolicited.

Port Forwarding and DMZ

In Port Forwarding, any unsolicited data coming in on a defined Public Port will be routed to the corresponding Private Port and Host IP of a device connected to the specified Physical Interface. In addition to a single port forwarded, you can also forward a range of ports.

DMZ defines a single LAN connected device where all unsolicited data should be routed. Anything coming into the ALEOS device on a public port will go directly to that LAN connected device using the same private port.

Note: Port Forwarding and DMZ require Private Mode.

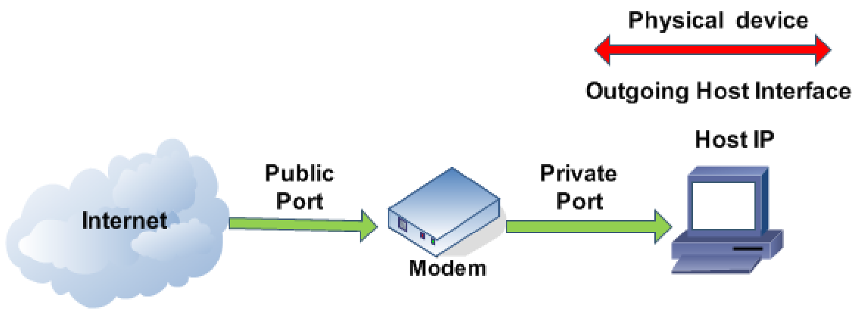


Figure 7-1: Port Forwarding

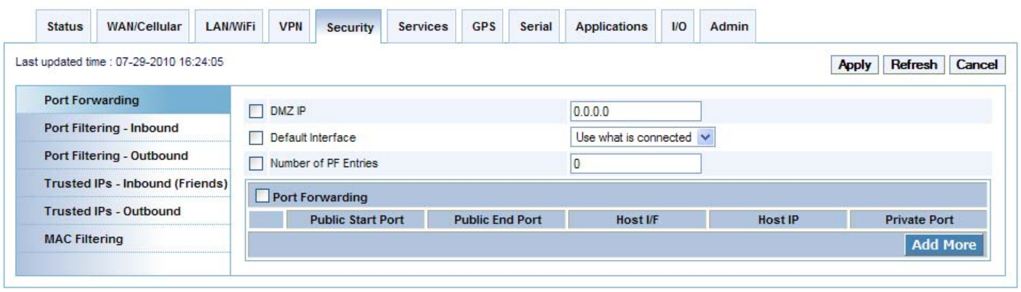


Figure 7-2: ACEmanager: Security - Port Forwarding

Note: The total number of port forwarding supported is 19.

Command	Description
DMZ IP	IP address of a DMZ. The AirLink Device allows a single client to connect to the Internet through a demilitarized zone (DMZ). The DMZ is particularly useful for certain services like VPN, NetMeeting, and streaming video that may not work well with a NAT router. DMZ host is unavailable if IP passthrough is enabled.
Default Interface	Physical connection type to the device. (USB, Ethernet, Serial) 0 = Use whats connected; 2 = Serial PPP; 4 = Ethernet; 5 = USB NDIS; 6 = WiFi
Number of PF entries	The number of port forwarding rules.
Public Start Port	The first of a range or a single port on the public network (cellular network accessible).
Public End Port	The end of the range on the public network (cellular network accessible).
Host Interface (I/F)	Physical connection type to the device. (USB, Ethernet, Serial) Ethernet;Serial PPP; USB NDIS; WiFi

Command	Description
Host IP	IP address of a device connected to the Host I/F interface.
Private Port	The single or starting port on the device at the Host IP. If a public end port is defined, the private port range will be the difference of the public start and end point.

Example of configuring a port forward rule for port forwarding range of 5 ports on an Ethernet connected device:

1. Set number of PF entries to 1.
2. Click on “Add More” to display a rule line.
3. Enter 8080 for the public start port.
4. Enter 8085 for the public end port.
5. Select Ethernet as the Host I/F.
6. Enter 192.168.13.100 as the Host IP.
7. Enter 80 as the private port.

An unsolicited data request coming in to the AirLink device on port 8080, will be forwarded to the LAN connected device, 192.168.13.100, at port 80. In addition, an unsolicited data request coming in from the internet on port 8081,8082, 8083, 8084, and 8085 will be forwarded to 81, 82, 83, 84, and 85 respectively.

Example of configuring the DMZ on an Ethernet connected device:

1. Enter 192.168.13.100 for the DMZ IP.
2. Select Ethernet as the Default Interface.

An unsolicited data request coming in to the AirLink device on any port, will be forwarded to the LAN connected device, 192.168.13.100, at the same port.

Note: The DMZ settings are independent of the number of Port Forward entries and can be used with port forwarding to pass anything not forwarded to specific ports.

Port Filtering- Inbound

Port Filtering-Inbound restricts unsolicited access to the AirLink device and all LAN connected devices.

Port Filtering can be enabled to block ports specified or allow ports specified. When enabled, all ports not matching the rule will be allowed or blocked depending on the mode.

Port Filtering can be configured on individual ports or for a port range. Click Add More for each port filtering rule you want to add.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

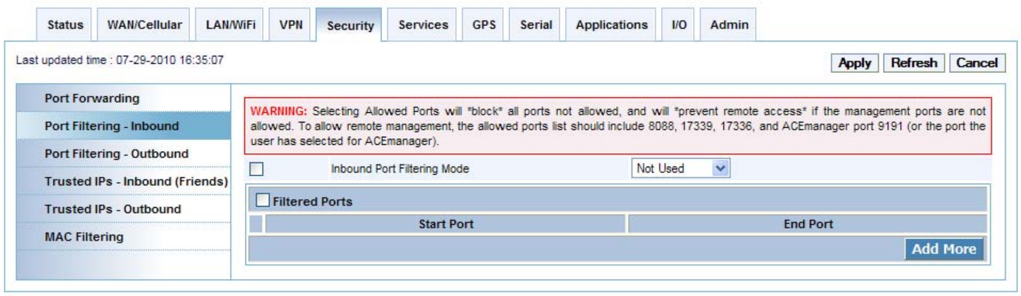


Figure 7-3: ACEmanager: Security - Port FIltering-Inbound

Command	Description
Inbound Port Filtering Mode	0 = Not Used; 1 = Blocked Ports; 2 = Allowed Ports Allowed Ports - All ports through which traffic is allowed are listed below. Blocked Ports - All ports though which traffic is blocked are listed below.
Start Port	The first of a range or a single port on the public network (cellular network accessible).
End Port	The end of the range on the public network (cellular network accessible).

Warning: *Selecting Allowed Ports will *block* all ports not allowed, and will *prevent remote access* if the management ports are not allowed. To allow remote management, the allowed ports list should include 8088, 17339, 17336, and AceManager port 9191 (or the port the user has selected for AceManager).*

Port Filtering-Outbound

Port Filtering-Outbound restricts LAN access to the external network, i.e. the Internet.

Port Filtering can be enabled to block ports specified or allow ports specified. When enabled, all ports not matching the rule will be allowed or blocked depending on the mode.

Port Filtering can be configured on individual ports or for a port range. Click Add More for each port filtering rule you want to add.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

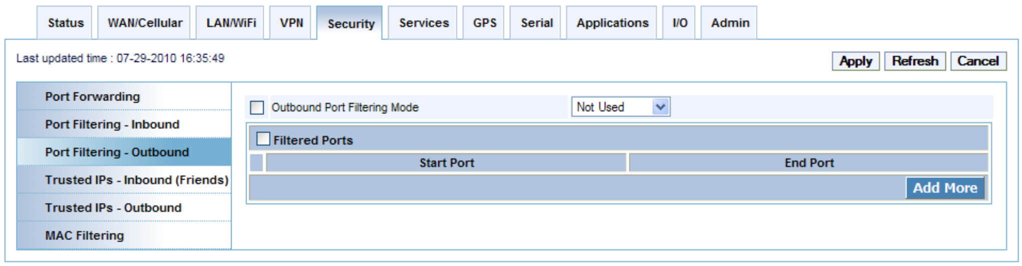


Figure 7-4: ACEmanager: Security - Port Filtering-outbound

Command	Description
Outbound Port Filtering Mode	Allowed and blocked ports through which traffic is either allowed or blocked (respectively) are listed. *Note: Outbound IP filter supports up to 9 ports.*
Start Port	The first of a range or a single port on the LAN.
End Port	The end of the range on the LAN.

Trusted IPs - Inbound

Trusted IPs-Inbound restricts unsolicited access to the AirLink device and all LAN connected devices.

Tip: *Trusted IPs-Inbound was called Friends List in legacy AirLink products.*

When enabled, only packets with source IP addresses matching those in the list or range of trusted hosts will have unrestricted access to the AirLink device and/or LAN connected devices.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

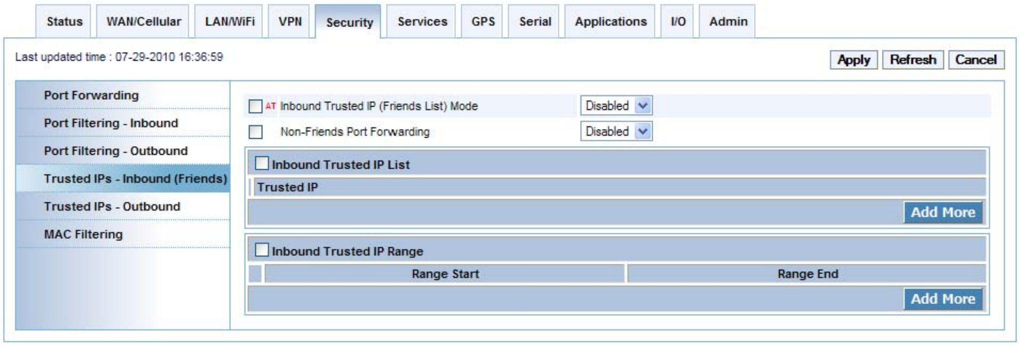


Figure 7-5: ACEmanager: Security - Trusted IPs - Inbound (Friends)

Command	Description
Inbound Trusted IP (Friend's List) Mode	Disabled or Enabled. Disables or Enables port forwarding rules.
Non-Friends Port Forwarding	Non-Friends port forwarding is like an allow rule for any of the forwarded ports. If it is enabled, the port forwarding rules apply to all incoming packets. If it is diabled, only Friends List IPs get through.
Trusted IP	Each entry can be configured to allow a single IP address, for example 64.100.100.2, or the IP addresses from a complete subnet, such as 64.100.10.255 allowing all IP addresses from 64.100.10.0 to 64.100.10.255.
Range Start	Specify the IP address range that is allowed access, for example 64.100.10.2 to start and 64.100.10.15 to end would allow 64.100.10.5 but would not allow 64.100.10.16.
Range End	

Trusted IPs - Oubound

Trusted IPs-Outbound restricts LAN access to the external network, i.e. the Internet.

When enabled, only packets with the destination IP addresses matching those in the list of trusted hosts will be routed from the LAN to the external location.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

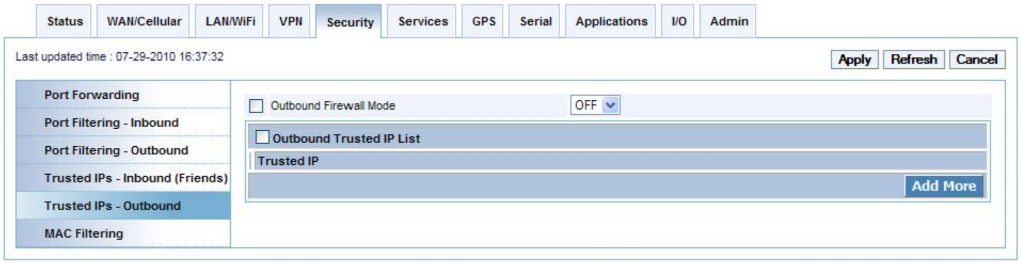


Figure 7-6: ACEmanager: Security - Trusted IPs - Outbound

Command	Description
Outbound Firewall Mode	Disabled or Enabled. Disables or Enables port forwarding rules.
Trusted IP	Each entry can be configured to allow a single IP address, for example 64.100.100.2, or the IP addresses from a complete subnet, such as 64.100.10.255 allowing all IP addresses from 64.100.10.0 to 64.100.10.255.

MAC Filtering

MAC filtering restricts LAN connection access. You can specifically block or allow a connection from a computer or other device by blocking or allowing the MAC address of its network interface adapter.

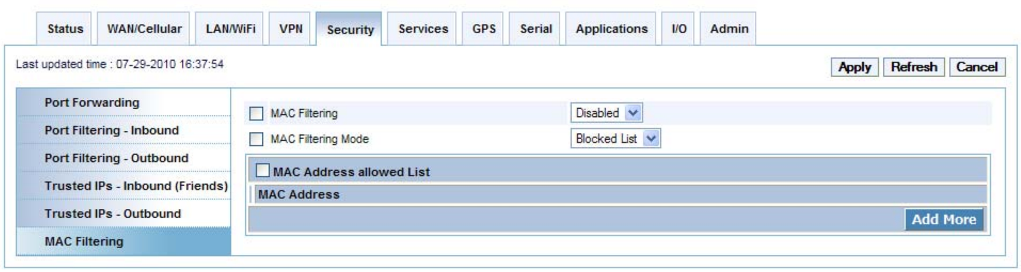


Figure 7-7: ACEmanager: Security - MAC Filtering

Command	Description
MAC Filtering	Enable or disable MAC Filtering.
MAC Filtering Mode	Allows or blocks the MAC Addresses listed. You can add the MAC addresses by clicking on *Add More*.
MAC Address	This is the MAC Address of the interface adapter on a computer or other device.

8: Services Configuration

The Services tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

The services sections allows configuration of external services that extend the functionality of the AirLink Device.

ACEmanager

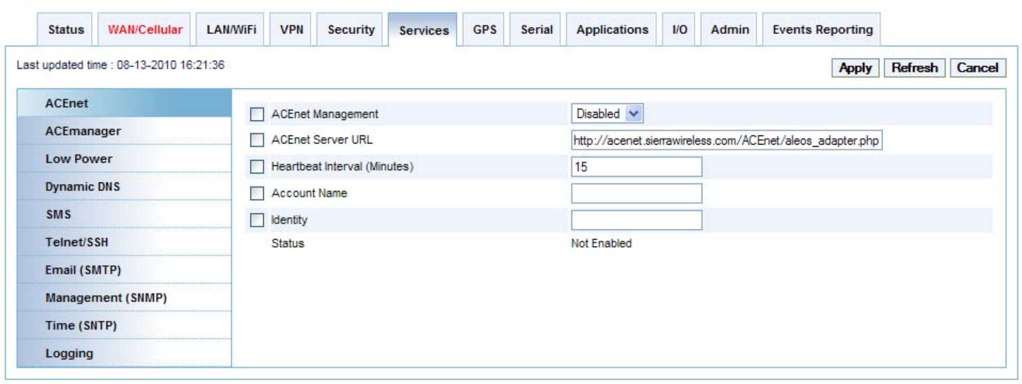


Figure 8-1: ACEmanager: Services - ACEmanager

Command	Description
ACEnet Management	Enable for ACEmanager to run in: • Tethered Host only • Tethered Host and OTA • All
ACEnet Server URL	This is the ACEnet server URL address.
Heartbeat Interval (Minutes)	The default is 15 minutes. This field determines how often the AirLink device checks for software updates and settings changes from ACEnet. ACEnet can also query the AirLink device at a regular interval if settings allow. Please refer to ACEnet documentation for more information.

Command	Description
Account Name	Your account name
Identity	Connected or Not Connected.
Status	Displays the status of ACEnet connection.
ACEmanager port	Port for ACEmanager, for example, 9191. Reboot the device if you change the port settings.

Low Power

The AirLink device will put itself into a low power using mode when configured events occur. Low Power mode is essentially a standby mode which uses minimal power while being ready to “come alive” quickly. If you are not connecting to an MP PinPoint line device, you will not see this group.

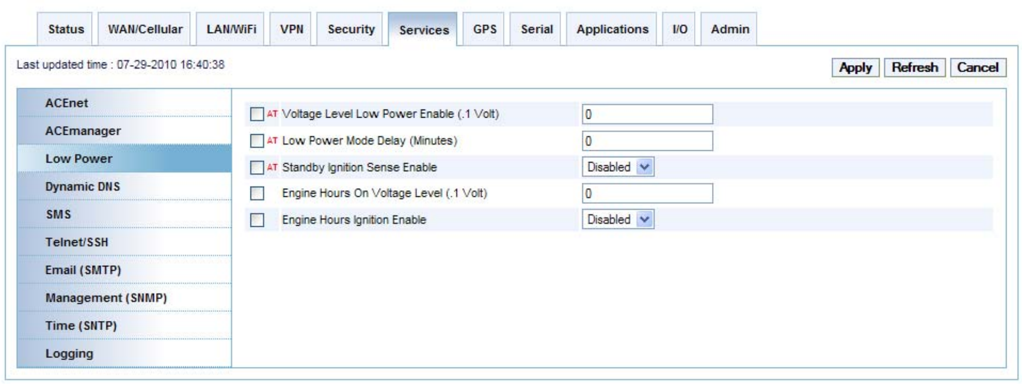


Figure 8-2: ACEmanager: Services - Low Power

Command	Description
Voltage Levl Low Power Enable (.1Volt)	Set or query the voltage level at which the device goes into low power mode. • Ignore voltage for power control. • threshhold in tenths of volts Example: ATVLTG=130 would place the device in a low power use, standby state if the voltage goes below 13.0V. *Note: When Ignition sense is enabled, there is no no need to configure this parameter with ignition sense enable.*
Low Power Mode Delay (Minutes)	Number of minutes after one of the power down events (VTLG or DTRP) happens until the AirLink device enters the low power mode. If DTRP and VLTG are both 0 (zero), this setting does nothing. • n=0-255 minutes *Note: There is always a minimum of 1 minute between power down event and actual shutdown (to give the AirLink device time to prepare); entering zero will not power down the device immediately, but after one minute.In the first 5 minutes after AirLink device powers up, power down events are ignored to give the user time to change configurations.*
Standby Ignition Sense Enable	Standby Ignition Sense Enable: the AirLink device will monitor the ignition sense on the power connector and enter the low power consumption stand-by mode when the ignition is turned-off. • n=0 : Disable • n=1 : Enable
Engine Hours on Voltage Level (.1 Volt)	Set the voltage above which the Engine should be considered "ON". To enter a voltage of 13.0 volts, enter 130.
Engine Hours Ignition Enable	Engine Hours will be counted when enabled.

Configuring Engine Hours

ALEOS can keep track of Engine Hours and how long the engine has been on, which is determined by either Ignition Sense or the Power In voltage. In the Low Power group, under Common, there two configuration fields to govern how Engine Hours is determined.

- **Engine On Voltage Level (.1 Volt)** - Use the PowerIn voltage to monitor engine usage. Set the voltage to higher than the maximum “at rest” voltage of your battery to track how long the device has power.
- **Engine Hours Ignition Enable** - Use ignition sense to monitor how long the engine has been on.

A typical battery will be below 13.0 Volts, while a typical vehicle maintains the voltage at 14.4 volts. So a value of 130 (13.0 Volts) will identify when the engine is on, correctly.

Dynamic DNS

Dynamic DNS allows a AirLink Device WAN IP address to be published to appropprietary Sierra Wireless dynamic DNS service called IP Manager.

If you have a fleet of Sierra Wireless AirLink devices or even if you only have one, it can be difficult to keep track of the current IP addresses, especially if the addresses aren't static but change every time the devices connect to the cellular network. If you need to connect to a gateway, or the device behind it, it is so much easier when you have a domain name (car54.mydomain.com, where are you?).

Reasons to contact the device and/or the connected device:

- Requesting a location update from a delivery truck.
- Contacting a surveillance camera to download logs or survey a specific area.
- An oil derek that needs to be triggered to begin pumping.
- Sending text to be displayed by a road sign.
- Updating the songs to be played on a juke box.
- Updating advertisements to be displayed in a cab.
- Remote access to a computer, a PLC, an RTU, or other system.
- Monitoring and troubleshooting the status of the device itself without needing to bring it in or go out to it.

A dynamic IP address is suitable for many Internet activities such as web browsing, looking up data on another computer system, data only being sent out, or data only being received after an initial request (also called Mobile Originated). However, if you need to contact the AirLink device directly, a device connected to the AirLink device, or a host system using your AirLink device (also called Mobile Terminated), a dynamic IP won't give you a reliable address to contact (since it may have changed since the last time it was assigned).

Domain names are often only connected to static IP addresses because of the way most domain name (DNS) servers are set-up. Dynamic DNS servers require notification of IP Address changes so they can update their DNS records and link a dynamic IP address to the correct name.

- Dynamic IP addresses are granted only when your AirLink device is connected and can change each time the gateway reconnects to the network.
- Static IP addresses are granted the same address every time your AirLink device is connected and are not in use when your gateway is not connected.

Since many cellular providers, like wire-based ISPs, do not offer static IP addresses or static address accounts cost a premium vs. dynamic accounts, Sierra Wireless AirLink Solutions developed IP Manager to work with a Dynamic DNS server to receive notification from Sierra Wireless AirLink devices to translate the dynamic IP address to a fully qualified domain name. Thus, you can contact your AirLink device directly from the Internet using a domain name.

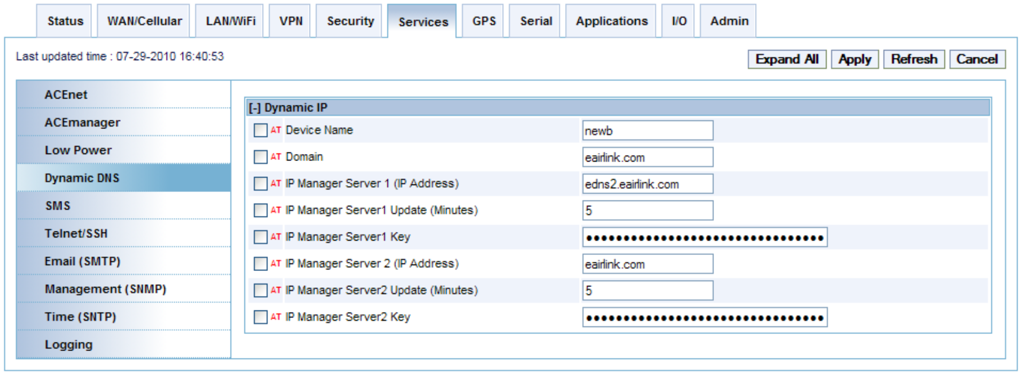


Figure 8-3: ACEmanager: Services - Dynamic DNS

Command	Description
Device Name	The name you want for the device. There are some restrictions listed below for the device name.
Domain	The domain name to be used by the device. This is the domain name of the server configured for *IPMANAGER1
IP Manager 1	The IP address or domain name of the dynamic DNS server which is running IP Manager.
IPMServer Update1/ IPMServer Update 2	How often, in minutes, you want the address sent to IP Manager. If this is set to zero, the device will only send an update if the IP address changes (example, if your AirLink device is reset or is assigned a different IP address).
IPMServer 1 Key/ IPMServer 2 Key	User defined password key which is used instead of AirLink secret key when using an IP Manager server other than the one provided by Sierra Wireless.

Tip: *Some PPPoE connections can use a Service Name to differentiate PPPoE devices. Use the device name to set a Station Name for the PPPoE connection.*

Understanding Domain Names

A domain name is a name of a server or device on the Internet which is associated with an IP address. Similar to how the street address of your house is one way to contact you and your phone number is another, both the IP address and the domain name can be used to contact a server or device on the Internet. While contacting you at your house address or with your phone number employ different methods, using a domain name instead of the IP address actually uses the same method, just a word based name is commonly easier to remember for most people than a string of numbers.

Understanding the parts of a domain name can help to understand how IP Manager works and what you need to be able to configure the device. A fully qualified domain name (FQDN) generally has several parts.

- **Top Level Domain** (TLD): The TLD is the ending suffix for a domain name (.com, .net, .org, etc.)
- **Country Code Top Level Domain** (ccTLD): This suffix is often used after the TLD for most countries except the US (.ca, .uk, .au, etc.)
- **Domain name**: This is the name registered with ICANN (Internet Corporation for Assigned Names and Numbers) or the registry for a the country of the ccTLD (i.e. if a domain is part of the .ca TLD, it would be registered with the Canadian domain registry). It is necessary to have a name registered before it can be used.
- **Sub-domain or server name**: A domain name can have many sub-domain or server names associated with it. Sub-domains need to be registered with the domain, but do not need to be registered with ICANN or any other registry. It is the responsibility of a domain to keep track of its own subs.

car54.mydomain.com

- ***.com*** is the TLD
- *mydomain* is the domain (usually noted as mydomain.com since the domain is specific to the TLD)
- *car54* is the subdomain or server name associated with the device, computer, or device registered with mydomain.com

car54.mydomain.com.ca

This would be the same as above, but with the addition of the country code. In this example, the country code (.ca) is for Canada.

Tip: *A URL (Universal Resource Locator) is different from a domain name in that it also indicates information on the protocol used by a web browser to contact that address, such as* `http://www.sierrawireless.com`*.* www.sierrawireless.com *is a fully qualified domain name, but the http://, the protocol identifier, is what makes the whole thing a URL.*

Dynamic Names

When an IP address is not expected to change, the DNS server can indicate to all queries that the address can be cached and not looked up for a long period of time. Dynamic DNS servers, conversely, have a short caching period for the domain information to prevent other Internet sites or queries from using the old information. Since the IP address of a device with a dynamic account can change frequently, if the old information was used (such as with a DNS server which indicates the address can be cached for a long period of time) when the IP address changed, the domain would no longer point to the new and correct IP address of the device.

If your AirLink device is configured for Dynamic IP, when it first connects to the Internet, it sends a IP change notification to IP Manager. IP Manager will acknowledge the change and update the Dynamic DNS server. The new IP address will then be the address for your device’s configured name.

Once your device's IP address has been updated in IP Manager, it can be contacted via name. If the IP address is needed, you can use the domain name to determine the IP address.

Note: The fully qualified domain name of your AirLink device will be a subdomain of the domain used by the IP Manager server.

SMS

ALEOS has the ability to :

- Receive commands via SMS message
- Provide information
- Perform an action
- Act as an SMS gateway for hosts connected to its local interfaces

Warning: *To use SMS with your AirLink device, you will need an account with SMS enabled and your carrier cannot block SMS for data accounts.*

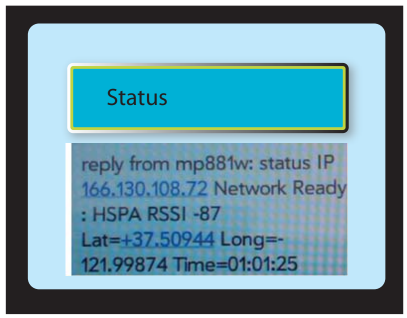
Note: The ability to send or receive SMS requires specific security settings.

Command Parser

The ALEOS command parser SMS feature allows some remote management of the AirLink device with SMS messaging. SMS allows users to control:

- Current Status
- Reset AirLink device
- Control up to two relays at a device at I/O

When an SMS command is received from a pre-defined "Trusted" phone number, the AirLink device performs the action requested and sends a response back to that same phone number.

SMS Command	Device Action	SMS Response
Note: All responses start with "reply from [modem name]:"		
status	**None**	**Raven-line, pinpoint-line or MP-line** [Network IP] [Network Status]: [technology type] RSSS [original] **PinPoint/MP adds** Lat = [Latitude] Long = [Longitutde] Time = [hh:mm:ss] 
reset	Resets the device 30 seconds after the first response message is sent.	First message: Reset in 30 seconds Second message: Status message when back up.
relay x y	Sets the applicable relay to the desired setting.	relay x set to y x can be 1 or 2 y can be 0 or 1

SMS Gateway

The SMS gateway feature allows messages to or from a locally connected host to use SMS for over the air transmission.

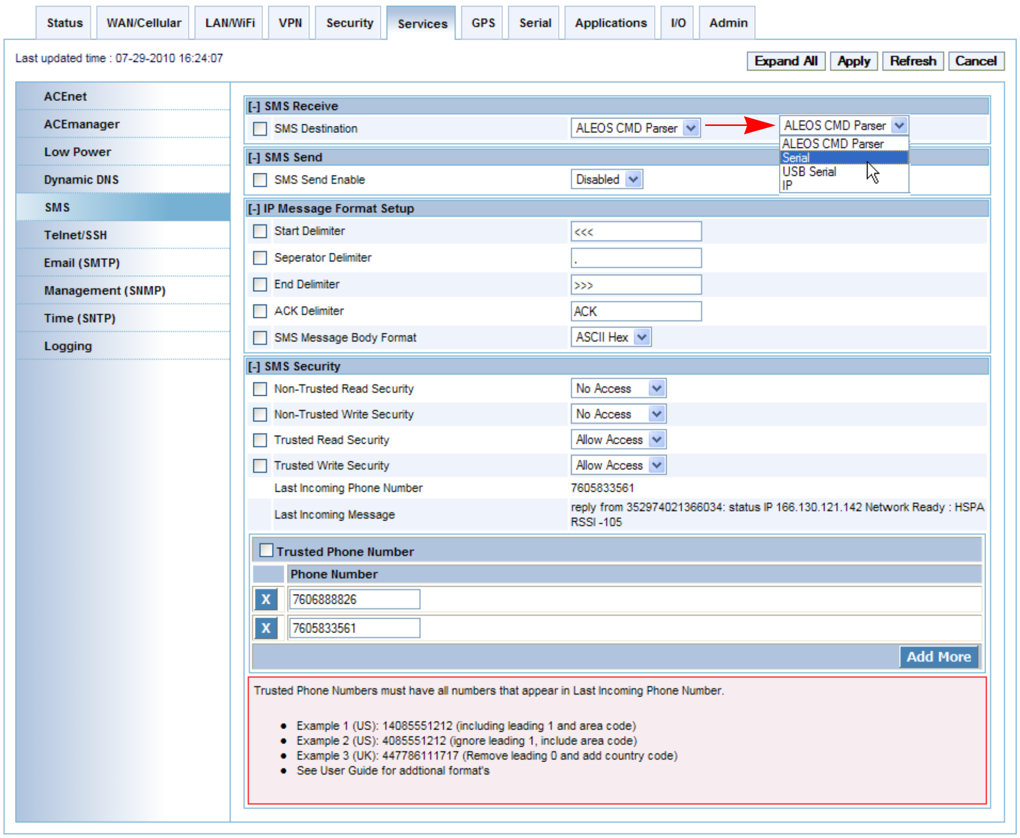
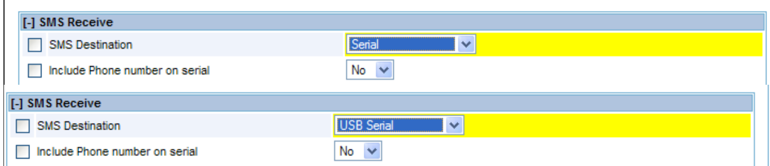
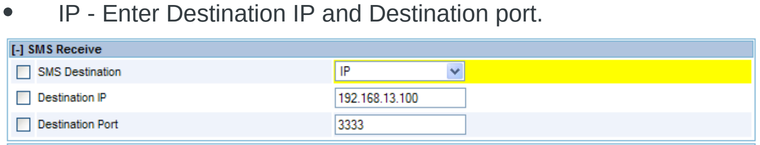


Figure 8-4: ACEmanager: Services - SMS

Command	Description
SMS Destination	Allows you to chose where the SMS message is going to be locally received and if it is going to be received by ALEOS command parser or by a host on the other side (Host, USB serial or IP) select the SMS destination. Select your destination for the SMS and based on your selection additional fields may become available. Incoming messages are sent to the specified host. This can be a serial interface or an IP and port. If no host routing is configured, ALEOS treats the message as an ALEOS SMS Command. Messages sent to an IP address and port are put in the Airlink SMS Protocol in a UDP packet. ALEOS then routes this packet to the matching host interface (Ethernet, USBNet, WiFi) If you chose: • Serial or USB Serial - Select “Yes” or “No” to Incoming Phone number on serial.  • IP - Enter Destination IP and Destination port. 
SMS Send Enable	Send SMS from the connected Host, which is the device connected locally to the ALEOS device such as a computer ir digital sign. When this field is enabled it will require a ALEOS port. To send an SMS (outgoing) • From the seria port” From the CLI there is a new AT command to send SMS messages: AT*SMSM2M="<phone> <message>" This allows an SMS messages to be sent to another modem as a single line item. • From a Host Device PC's and other devices connected to the Host IP interfaces (Ethernet, USBNet, WiFi) can also send SMS messages from the modem. To send an outgoing SMS from the host device, a program on the PC will need to send a message to a user defined port in ALEOS. The message has to be in AirLink SMS Protocol, that contains the phone number and message body (text). ALEOS will parse the message and send an SMS. *See below for examples of the SMS body text.*
Delimiter	Start Delimiter - Inbound message at the beginning of the message. End Delimiter - Inbound message at the end of the message. For example, SMS to the phone number is “Left Lane Closed”. ALEOS to Host - <<<left lane closed>>> The packet sent to the host will have start and end delimiter which surrounds the message.
ACK Delimiter	ALEOS will provide an ACK on every SMS message when it is passed to the radio. Infa application to wait for ACK before sending next SMS message. If ALEOS does not send an ACK wait for 30 seconds and retry.

Command	Description
SMS Message Body Format	The only SMS body format available is the ASCII-Hex. The other types of SMS body format are set SMS protocols.
Non Trusted Read Security	This refers to the phone numbers entered in the trusted phone number list. Indicate with your selection - Access or No Access if you want to allow or block non trusted and trusted phone numbers to either read or write. Default is “No Access” and trusted phone number gets read or write. *Note: All four settings of read and write respectively are independant of each other.*
Trusted Read Security	
Non Trusted Write Security	
Trusted Write Security	
Last Incoming Phone Number	The last incoming phone number is displayed here and will be erased with a reboot.
Last Incoming Message	The last incoming message is the last incoming sms from the phone number.
Trusted Phone Number	Trusted phone numbers are listed here.

Add a Trusted Phone Number

Follow the instructions below to add a Trusted Phone Number on the SMS page.

1. Send an SMS command to the device and hit Refresh. No maintenance response will be sent to a number until it is defined as Trusted.
2. Once you have the Last incoming Phone number, that shows up on the SMS screen in ACEmanager, note the exact phone number displayed.
3. Click on Add More to add a Trusted Phone Number.

Note: The Trusted Phone number can be 15 characters and has to be numbers only.

4. Enter the Last incoming Phone number as the Trusted Phone Number.
5. Click on Apply.

Note: Do not enter any extra digits and use the Last incoming displayed as a guide to type the phone number. Use “1” only if it is used in the beginning of the Last incoming Phone number.

AirLink SMS Protocol

There are two new commands and they are:

- at*smsm2m_8 - for 8 bit data mode.
- at*smsm2m_u - for unicode.

Unlike at*smsm2m, the data following the phone number must be a hex string.

The hex string is converted to bytes before sending.

For example:

at*smsm2m_8="17604053757 5448495320495320412054455354"

sends the message "THIS IS A TEST"

but the message is 8 bit data.

Similarly,

at*smsm2m_8="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f"

will send the bytes:

00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f

Sample message using ethernet (from the Host to ALEOS):

<start> 8889008989<sep>8BIT<sep>8<sep> 0F0A000989F68898<end>

Format Message

Telnet

The device can be connected to using the Telnet protocol. Once in a telnet session with the device you can send AT commands.

A secure mechanism to connect remote clients is requirement for many users. In ACEmanager now, we have Secure Shell (SSH), which will ensure confidentiality of the information and make the communication less susceptible to snooping and man-in-the-middle attacks.

SSH also provides for mutual authentication of the data connection.

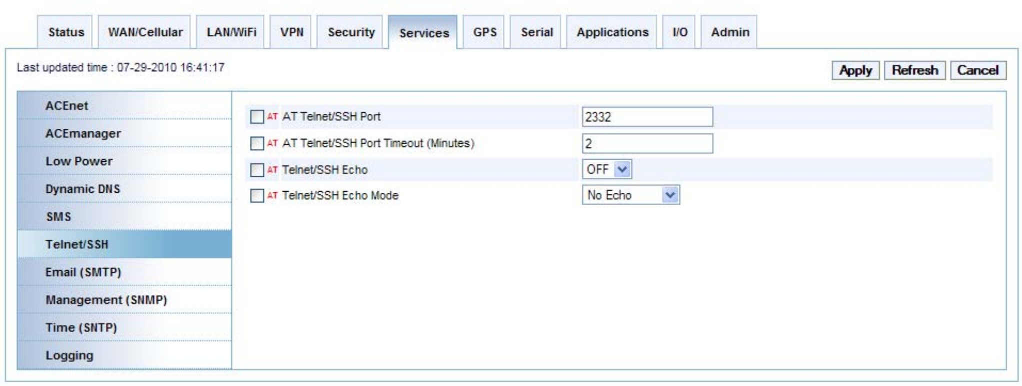


Figure 8-5: ACEmanager: Services - Telnet

Command	Description
AT Server mode	Select either Telnet or SSH mode.
AT Telnet/SSH Port	Sets or queries the port used for the AT Telnet / SSH server. If 0 is specified, the AT Telnet server will be disabled. The default value is 2332. • n=0 : Disabled. • n=1: 65535 **Tip:** *Many networks have the ports below 1024 blocked. It is recommended to use a higher numbered port.* After configuring SSH, apply and rest your device.
AT Telnet Port Timeout (Minutes)	Telnet port inactivity time out. By default, this value is set to close the AT telnet connection if no data is received for 2 minutes. • n=minutes
Telnet/SSH Echo	Enable or disable toggle AT command echo mode.
Telnet/SSH Echo Mode	This is a negotiation protocol. The options are : • No echo - Neither local or telnet echo • Remote echo - tells telnet remotelt echo. *Note: This field is not available for SSH.*

Note: When you are connected to SSH locally, you cannot have OTA SSH connected.

Email (SMTP)

For some functions, the device needs to be able to send email. Since it does not have an embedded email server, you need to specify the email setting for the device to use.

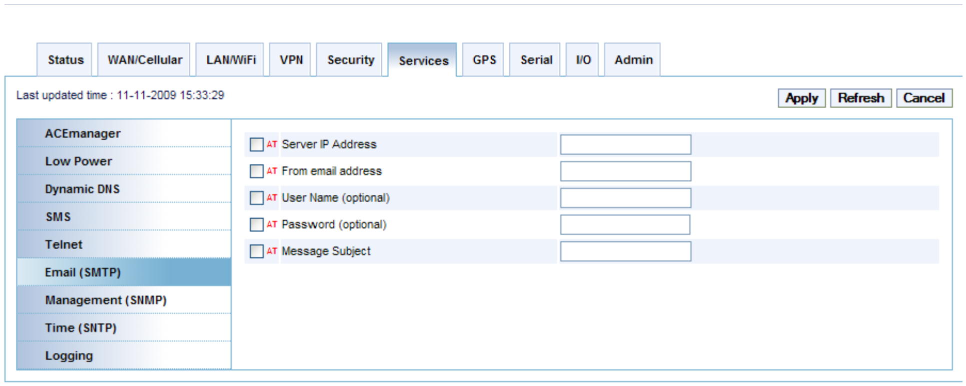


Figure 8-6: ACEmanager: Services - Email (SMTP)

Command	Description
Server IP Address	Specify the IP address or Fully Qualified Domain Name (FQDN) of the SMTP server to use. • d.d.d.d = IP Address • name = domain name (maximum: 40 characters).
From email address	Sets the email address from which the SMTP message is being sent. • email = email address (maximum: 30 characters).
User Name (Optional)	Specifies the username to use when authenticating with the server.
Password (Optional)	Sets the password to use when authenticating the email account (*SMTPFROM) with the server (*SMTPADDR). • pw = password *Note: Not required to use SMTP settings but may be required by your cellular carrier.*
Message Subject	Allows configuration of the default Subject to use if one isn't specified in the message by providing a “Subject: xxx” line as the initial message line. • subject = message subject

Management (SNMP)

The Simple Network Management Protocol (SNMP) was designed to allow remote management and monitoring of a variety of devices from a central location. The SNMP management system is generally composed of agents (such as your PinPoint XT, a router, a UPS, a web server, a file server, or other computer equipment) and a Network Management Station (NMS) which monitors all the agents on a specific network. Using the management information base (MIB), an NMS can include reporting, network topology mapping, tools to allow traffic monitoring and trend analysis, and device monitoring.

Authentication ensures SNMP messages coming from the agent, such as the PinPoint XT, have not been modified and the agent may not be queried by unauthorized users. SNMPv3 uses a User-Based Security Model (USM) to authenticate and, if desired or supported, message encryption. USM uses a user name and password specific to each device.

The PinPoint XT can be configured as an SNMP agent and supports SNMPv2c and SNMPv3.

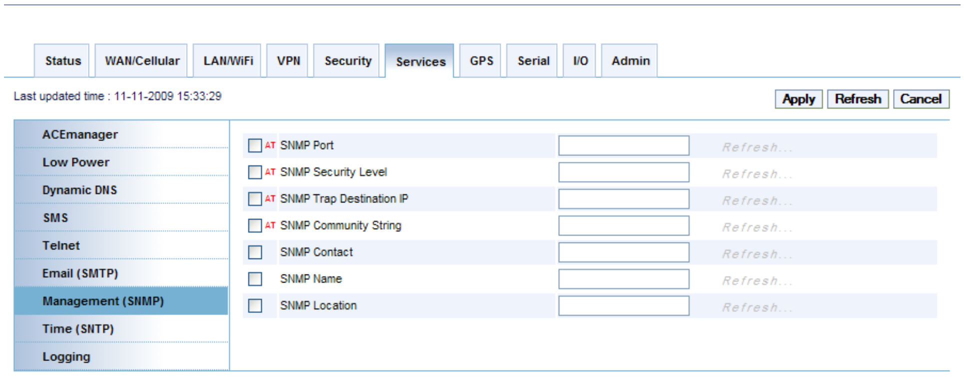


Figure 8-7: ACEmanager: Services- Management (SNMP)

Command	Description
SNMP Port	This controls which port the SNMP Agent listens on. • SNMP is disabled • 65535
SNMP Security Level	Selects the security level requirements for SNMP communications. • No security required. SNMPv2c and SNMPv3 communications are allowed. • Authentication equivalent to “authNoPriv” setting in SNMPv3. SNMPv3 is required to do authentication, SNMPv2c transmissions will be silently discarded. • Authentication and encryption, equivalent to “authPriv”' setting in SNMPv3. SNMPv3 is required to do authentication and encryption, SNMPv2c and SNMPv3 authNoPriv transmissions will be silently discarded. Messages are both authenticated and encrypted to prevent a hacker from viewing its contents.
SNMP Trap Destination	Controls destination for SNMP Trap messages. If port is 0 or host is empty, traps are disabled. Traps are sent out according to the SNMP security level (i.e. if the security level is 2, traps will be authenticated and encrypted). Currently, the only trap that can be generated is linkup. • host = IP address • port = TCP port
SNMP community String	The SNMP Community String acts like a password to limit access to the device’s SNMP data. • string = string of no more than 20 characters (default = public).
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.

Command	Description
SNMP Name	This is the name of the device you want to refer to. This is a customer defined field.
SNMP Location	Location of where your device is stored. This is a customer defined field.

Time (SNTP)

The device can be configured to synchronize it's internal clock with a time server on the Internet using the Simple Network Time Protocol.

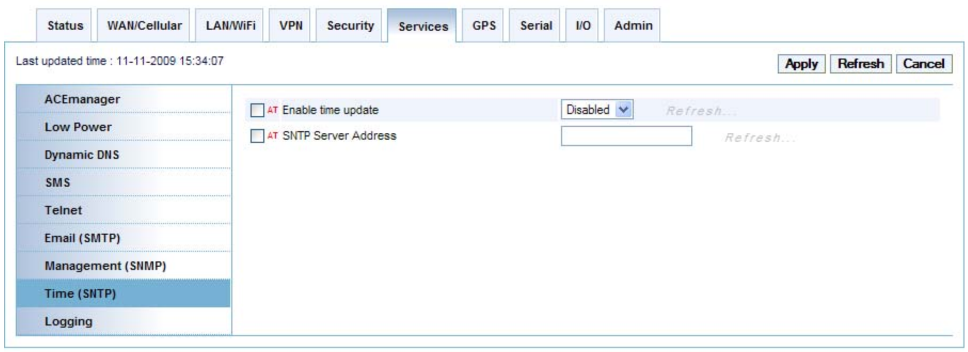


Figure 8-8: ACEmanager: Services - Time (SNTP)

Command	Description
Enable Time Update	Enables daily SNTP update of the system time. • n=0 : Off • n=1 : On
SNTP Server Address	SNTP Server IP address, or fully qualified domain name, to use if *SNTP=1. If blank, time.nist.gov is used. • d.d.d.d=IP address • name=domain name

Logging

For troubleshooting purposes, tech support may direct you to enable certain logging elements and then, after a span of time, download a log file from the device using Modem Doctor.

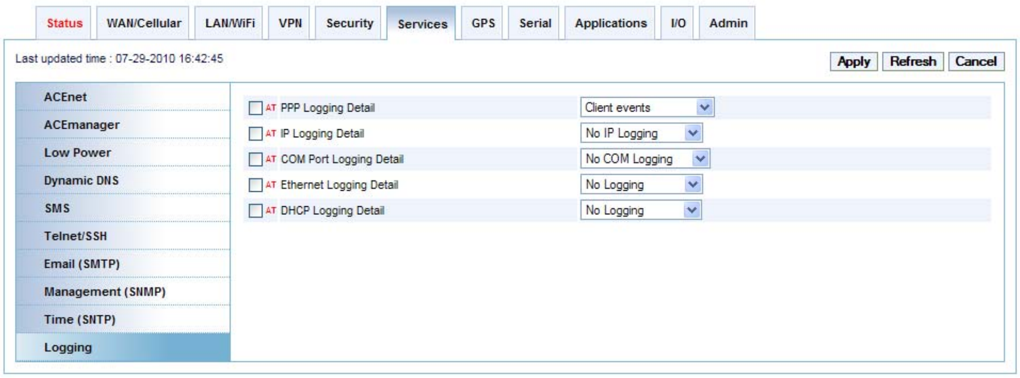


Figure 8-9: ACEmanager: Services - Logging

Command	Description
PPP Logging Detail	Sets the logging level for the PPP stack. • No logging • Log client events (default) • Log server events • Log client and Server events
IP Logging Detail	Sets the logging level for the IP subsystem. • No IP logging • Invalid Packets • Received Packets • Received and Sent Packets
COM Port Logging Detail	Set the logging level for the host or module COM port. • No logging • Host COM Port • Module COM Port
Ethernet Logging Detail	Sets the logging level for the Ethernet port. • No logging • Log errors: invalid/corrupt packets, etc. • Log the header of all received packets. Note that this can quickly exhaust available space for the event log.
DHCP Logging Detail	Enable or disable internal DHCP logging. • No logging • Log DHCP events

9: GPS Configuration

The GPS tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

GPS

This group includes commands specific to GPS features and the AirLink Device.

The AirLink device is equipped with a Global Positioning System receiver (GPS) to ascertain its position and track the movements of a vehicle or other devices which move. The AirLink device relays the information of its location as well as other data for use with tracking applications.

Tracking Applications used with Sierra Wireless PinPoint line devices:

- Air-Trak
- Track Your Truck
- Track Star
- DeLorme Street Atlas USA
- Microsoft Streets and Trips
- CompassCom
- Zoll Data
- and many more...

GPS Overview

The Global Positioning System (GPS) is a satellite navigation system used for determining a location and providing a highly accurate time reference almost anywhere on Earth. The US military refers to GPS as Navigation Signal Timing and Ranging Global Positioning System (NAVSTAR GPS).

GPS consists of a “constellation” of at least 24 satellites in 6 orbital planes. Each satellite circles the Earth twice every day at an altitude of 20,200 kilometers (12,600 miles). Each satellite is equipped with an atomic clock and constantly broadcasts the time, according to its own clock, along with administrative information including the orbital elements of its motion, as determined by ground-based observatories.

A GPS receiver, such as the AirLink device, requires signals from four or more satellites in order to determine its own latitude, longitude, and elevation. Using time synced to the satellite system, the receiver computes the distance to each satellite from the difference between local time and the time the satellite signals were sent (this distance is called psuedoorange). The locations of the satellites are decoded from their radio signals and a database internal to the receiver. This process yields the location of the receiver. Getting positioning information from fewer than four satellites, using imprecise time, using satellites too closely positioned together, or using satellites too close to the Earth's curve will yield inaccurate data.

The GPS data is then transmitted to a central location which uses a tracking application to compile information about location, movement rates, and other pertinent data.

Note: Depending on the location of the satellites in relation to the device's location and how many signals are being received, the AirLink device may encounter "GPS drift". The AirLink device may report it is in a location a few feet from its actual location because it does not employ differential GPS.

AirLink device Supported Protocols

The AirLink device supports three different GPS reporting protocols.

Remote Access Protocol (RAP)

The Remote Access Protocol (RAP) is a proprietary binary message format developed by Sierra Wireless AirLink Solutions. RAP was originally designed to work specifically with AirLink Tracking System (ATS), but other 3rd party applications have been developed to take advantage of the RAP messaging format.

In the original RAP, a PinPoint line device uses the UDP (User Datagram Protocol) to communicate with the host server.

In RAP-based AVL, each PinPoint line device sends its command status and responses to the Host server and the Host sends commands to one or more PinPoint line devices. For reliability, the Host expects each command to be acknowledged within a time-out period. If the acknowledgement packet (ACK) is not received within the time-out period, the Host will retransmit the command.

The RAP messages are in Hex and are referred to by their message ID. Reports can include GPS data alone, as well as GPS data with the date and time, radio frequency data, and state changes of I/O as well as sending reports based on power states.

Examples of tracking applications using RAP:

- Air-Trak
- TrackStar
- CompassCom
- Zoll Data

- HTE
- Spillman
- and others...

National Marine Electronics Association (NMEA)

National Marine Electronics Association (NMEA) is a protocol by which marine instruments and most GPS receivers can communicate with each other. NMEA defines the format of many different GPS message (sentence) types, which are intended for use by navigational equipment.

Example of a tracking application using NMEA:

- Microsoft Streets and Trips

Tip: *For more information on the AirLink device supported NMEA message formats, please refer to the Appendix.*

Trimble ASCII Interface Protocol (TAIP)

Trimble ASCII Interface Protocol (TAIP) is a digital communication interface based on printable ASCII characters over a serial data link. TAIP was designed specifically for vehicle tracking applications but has become common in a number of other applications, such as data terminals and portable computers, because of its ease of use.

Example of a tracking application using TAIP:

- DeLorme Street Atlas USA

Tip: *For more information on TAIP message formats, refer to the Appendix and to the Sierra Wireless MP 3G device TAIP Reference.*

Datum

The GPS datum is the method of ascertaining the position of the GPS device using a specific reference point location. The datum used can influence the accuracy of the GPS positioning.

In addition to different reporting protocols, the AirLink device supports the most widely used GPS datum:

WGS84

NAD83

NAD27

Before you Configure GPS

To decide what configuration you need for your AirLink device, there are some fundamental considerations you should determine:

- **Protocol:** What is the GPS protocol used by your tracking application and what type of reports will you need?
- **Datum:** What is the datum supported by your tracking application?
- **Dynamic IP Address:** Will you need DNS support to handle a dynamic IP address account?
- **Multiple GPS servers:** Will you need to have GPS data send to more than one GPS server?

Server 1

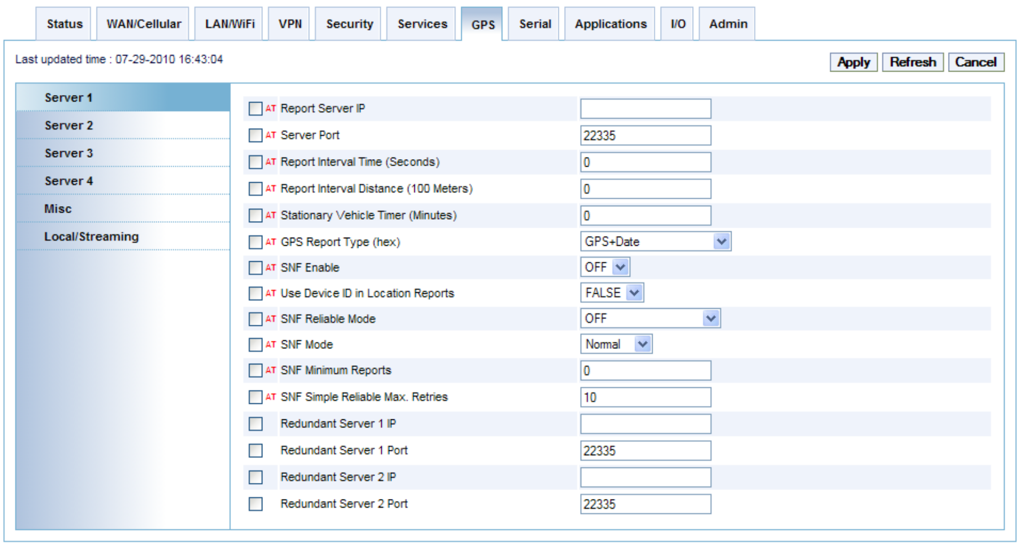


Figure 9-1: ACEmanager: GPS Server 1

Table 9-1: GPS: Server 1

Command	Description
Report Server IP	IP address where GPS reports are sent (ATS Server IP). Also see *PPPORT. • d.d.d.d=IP address Example: AT*PPIP=192.100.100.100
Server Port	Port where GPS reports are sent. • n=1-65535

Table 9-1: GPS: Server 1

Command	Description
Report Interval Time	GPS Report Time Interval. See also *PPMINTIME, *PPTSV, +CTA. n=seconds (1 - 65535) *Note: Your cellular carrier may impose a minimum transmit time.* **Caution:** *A report time of less than 30 seconds can possibly keep an RF link up continuously. This will eventually cause the AirLink Device to overheat and shutdown. An RF resource may continue be tied up to transfer small amounts of data. Generally the RF channel will be released and go dormant in 10-20 seconds of no data sent or received.*
Report Interval Distance	GPS Report Distance Interval in 100 Meter Units (kilometer). 1 mile is approximately 1600 kilometers. • n=0 : Disabled • n=1-65535
Stationary Vehicle Timer (Minutes)	Timer for Stationary Vehicles. Time interval in minutes that the AirLink Device device will send in reports when it is stationary. • n=0 : Disabled • n=1-255 minutes For example, if *PPTIME=10, the AirLink Device will send in reports at least every 10 seconds while it is moving; however, once it stops moving, it will slow the reports down to this *PPTSV value. *Note: In order for the PPTSV (Stationary Vehicle timer) to take effect, the PPTIME value must be set to a value greater than 0 and less than the PPTSV value. The PPTSV timer checks for vehicle movement at the PPTIME interval, so if PPTIME is disabled, then PPTSV will also be disabled.*
GPS Report Type (hex)	GPS report type. • n=0 : Use legacy reports specified in *MF value. Note: Must also have *PPDEVID=0. • n=0x11 : Standard GPS Report • n=0x12 : Standard GPS Report + UTC Date • n=0x13 : Standard GPS Report + UTC Date + RF data • n=0xD0 : Xora reports. • n=0xE0 : GGA and VTG NMEA reports • n=0xE1 : GGA, VTG and RMC NMEA reports • n=0xF0 : TAIP reports • n=0xF1 : Compact TAIP data
SNF Enable	Store and Forward will cause GPS reports to be stored up if the AirLink Device goes out of network coverage. Once the vehicle is in coverage the GPS reports will be sent en masse to the server. • n=0 : Disabled • n=1 : Enabled (default)

Table 9-1: GPS: Server 1

Command	Description
Use Device ID in Location Reports	Whether or not the AirLink Device should include the 64-bit device ID in its GPS reports. *PPDEVID MUST be 1 if the device uses a Dynamic IP. n=0 : Disable ID. n=1 : Enable/display ID.
SNF Reliable Mode	Store and Forward Reliability: GPS reports will be retransmitted if not acknowledged by the server. • n=0 : Disabled • n=1 : Reliable mode enabled for RAP messages • n=2 : Simple reliable mode
SNF Mode	Store and Forward Behavior. When *PPSNF=1, the type of Store and Forward behavior is defined by: • n=0 : Normal Store and Forward. Data is stored when the AirLink Device is out of cellular coverage; when the AirLink Device is in coverage, data is sent to server as soon as possible. This is the default form AirLink Device devices with RAP version 1.3 or lower. • n=1 : Data sent only when polled. Data is stored until polled using the Poll command sent by a server. • n=2 : Grouped Reports. Data is stored until the desired minimum number of reports (see *PPSNFM) has been stored. The data is then sent to the server in groups with at least the specified number of reports.
SNF Minimum Reports	Store and Forward Minimum Reports. Specifies the minimum number of reports that must be stored before they are forwarded to the server. The data is then sent to the server in packets that contain at least this number of reports. • n=0-255
SNF Simple Reliable Max. Retries	Maximum number retries when in Simple Reliable Mode. • n=0 : Disabled • n=1-255 retries

Server 2 to Server 4

There are additional servers where GPS data can be sent simultaneous to server 1.

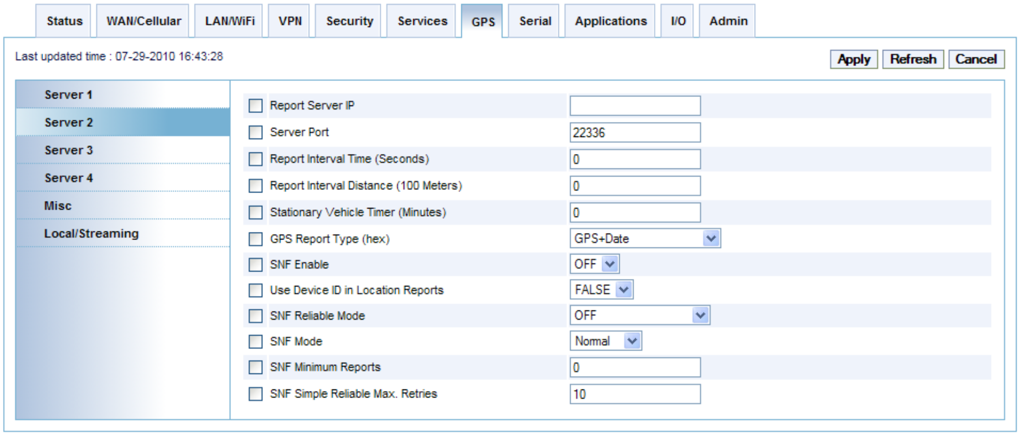


Figure 9-2: ACEmanager: GPS - Server 2

Command	Description
Report Server IP	IP address where GPS reports are sent (ATS Server IP). Also see *PPPORT. • d.d.d.d=IP address Example: AT*PPIP=192.100.100.100
Server Port	Port where GPS reports are sent. • n=1-65535
Report Interval Time	GPS Report Time Interval. See also *PPMINTIME, *PPTSV, +CTA. n=seconds (1 - 65535) *Note: Your cellular carrier may impose a minimum transmit time.* **Caution:** *A report time of less than 30 seconds can possibly keep an RF link up continuously. This will eventually cause the AirLink Device to overheat and shutdown. An RF resource may continue be tied up to transfer small amounts of data. Generally the RF channel will be released and go dormant in 10-20 seconds of no data sent or received.*
Report Interval Distance	GPS Report Distance Interval in 100 Meter Units (kilometer). 1 mile is approximately 1600 kilometers. • n=0 : Disabled • n=1-65535

Command	Description
Stationary Vehicle Timer (Minutes)	Timer for Stationary Vehicles. Time interval in minutes that the AirLink Device device will send in reports when it is stationary. • n=0 : Disabled • n=1-255 minutes For example, if *PPTIME=10, the AirLink Device will send in reports at least every 10 seconds while it is moving; however, once it stops moving, it will slow the reports down to this *PPTSV value. *Note: In order for the PPTSV (Stationary Vehicle timer) to take effect, the PPTIME value must be set to a value greater than 0 and less than the PPTSV value. The PPTSV timer checks for vehicle movement at the PPTIME interval, so if PPTIME is disabled, then PPTSV will also be disabled.*
GPS Report Type (hex)	GPS report type. • n=0 : Use legacy reports specified in *MF value. Note: Must also have *PPDEVID=0. • n=0x11 : Standard GPS Report • n=0x12 : Standard GPS Report + UTC Date • n=0x13 : Standard GPS Report + UTC Date + RF data • n=0xD0 : Xora reports. • n=0xE0 : GGA and VTG NMEA reports • n=0xE1 : GGA, VTG and RMC NMEA reports • n=0xF0 : TAIP reports • n=0xF1 : Compact TAIP data
SNF Enable	Store and Forward will cause GPS reports to be stored up if the AirLink Device goes out of network coverage. Once the vehicle is in coverage the GPS reports will be sent en masse to the server. • n=0 : Disabled • n=1 : Enabled (default)
Use Device ID in Location Reports	Whether or not the AirLink Device should include the 64-bit device ID in its GPS reports. *PPDEVID MUST be 1 if the device uses a Dynamic IP. • n=0 : Disable ID • n=1 : Enable/display ID
SNF Reliable Mode	Store and Forward Reliability: GPS reports will be retransmitted if not acknowledged by the server. • n=0 : Disabled • n=1 : Reliable mode enabled for RAP messages • n=2 : Simple reliable mode

Command	Description
SNF Mode	Store and Forward Behavior. When *PPSNF=1, the type of Store and Forward behavior is defined by: • n=0 : Normal Store and Forward. Data is stored when the AirLink Device is out of cellular coverage; when the AirLink Device is in coverage, data is sent to server as soon as possible. This is the default form AirLink Device devices with RAP version 1.3 or lower. • n=1 : Data sent only when polled. Data is stored until polled using the Poll command sent by a server. • n=2 : Grouped Reports. Data is stored until the desired minimum number of reports (see *PPSNFM) has been stored. The data is then sent to the server in groups with at least the specified number of reports.
SNF Minimum Reports	Store and Forward Minimum Reports. Specifies the minimum number of reports that must be stored before they are forwarded to the server. The data is then sent to the server in packets that contain at least this number of reports. • n=0-255
SNF Simple Reliable Max. Retries	Maximum number retries when in Simple Reliable Mode. • n=0 : Disabled • n=1-255 retries

Misc

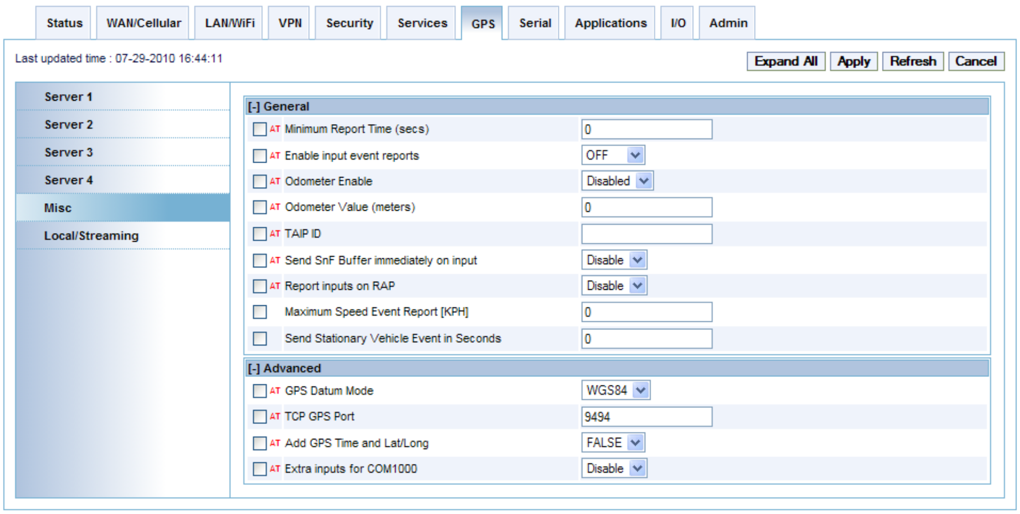


Figure 9-3: ACEmanager: GPS - Misc

Table 9-2: GPS: Misc

Command	Description
Enable input event reports	Enable sending input changes as events (different report types). • n=0 : Disable • n=1 : Enable
Odometer Enable	Enable odometer reporting. • n=0 : Disabled (default) • n=1 : Enabled
Odometer Value (meters)	The current odometer value of the AirLink Device. The value is in meters. Maximum value is approximately 4.3 billion meters (2.5 million miles). 1 mile is approximately 1600 meters. • n=meters
TAIP ID	Sets/queries the TAIP ID. This ID is returned in TAIP reports if it has been negotiated with the TAIP client. This value is only used in conjunction with TAIP emulation mode (*PPGPSR=F0). • nnnn=TAIP ID (4 characters)
Send SNF Buffer imeediately on input	Flushes store and forward buffer when an input event (DTR/RTS) occurs. • n=0 : Disable • n=1 : Enable

Table 9-2: GPS: Misc

Command	Description
***PPREPORTINPUTSR eport inputs on RAP**	Enable input reporting. • n=0 : Disabled • n=1 : Enabled *Note: If both AT*PPCOM1000=1 and AT*PPREPORTINPUTS=1 are enabled, the AirLink Device digital inputs will be reported and the COM1000 inputs will be ignored.*
GPS Datum Mode	Specifies the GPS datum to use for position reports. For accurate results, this value should match the datum used by receiving mapping application. • n=0 : WGS84 • n=92 : NAD27 • n=115 : NAD83
***PPTCPPOLLTCP GPS Port**	Specifies the port to listen on for TCP GPS report polling. The request to this port needs to come from the same IP address in *PPIP. • n=0 : Disabled • n=1-65535 (default 9494)
Add GPS Time and Lat/Long	Set or query GPS stamping of UDP Reliable packets. When set, data received on the host serial port will be encapsulated with the GPS date and time. • n=0 : Disabled (default) • n=1 : Enabled
Extra inputs for COM1000	Enables support for extra inputs from a COM1000. • n=0 : Disable • n=1 : Enable **Tip:** *If both AT*PPCOM1000=1 and AT*PPREPORTINPUTS=1 are enabled, the AirLink Device device's digital inputs will be reported and the COM1000 inputs will be ignored.*

Local/Streaming

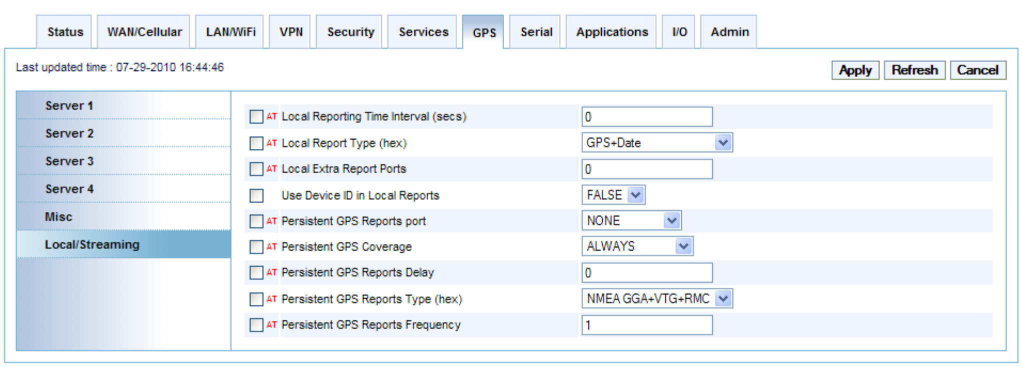


Figure 9-4: ACEmanager: GPS - Local streaming

Command	Description
Local Reporting Time Interval	Local ATS - Causes GPS reports to also be sent out the serial or Ethernet link every n seconds, when there is a PPP connection to the serial host or a connection to the Ethernet port is established. • Disable • 1-255 seconds **Tip:** *Sends to the PPP peer IP S110 with the Destination Port number S53.*
Local Report Type	Indicates the type of GPS report to send to the local client (PPP/SLIP peer). See *PPGPSR. • n=0x11 : Standard GPS Report • n=0x12 : Standard GPS Report + UTC Date • n=0x13 : Standard GPS Report + UTC Date + RF data • n=0xD0 : Xora reports. • n=0xE0 : GGA and VTG NMEA reports • n=0xE1 : GGA, VTG and RMC NMEA reports • n=0xF0 : TAIP reports • n=0xF1 : Compact TAIP data
Local Extra Report Ports	Have local ATS reporting (LATS) send up to 7 extra copies of a GPS report to the subsequent ports. • Just the original report is sent (default). • Send GPS report copies to that number of ports. Example: If AT*PPLATSEXTRA=7 and the port in S53 is 1000, then GPS reports will be sent to ports 1000-1008.
Use Device ID in Local Reports	Use Device ID in Local Reports.
Persistent GPS Reports port	Send NMEA GPS strings out serial link. Similar to ATGPS except that the *PGPS value can be saved to NVRAM so that it will continue to operate after resets. • Disabled • Send NMEA GPS strings out serial link. • Send NMEA GPS strings out the USB port. • Send NMEA GPS strings out both the serial and the USB port.
Persistent GPS Coverage	Allows a PP to be configured to send GPS sentences out of the serial port when the PP loses cellular coverage. This feature is configured by 2 fields. This command controls the status of the sentences. • Always sent • Sent when out of cellular coverage When set to 1, no reports are saved in SnF.

Command	Description
Persistent GPS Repory Delay	PGPSD is a 16-bit value that is the number of seconds to wait when "Out of Coverage" occurs before switching to, sending the messages out the serial port and not into SnF. • Any messages put into SnF during this switchover delay period will be sent OTA, when coverage is re-acquired. *Note: The two persistent GPS report parameters, *PGPSR and *PGPSF, will control the report type and frequency of the messages sent out the serial port, when out of coverage.*
Persistent GPS Report type	Persistent GPS Report type to send via the serial link
Persistent GPS Reports Frequency	Persistant GPS frequency • n= number of seconds per report Max Value: 65535 up to 18 hours

10: Serial Configuration

The Serial tab that displays in ACEmanager, is applicable to all AirLink devices with a serial port.

Most AirLink devices are equipped with a serial port. This port can be used to connect devices or computers using a DB9-RS232 connection.

Note: These commands are specific to the RS232 port and generally do not apply to the USB/serial.

Port Configuration

The Serial group includes commands specific to general use of the serial port.

The Port Configuration has four categories of configurable parameters:

- Port Configuration
- Advanced
- TCP
- UDP

The figure on next page displays the screen.

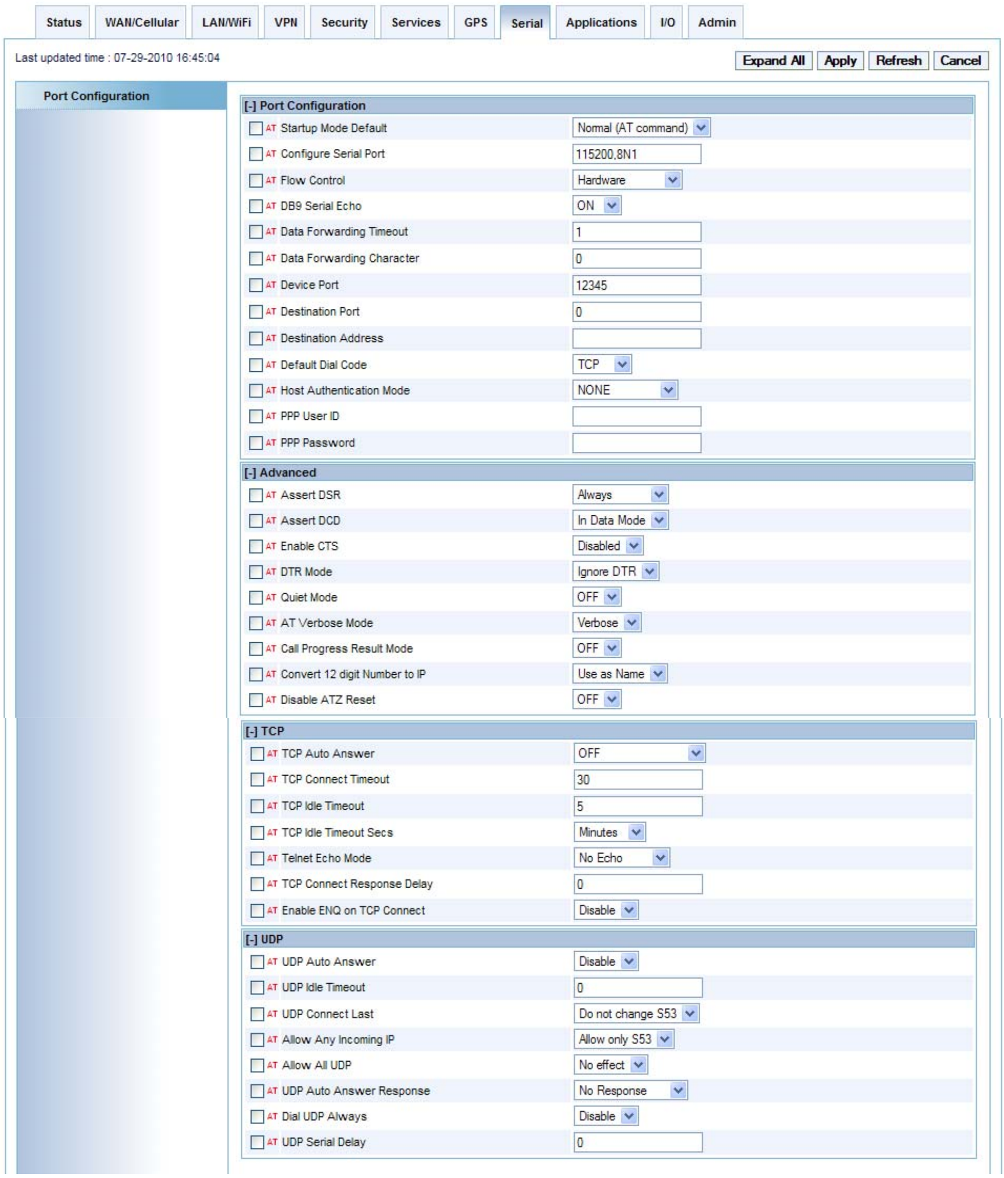


Figure 10-1: ACEmanager: Serial - Port Configuration

Table 10-1: Serial Port

Command	Description
Startup Mode Default	Default power-up mode for the serial port: When the AirLink device is power-cycled, the serial port enters the mode specified by this command after 5 seconds. On startup, typing ATMD0 into a terminal application connected to the serial port within 5 seconds changes the mode to normal (AT command) mode. See also S53 to set the port for UDP . • SLIP • PPP • UDP • TCP • PassThru • DM mode • PinPoint MDT • Reliable UDP • UDP Multicast
Configure Serial Port	Format: [speed],[data bits][parity][stop bits] Valid speeds are 300-115200, data bits: 7 or 8, parity: O,E,N,M, stop bits: 1,1.5,2
Flow Control	Serial port flow control setting. • No flow control is being used. • RTS/CTS hardware flow control is being used. • Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@.
DB9 Serial Echo	Toggle AT command echo mode. • Echo Off. • Echo On. With more than one connection types (serial, and Telnet, and USB/Serial) the echo command is set differently on each interface.
Data Forwarding Timeout	Data forwarding idle time-out. If set to 0, a forwarding time-out of 10ms is used. Used in UDP or TCP PAD mode. • tenths of a second
Data Forwarding Character	PAD data forwarding character. ASCII code of character that will cause data to be forwarded. Used in UDP or TCP PAD mode. No forwarding character.
Device Port	Default Destination Port to send TCP/UDP communications to
Destination Port	Default Destination Port to send TCP/UDP communications to.
Destination Address	IP address to send TCP/UDP communication to.
Default Dial Code	Default Dial Data Mode.
Assert DSR	Assert DSR always, or when the device is in a data mode (UDP, TCP, etc.) or when the device is in network coverage.

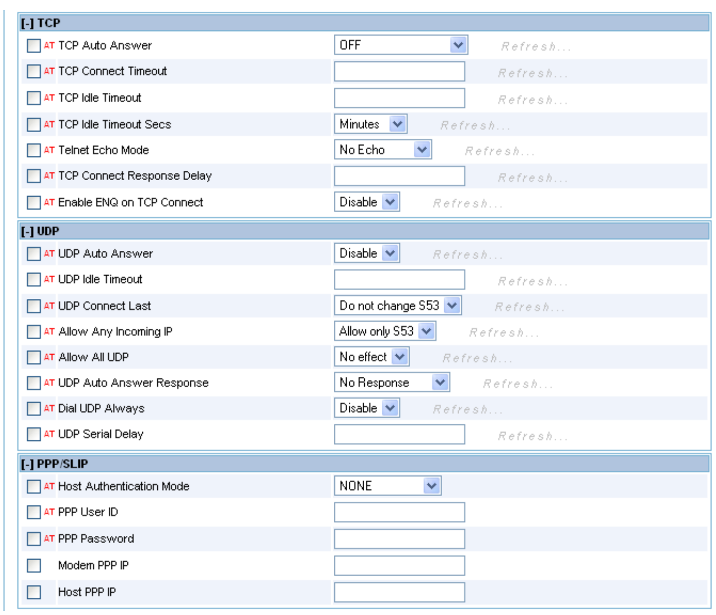
Table 10-1: Serial Port

Command	Description
Assert DCD	Assert DCD always, or when the device is in a data mode (UDP, TCP, etc.) or when the device is in network coverage.
Enable CTS	Assert CTS when there is network coverage.
DTR Mode	Use DTR from serial device, or ignore DTR. (Same as S211).
Quiet Mode	Disable or enable display of device responses.
AT Verbose Mode	Configure AT command responses.
Call Progress Result Mode	When enabled adds 19200 to CONNECT messages.
Convert 12 digit Number to IP	Converts 12 digit number to an IP address 111222333444 -> 111.222.333.444.
DATZ	When ON, +++ ATZ will NOT reset the device.

Raven Line devices

If you are connected to a Raven line device, in addition to the fields above, more sections will appear on the Serial Port Configuration page. The additional sections are as follows:

- TCP
- UDP
- PPP/SLIP
- PASS THRU
- TELEMETRY- MODBUS



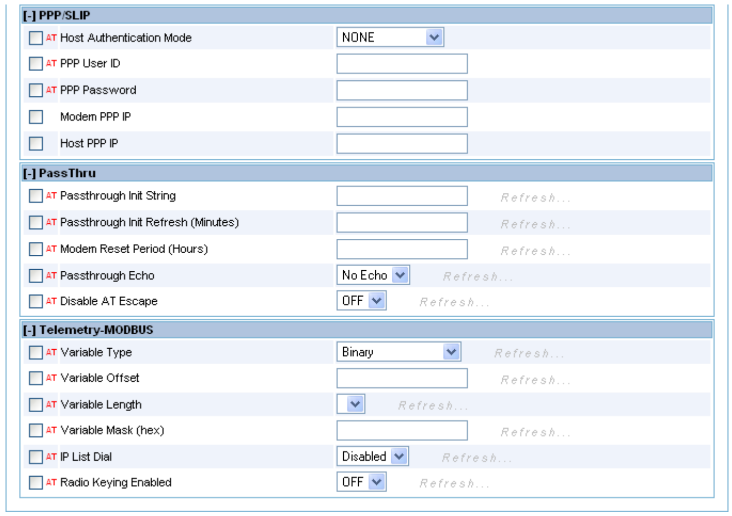


Figure 10-2: ACEmanager: Serial - Port Configuration (Raven line devices only)

Command	Description
TCP Auto Answer	This register determines how the MP device responds to an incoming TCP connection request. The MP device remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the MP device must be set for a successful TCP connection. The MP device will send a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgement of the connection request and the TCP session is established. • n=0 : Off (Default). • n=1 : On. • n=2 : Use Telnet server mode on TCP connections. • n=3 : With a Telnet connection, overrides the client's default echo, allowing the server on the host port to perform the echo. CRLF sequences from the telnet client will also be edited to simply pass CRs to the server on the host port.
TCP Connect Timeout	Specifies the number of seconds to wait for a TCP connection to be established when dialing out.
TCP Idle Timeout	Interval to terminate a TCP connection when no in or outbound traffic. This value affects only the TCP connection in TCP PAD mode. • n=interval
TCP Idle Timeout Secs	TCP connection time-out (TCPS) units. Specifies a time interval upon which if there is no in or outbound traffic through a TCP connection, the connection will be terminated. • n=0 : minutes
TCP Connect Response Delay	Connect Delay: Number of seconds to delay the “CONNECT' response upon establishing a TCP connection. OR Number of tenths of seconds to delay before outputting ENQ on the serial port after the CONNECT when the ENQ feature is enabled. • n=0 - 255

Command	Description
Telnet Echo Mode	Telnet Client Echo Mode. • n=0 : No Echo • n=1 : Local Echo (Default) • n=2 : Remote Echo
Enable ENQ on TCP Connect	Outputs an ENQ [0x05] after the TCP CONNECT delayed by the Delay Connect Response time (S221). • n=0 : Disabled (Default). • n=1 : Enable ENQ on CONNECT.

Command	Description
MD	Default power-up mode for the serial port: When the MP device is power-cycled, the serial port enters the mode specified by this command after 5 seconds. On startup, typing ATMD0 within 5 seconds changes the mode to normal (AT command) mode. See also S53 to set the port for UDP . • hh (hex byte)=00 : normal • hh=01 : SLIP • hh=02 : PPP • hh=03 : UDP • hh=04 : TCP • hh=07 : PassThru • hh=0F : MP MDT • hh=13 : Modbus ASCII • hh=23 : Modbus RTU (Binary) • hh=33 : BSAP • hh=63 : Variable Modbus • hh=73 : Reliable UDP • hh=83 : UDP Multicast
UDP Auto Answer	Enables UDP auto answer (half-open) mode. • n=0 : Normal mode • n=2 : Enable UDP auto answer mode.
UDP Idle Timeout	Set or query UDP auto answer idle time-out. If no data is sent or received before the time-out occurs, the current UDP session will be terminated. While a session is active, packets from other IP addresses will be discarded (unless *UALL is set). • n=0 : No idle time-out (Default). • n=1 - 255 : Time-out in seconds.
UDP Connect Last	If enabled, sets S53 to the last accepted IP address through UDP auto answer. This can be used in conjunction with MD3 so that when there is no UDP session, new ethernet host data will cause a connection to be restored to the last IP accepted through UDP auto answer. • n=0 : Does not change S53 setting. (Default). • n=1 : Set S53 to the last accepted IP.

Command	Description
Allow Any Incoming IP	Allow IP address. • n=0 : Allow only the IP address specified in S53 to connect when UDP auto answer is enabled (S82=2). • n=1 : Allow any incoming IP address to connect when UDP auto answer is enabled (S82=2). Always subject to any Friends filters that may be defined.
Allow All UDP	Accepts UDP packets from any IP address when a UDP session is active. If there is no UDP session active, an incoming UDP packet will be treated according to the UDP auto answer and AIP settings. • n=0 : No effect (Default). • n=1 : Accept UDP data from all IP addresses when in a UDP session.
UDP Auto Answer Response	Half-Open Response - In UDP auto answer (half-open) mode. • n=0 : No response codes when UDP session is initiated. • n=1 : RING CONNECT response codes sent out serial link before the data from the first UDP packet. *Note: Quiet Mode must be Off.*
Dial UDP Always	The dial command always uses UDP, even when using ATDT. • n=0 : Dial using the means specified (default). • n=1 : Dial UDP always, even when using ATDT. *Note: When this parameter is set you cannot establish a TCP PAD connection.*
UDP Serial Delay	Waits the specified delay before sending the first UDP packet and the subsequent UDP packets out to the port Ethernet. • n=0 : No UDP packet delay (Default). • n=1 - 255 : Delay in 100ms units, from 100 ms to 25.5 sec.

Command	Description
Host Authentication Mode	Host Authentication Mode: Use PAP or CHAP to request the user login and password during PPP or CHAP negotiation on the host connection. The username and password set in *HOSTUID and *HOSTPW will be used. • Disable PAP or CHAP request (Default) • PAP and CHAP • CHAP
PPP User ID	Host User ID for PAP or CHAP. • user id (up to 64 bytes)
PPP Password	Host Password for PAP or CHAP.

Command	Description
device PPP IP	The IP for the AirLink device when comming through RS232.
Host PPP IP	The IP for the Host RS232 Interface.

Command	Description
Passthrough Init String	Any AT Command string to be passed to the OEM module before entering PASSTHRU mode, e.g. AT&S1V1, etc. • string=AT command(s)
Passthrough Init Refresh (Minutes)	Number of minutes of inactivity in PASSTHRU mode to resend the *PTINIT string to the hardware module. • n=0 : Disabled • n=1-255 minutes
device Reset Period (Hours)	In PASSTHRU mode, device will be reset after this period if no data has been sent or received. Value is in hours. • n=0 : Disabled • n=1-255 hours
Passthrough Echo	PassThru Echo : Echo data to the host. • n=0 : Data will be passed to the host. • n=1 : PASSTHRU mode will echo all host received data and will not pass the data to the device while the device is not asserting DCD. *Note: If the device is asserting DCD, data will be passed from the host to the device as it normally is when *CSX1=0.*
Disable AT Escape	AT Escape Sequence detection. • n=0 : Enable • n=1 : Disable

Command	Description
Variable Type	The data-type of the RTU ID in a modbus-variant protocol. This parameter is used to define the data-type of the RTU ID in Modbus-like protocol data packets. This parameter is used when the Mode Default (MD) is set to 63.
Variable Offset	Indicates the offset in the data of where the Modbus ID starts.
Variable Length	Length of the RTU ID in a modbus-variant protocol, in bytes. This parameter is used to define the length of the RTU ID in Modbus-like protocol data packets. This parameter is used when the when the Mode Default (MD) is set to hex 63

Command	Description
Variable Mask (hex)	16 bit hex mask to use when extracting the ID. Specify which bits in the ID field to use. This parameter is used when the when the Mode Default (MD) is set to : • hex 63 hh = 00-FFFF hex value • hh = 00 [default] no mask • use all 16 bits hh = 0F • use only the low order 4 bits
IP List Dial	This allows access the Modbus IP list using the first two digits of the dial string. Example: ATDT1234567 would go to ID "12" on the Modbus list and use the associated IP as the destination.
Radio Keying Enabled	Enable/disable MDS Radio transceiver keying. Radio keying is designed to assert CTS when a packet is received with following options: • Delay the time as specified • Send the data out the serial port • Wait the same amount time • Drop CTS This way, the CTS signal can be used to key a transmitter on and give it time to reach its power level before data is sent to it. Delay interval is specified in AT command S221.

MODBUS Address List

This tab will only display in Raven line devices.

To add an Adress Entry, click on Add More.

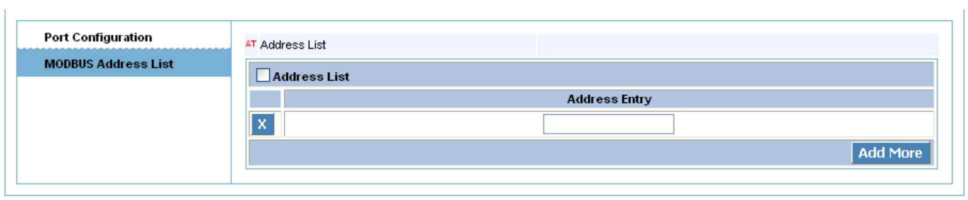


Figure 10-3: ACEmanager: MODBUS Address List

11: Application Configuration

The Application tab that displays in ACEmanager, is applicable to PinPoint X and PinPoint XT AirLink devices.

Garmin provides navigation devices for versatile fleet monitoring solutions. AirLink devices provides an internet access to Garmin devices and a mechanism to enable via cellular. ALEOS also monitors links to the Garmin and communication between the Garmin and the server.

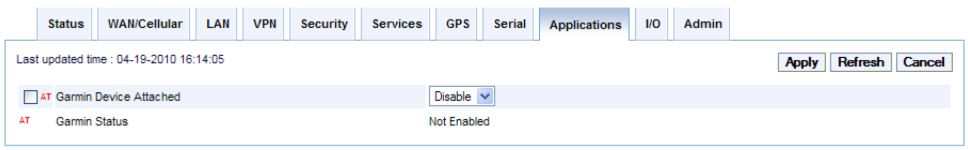


Figure 11-1: ACEmanager: Applications

To configure in ACEmanager, Set HostMode to TCP mode:

1. Under the **Serial – Port Configuration** tab, set the MD, the Startup Mode Default, parameter, to the TCP pad mode.

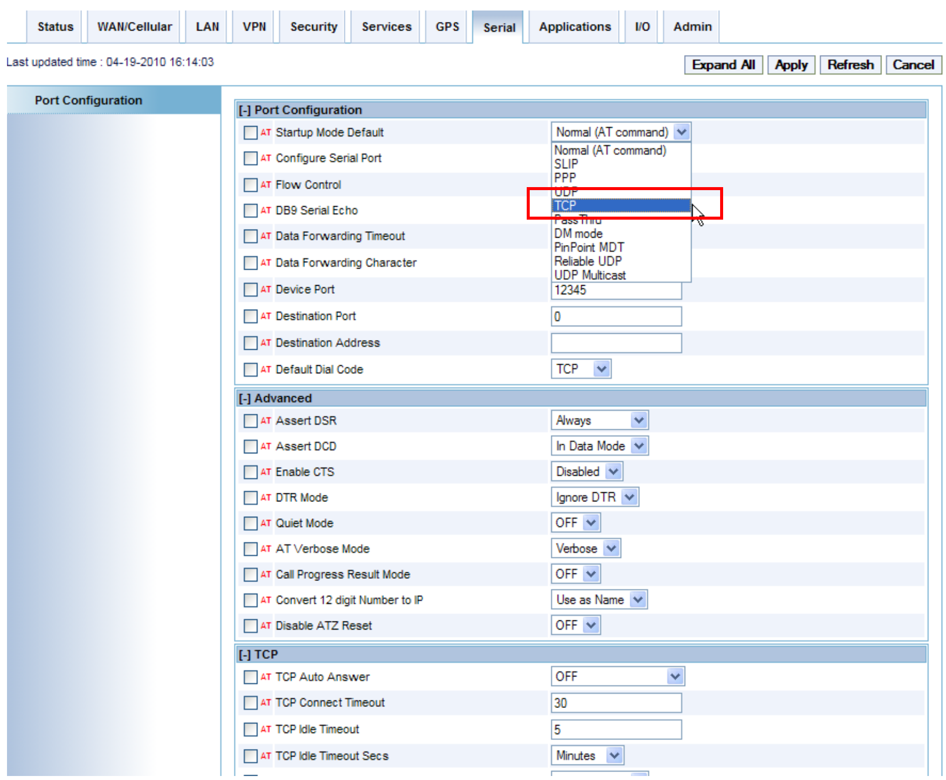


Figure 11-2: ACEmanager: Serial - Port Configuration

2. Set the Server Address and Port for TCP. Under **Serial – Port Configuration** tab, the Destination Address and Destination Port needs to be the address and port of the Server that the TCP application will communicating with.

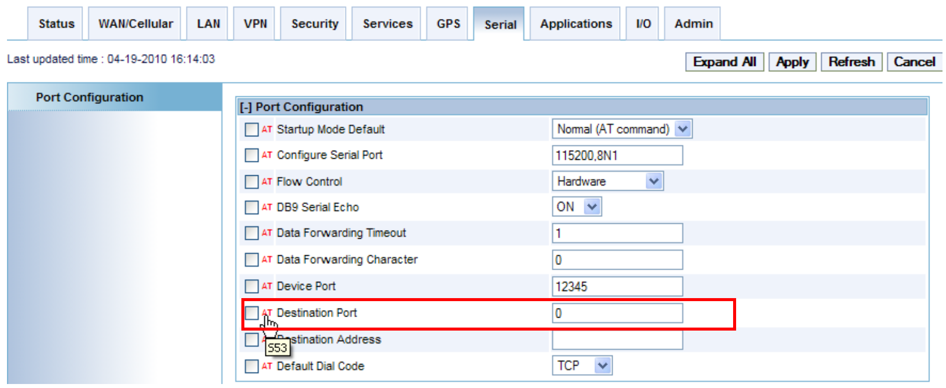


Figure 11-3: ACEmanager: Serial - Port Configuration

3. Configure the serial port. To communicate with Garmin, set it to **9600, 8n1** with **No Flow Control** and **DTR Mode = 0**

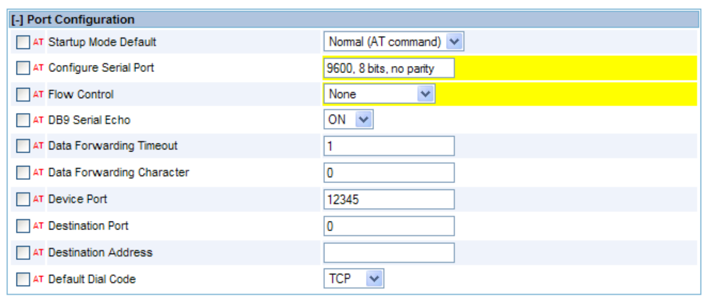


Figure 11-4: ACEmanager: Serial - Port Configuration parameters

4. Configure the Garmin Parameters. Under the **Applications** tab, set the Garmin Device Attached to 1 to enable talking to the Garmin.

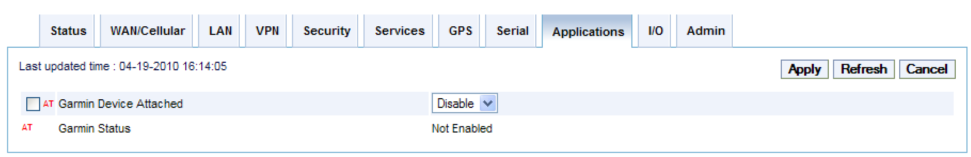


Figure 11-5: ACEmanager: Applications

After all the parameters have been set, reboot AirLink device and apply the changes.

- The “Garmin Device Attached” has the following states:
  - Enable
  - Disable

The Garmin Status field will display if the Garmin application is “Enabled” or “Not Enabled”.

12: Report Configuration

The Report tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink Raven Line devices only.

The report server is the main server where the Events Reports will be sent. It is the same as a RAP or “ATS” server. A primary server can be configured without a failover or redundant server which would be the same as a single server.

Since the Raven line devices have no GPS, it will not send RAP messages, but it will be able to send Events Reporting messages to that server in the same way a PinPoint or MP device would send RAP messages to a RAP or “ATS” server.

Reports Server

Reports using the Events Protocol are sent to the Reports Server.

Unlike RAP messages of the past which were limited to PinPoint line devices, the enhancements of Event Reporting allow the Raven devices to send reports to a remote server as well. The Reports Server would be running an application to parse the messages and send responses to the Raven devices.

Note: Whereas the PinPoint and MP line can use up to 4 different servers for GPS reports, the Raven line is limited to one.

Server 1

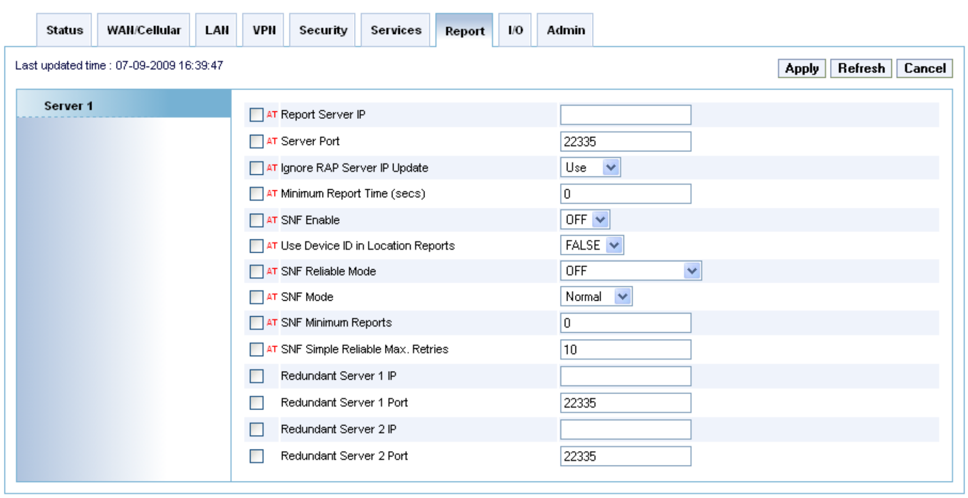


Figure 12-1: ACEmanager: Report - Server 1

Command	Description
Report Server IP	IP address where Event Reports are sent (RAP Server IP). Also see *PPPORT. • d.d.d.d=IP address Example: AT*PPIP=192.100.100.100
Server Port	Port where GPS reports are sent. • n=1-65535
Minimum Report Time (secs)	Report Time Interval. n=seconds (1 - 65535) *Note: Your cellular carrier may impose a minimum transmit time.* **Caution:** *A report time of less than 30 seconds can possibly keep an RF link up continuously. This could eventually cause the device to overheat and shutdown. An RF resource may continue be tied up to transfer small amounts of data. Generally the RF channel will be released and go dormant in 10-20 seconds of no data sent or received.*
SNF Enable	Store and Forward will cause GPS reports to be stored up if the device goes out of network coverage. Once the vehicle is in coverage the reports will be sent en masse to the server. • n=0 : Disabled • n=1 : Enabled (default)
Use IMEI for Device ID in Location Reports	Enabling this will force the use of the IMEI in the Device ID instead of the phone number.
Use Device ID in Location Reports	Whether or not the device should include the 64-bit device ID in its reports. The Device ID MUST be enabled if the device uses a Dynamic IP. n=0 : Disable ID. n=1 : Enable/display ID.
SNF Reliable Mode	Store and Forward Reliability: Reports will be retransmitted if not acknowledged by the server. • n=0 : Disabled • n=1 : Reliable mode enabled for RAP messages • n=2 : Simple reliable mode
SNF Mode	Store and Forward Behavior. When Store and forward is enabled, the type of Store and Forward behavior is defined by: • n=0 : Normal Store and Forward. Data is stored when the MP is out of cellular coverage; when the MP is in coverage, data is sent to server as soon as possible. This is the default form MP devices with RAP version 1.3 or lower. • n=1 : Data sent only when polled. Data is stored until polled using the Poll command sent by a server. • n=2 : Grouped Reports. Data is stored until the desired minimum number of reports (see *PPSNFM) has been stored. The data is then sent to the server in groups with at least the specified number of reports.

Command	Description
SNF Minimum Reports	Store and Forward Minimum Reports. Specifies the minimum number of reports that must be stored before they are forwarded to the server. The data is then sent to the server in packets that contain at least this number of reports. • n=0-255
SNF Simple Reliable Max. Retries	Maximum number retries when in Simple Reliable Mode. • n=0 : Disabled • n=1-255 retries
Redundant Server 1 IP and Redundant Server 2 IP	Send duplicate unreliable report to this Server.
Redundant Server 1 Port and Redundant Server 2 Port	Send duplicate unreliable report to this port.

Redundant Server

When a redundant server is enabled, each time a message is sent out to the main, or failover, a second identical message will be sent to the redundant server. This can allow the data to be used by two or more different applications.

The redundant servers can be running the same or different application than the primary and failover servers. The messages to the redundant server are independent of the primary/failover server settings or state.

You can set one or both redundant servers. The messages are sent independently to either or both.

Note: Messages will be sent regardless if the server is available or not and do not use any reliable mode format. Receipt of a message is not acknowledged nor is any message resent. Currently, redundant servers cannot use TCP.

Store and Forward

Store and Forward will store reports when the primary Reports Server is unavailable and forwards them when the server is available again. Store and Forward can also groupmultiple reports in to a single message, rather than individually.

The Report Server could be unavailable because the AirLink device leaves coverage, has very low signal (an RSSI of -105 or lower), or the server is unreachable, regardless will store reports in memory. When the AirLink device is able to reach the server again, it will forward the reports.

The AirLink device can also store messages and send them to the server in a packet or only when the messages are requested rather than individually to conserve bandwidth.

Reliability Modes

Reliability Modes provide methods for the AirLink device and receive an acknowledgement from the Reports Server to determine if a sent message was received.

- **Reliable Mode** - The AirLink device will transmit a sequence number (1 to 127) as part of a packet of messages that may contain one or more reports. To reduce overhead, the server only acknowledges receipt of every eighth packet. The AirLink device considers the eight packets a “window” of outstanding packets.

  If the AirLink device doesn’t receive acknowledgement for a “window”, the device will PING the server with a message containing the sequence numbers of the first and last packets that haven’t been acknowledged. The AirLink device will continue until the server acknowledges receipt. When the AirLink device receives the acknowledgement, it will advance its “window” to the next group. When the AirLink device is first powered on (or reset), it will send a Set Window message to sync up with the server for the current “window”.

  On the other side, if the server receives an out of sequence packet, it will send a message to the device noting the missing sequence and the AirLink device will retransmit.
- **Simple Reliable Mode** - The AirLink device will ‘give up’ after a configured number, **PPMAXRETRIES*, of attempts and discard messages that cannot be transmitted or received after that number of tries.

  The acknowledgement message is the ASCII string “UDPACK” followed by the sequence number.
- **UDP Sequence Reliable** - A sequence number is prepended to the report packet in a range of 0c30 to 0x7f inclusive. The sequence number is ASCII readable, allowing test tools to acknowledge the packets.

  The acknowledgement message is the ASCII string “SEQACK” followed by the sequence number.

  The sequence number is not stored and will be reinitialized to 0x30 when the AirLink device is reset or power cycled. If a message packet is not acknowledged within the specified number of retries, the packet and its contents will be dropped.
- **TCP Sequence Reliable** - The same as UDP Sequence Reliable but using TCP instead of UDP.
- **TCP Listen Reliable** - TCP Listen reliable is same as TCP Sequence Reliable except the Reports Server must initiate the connection before the AirLink device will send reports. This allows servers to by-pass some firewalls.

13: I/O Configuration

- Current State
- Configuration

The I/O tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices, which feature I/O ports.

This group includes configuration commands for the digital and analog inputs and relay and digital outputs as applicable to a specific device. Some of the values shown as a part of this group are not changeable but reflect the current status. Only those devices with available inputs and outputs will display this group.

Please refer to the Hardware Users Guide, in the Inputs, Relay Outputs, and Power Status chapter, for more information on the basic features of the I/O settings.

Note: The I/O configuration options and displayed status of the I/O depends on the AirLink device.

Current State

The current state screen will show the current values for the available inputs as well as the current values for pulse counts (digital) and transformed analog. The current state of the Relay or Digital Output is displayed and can be changed directly.

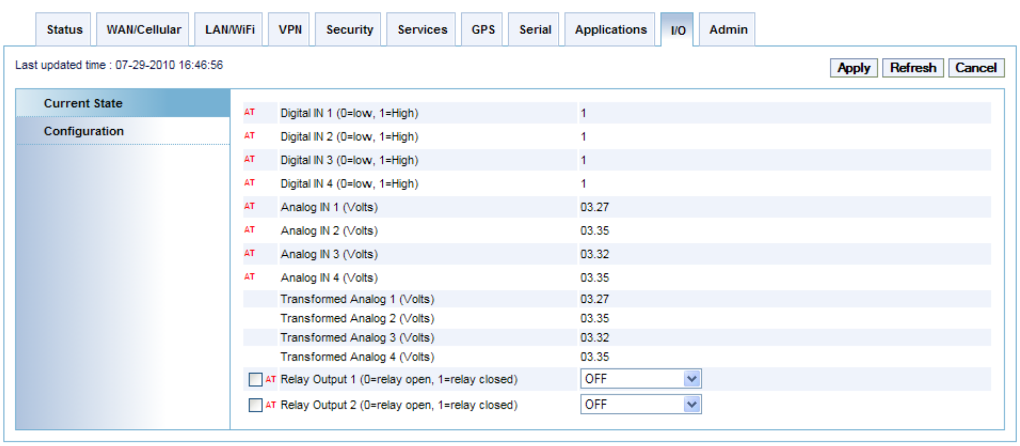


Figure 13-1: ACEmanager: I/0 - Current state

Table 13-1: I/O

Command	Description
Digital IN #	Query individual digital inputs. The digital inputs report either a 0 (open) or 1 (closed). • n=1-4 Input number
Pulse Count	On devices with a digital input that can be configured for use as a digital output, the pulse counts will also reflect output changes.
***ANALOGIN #**	Query individual analog inputs. The analog inputs report the voltage in volts. • n=1-4 Input number
Transformed Analog #	Trasnformed Analog is derived from your coefficient and raw analog. For example, if your Analog In1 is 2 and Coefficient is 4, with an Offset setting of 2 (definition as below), the Transformed Analog will be 10.
Relay Output #	Set or query the relay outputs. • n=1-2 Input number • s=OPEN or CLOSED

Configuration

To enhance the usability of the I/O, the configuration will allow you to set an initial value for the output relays and a coefficient, offset, and unit label for the analog in.

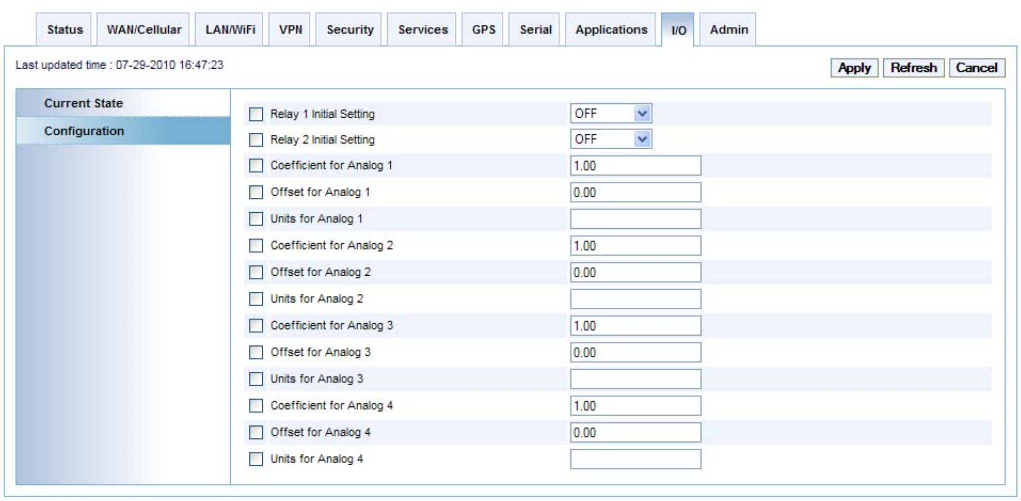


Figure 13-2: ACEmanager: IO - Configuration

Command	Description
Relay # Initial Setting	When the AirLink device reboots, the relay settings you want can be configured here. Relay setting can be: • ON • OFF • Last Value
Coefficient for Analog #	Coefficient is the multiplier for raw analogs (*ANALOGIN).
Offset for Analog #	Point at which Transformed Analog starts its count.
Units for Analog #	This is the label for the Analog measurement. For example, litres or mm etc.

Pulse Count

Following are some Pulse Count details:

- Pulses are counted on each of the digital inputs.
- Pulse counts 1-4 corresponds to digital 1-4 respectively.
- Pulses are counted on the falling edge.
- Pulses can not be counted when the device is powered off, or being reset. However, a single state change while off or reset will be properly counted.

Transformed Analog

The number for the available transformed needs to indicate a variable based on the number of Analog.

The analog input value is transformed into a meaningful value, such as weight or pressure, by multiplying the raw value from the input by the coefficient and adding the offset.

- **Coefficient for Analog 1-4** - The amount by which the raw analog value should be multiplied.
- **Offset for Analog 1-4** - The offset to be added to the product of the coefficient and the raw analog value.
- **Transformed Analog 1-4** - The value of the raw analog value multiplied by the coefficient and then added to the offset.
- **Units for Analog 1-4** - The name of the unit of measurement to be used in reports.

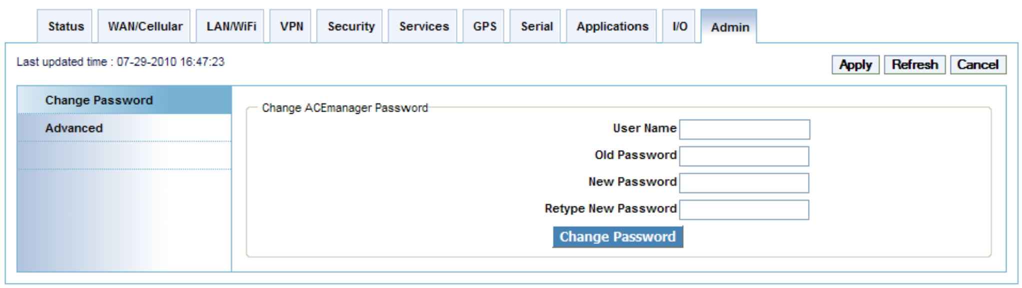
14: Admin

The Admin tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

The Admin section contains features which are intended for Administrator configuration only.

Change Password

It is highly recommended to change the default password of the AirLink Device.



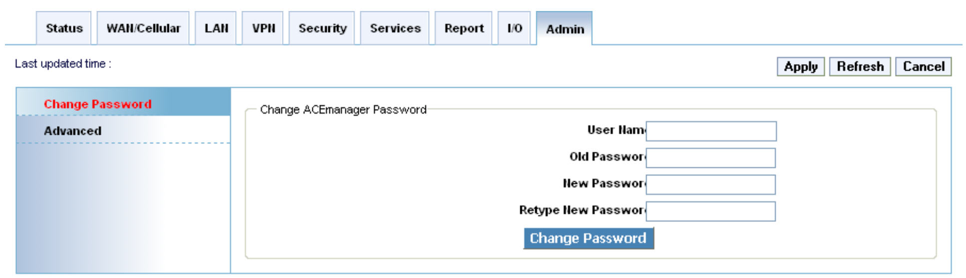


Figure 14-1: ACEmanager: Admin

To change the default password,

1. Enter the user name (admin).
2. Enter the old password.
3. Enter the new password twice.
4. Click on Change Password

You will be prompted to restart the AirLink Device. When the box has restarted, reconnect to ACEmanager and enter the new password.

Advanced

Features which should be rarely changed and will affect the operation of the device are present on this screen.

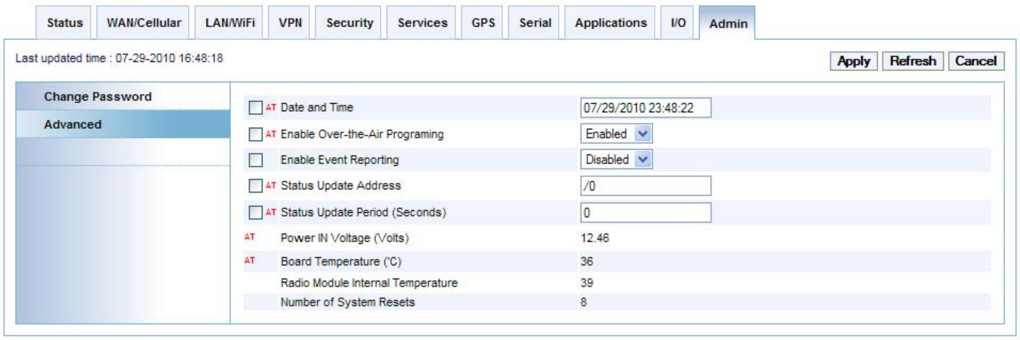


Figure 14-2: ACEmanager: Admin - Default

Command	Description
Date and Time	Sets and queries the internal clock. Either the date and time can be specified, or simply one of the two can be specified in which case the unspecified value will remain unchanged. The date and time are always specified 24 hour notation. • mm/dd/yyyy=date in month/day/year notation • hh:mm:ss=time in 24 hour notation - The time noted by this setting will be changed by the GPS or SNTP as applicable.
Enable Event Reporting	Enable or disable Event Reporting. If you choose to enable, click on Refresh all. • n=0 : Disables • n=1 : Enables
Status Update Address	Device Status Update Address where Name/Port is the domain name and port of the machine where the device status updates will be sent. The status parameters are sent in an XML format. • name=domain name • port=port
Radio Module Internal Temperature	The temperature of the internal radio module.
Number of System Resets	Counter of the number of system resets over the life of the device or since the configuration was reset.

15: Events Reporting Configuration

15

The Events Reporting tab that displays in ACEmanager, is applicable across all Sierra Wireless AirLink devices.

Events Reporting allows the users to generate reports from the events that take place. Event Reporting Protocol is an intuitive embedded protocol, which automatically formats the messages based on an event trigger. The messages generated are then reported to the remote server.

An event occurs, when any of the following takes place:

- Customer device opens or closes a switch
- Customer device raises or lowers analog voltage
- device RSSI goes below or above a threshold
- device power goes below or above a threshold.

A report is generated when the device sends a message caused by an event.

Both events and reports are configured by the customer and can be considered as the “next Generation” of RAP.

The Events groups define the triggers for reports.

Event Trigger

There are 16 data types that can trigger events. The configuration for the trigger will vary based on the data type. An “event” is when the data in the configured state. Some examples are: a switch is closed, the speed is greater than 70 MPH, the engine has been used for 1000 hours and needs maintenance.

Data Type	Configuration Type
Digital Input 1-4	Switch
Pulse Accumulator 1-4	Delta
Analog Input 1-4	Threshold
Scaled Analog 1-4	Threshold
GPS Fix	GPS Fix
Vehicle Speed	Threshold
Heading Change	Delta – zero based
Engine Hours	Delta
RSSI	Threshold
Network State	Network State
Network Service	Network Service
Network Error Rate	Delta – zero based
Time – Period Report	Delta – zero based
Power In	Threshold
Board Temperature	Threshold
CDMA HW Temp	Threshold

Event Configuration Types

- Switch - open, closed, on change
- Delta - change from last report. Value stored.
- Delta – zero based - change from last report. Value not stored.
- Threshold – Above, Below, on crossing.
- GPS Fix – fix obtained, fix lost, on change.
- Network State - when network service has been obtained.
- Network Service – Trigger when service found, lost, or on change.

Each event can be triggered to send one more report. In each group, is a related type of data:

Enable Events Reporting

Events Reporting is disabled by default and should be enabled by choosing Enabled for the Enable Event Reporting field under Admin group and Advanced tab. Click on Apply for the change to take effect.

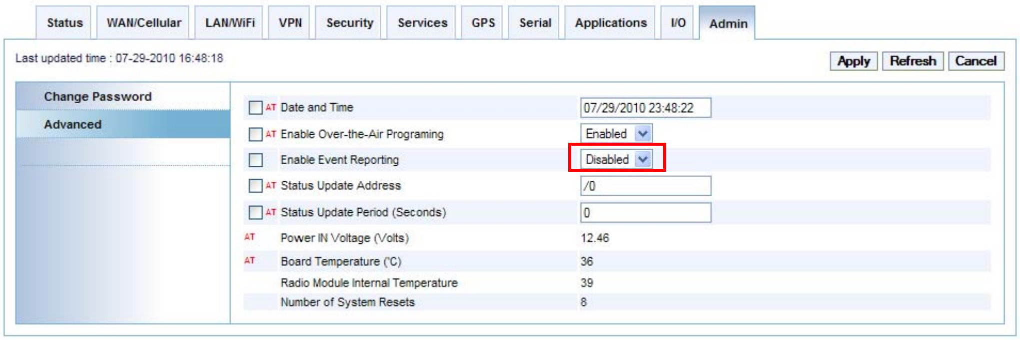


Figure 15-1: ACEmanager: Admin - Advanced

Digital Inputs

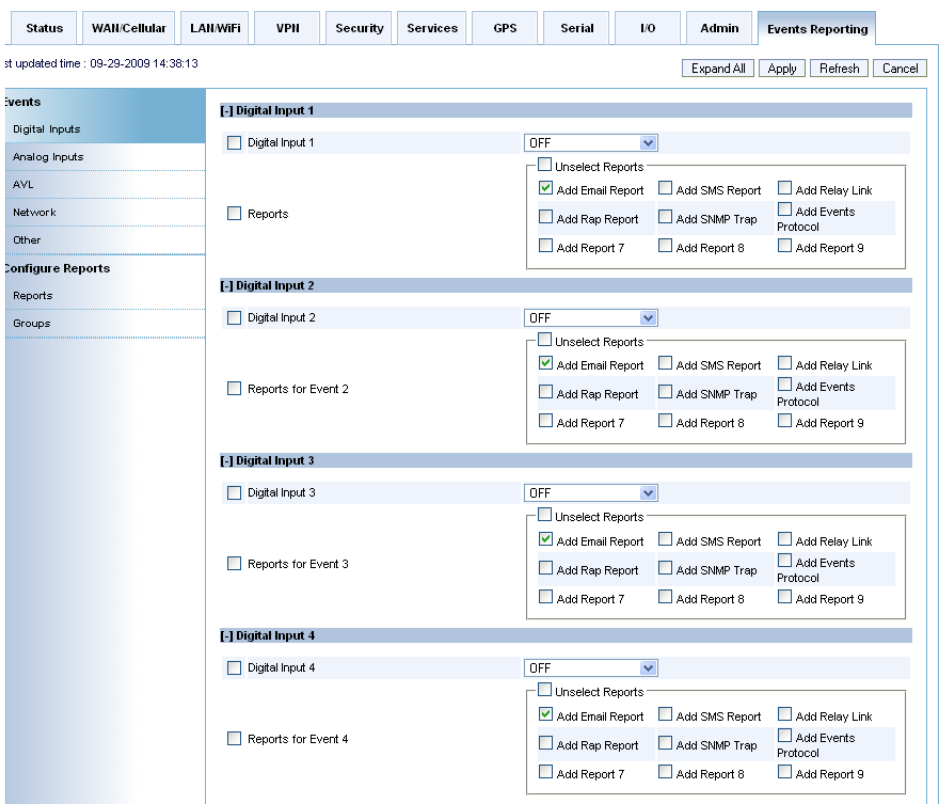


Figure 15-2: ACEmanager: Events Reporting - Events Digital Inputs

Each Digital Input (1-4 shown in the figure) will have a Digital Input check on or off box and a category of Reports that you can select or unselect.

Analog Inputs

Event triggers for the analog inputs and scaled, or transformed, values.

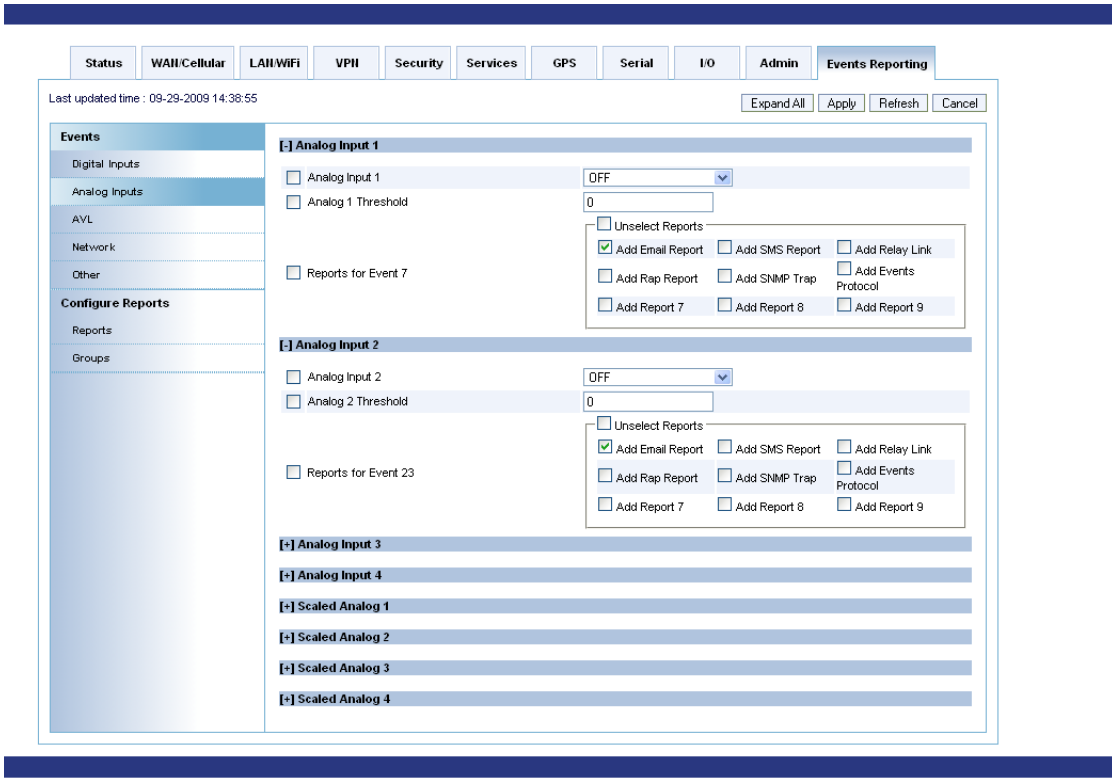


Figure 15-3: ACEmanager: Events Reporting - Analog Input

AVL

Event triggers for GPS Fix, Vehicle Speed, and Engine Hours.

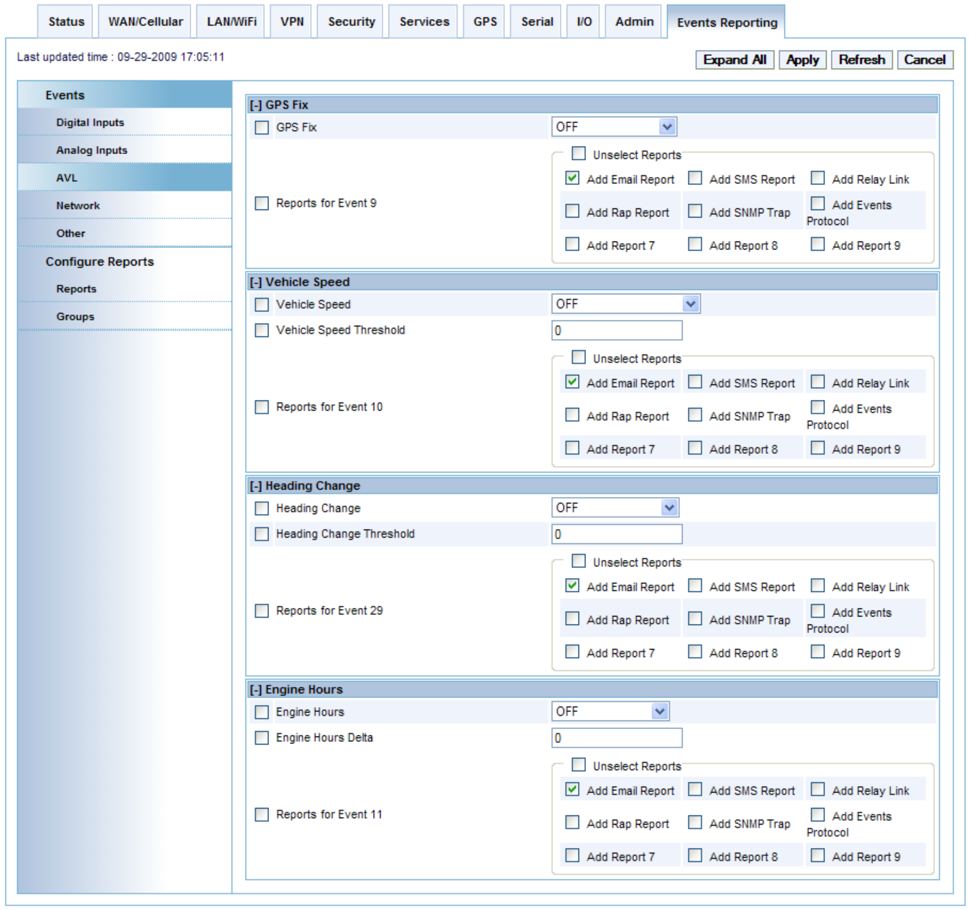


Figure 15-4: ACEmanager: Events Reporting - AVL

Network

Event triggers for the status of the cellular network connection.

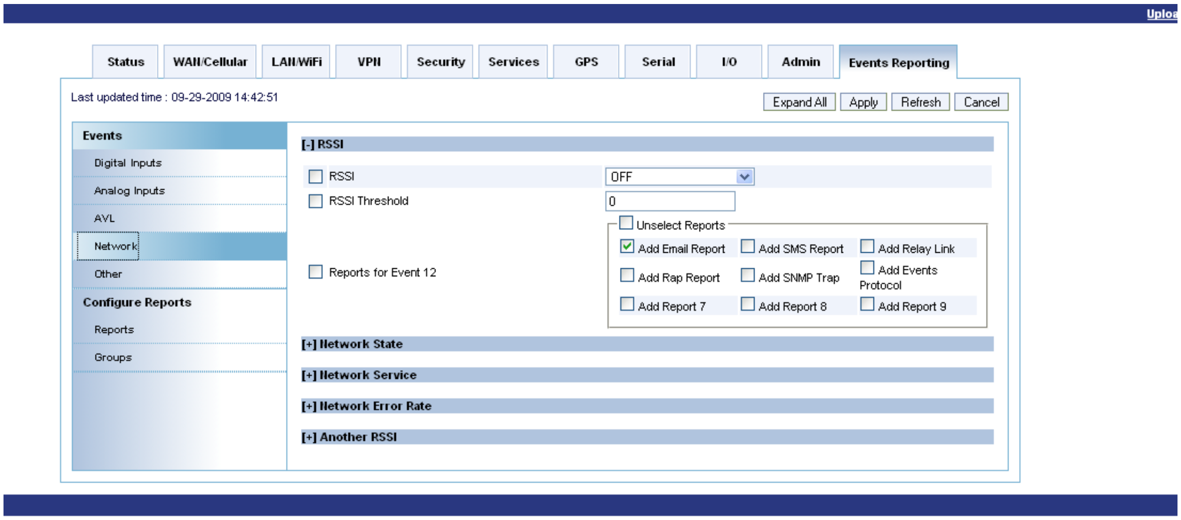


Figure 15-5: ACEmanager: Events Reporting - Network

Other

Event triggers for periodic reports, Power, and the temperature of the AirLink device.

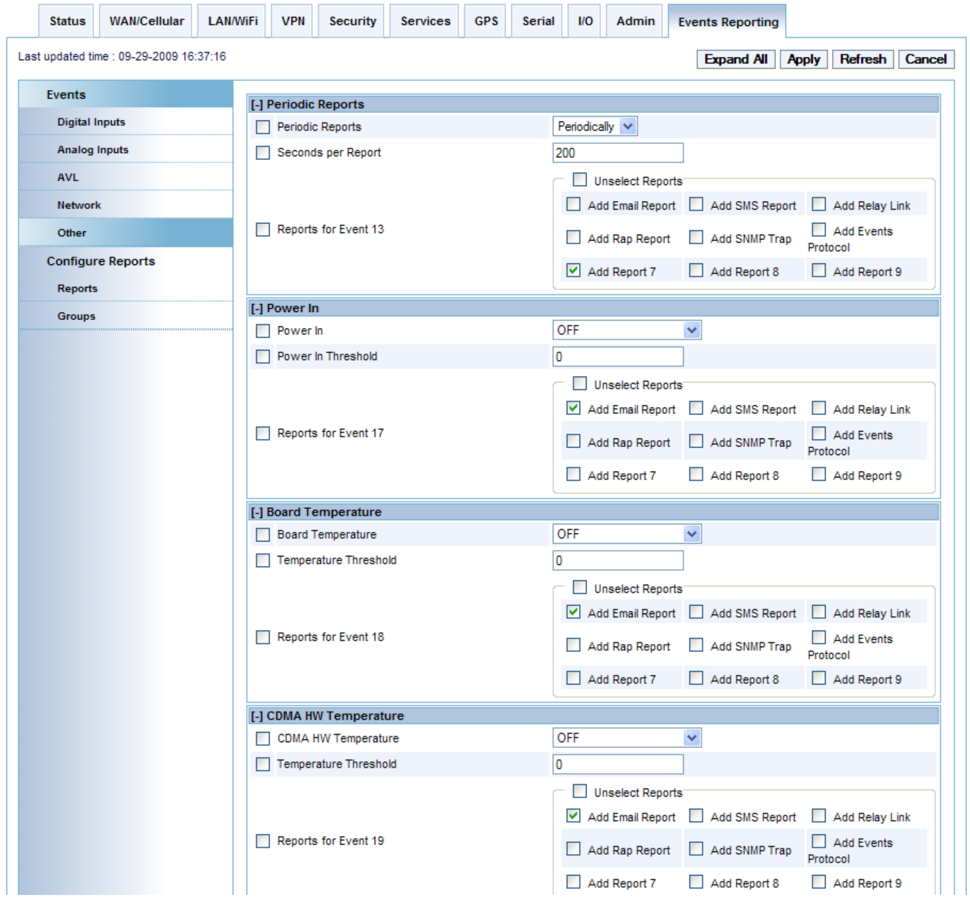


Figure 15-6: ACEmanager: Events Reporting - Other

Configuring Reports

There are six ways to send a report. The configuration will vary.

- Email
    - Destination email address
    - Subject, Message
    - Data groups
- SMS text message
    - Destination Phone number
    - Message
    - Data Groups.
- SNMP Trap notification
    - Destination IP is configured in the SNTP menu.
- Relay
    - Select the relay to link to, and Invert if necessary.
- RAP message
    - Destination report server and report type is configured in the PinPoint Menu.

- Events Protocol message to a server
  - Destination report server is configured in the PinPoint Menu
  - Report format – TLV, Binary, ASCII, XML. See Events Protocol (appendix A) for details.

The Reports group allows you to configure whose reports are sent and what date they contain.

The Setup page for Reports configures which types of reports will be available.

Reports

Each report type has its own configuration page. If a report type is not set to be allowed, its configuration page will be hidden. Some reports will be hidden by default.

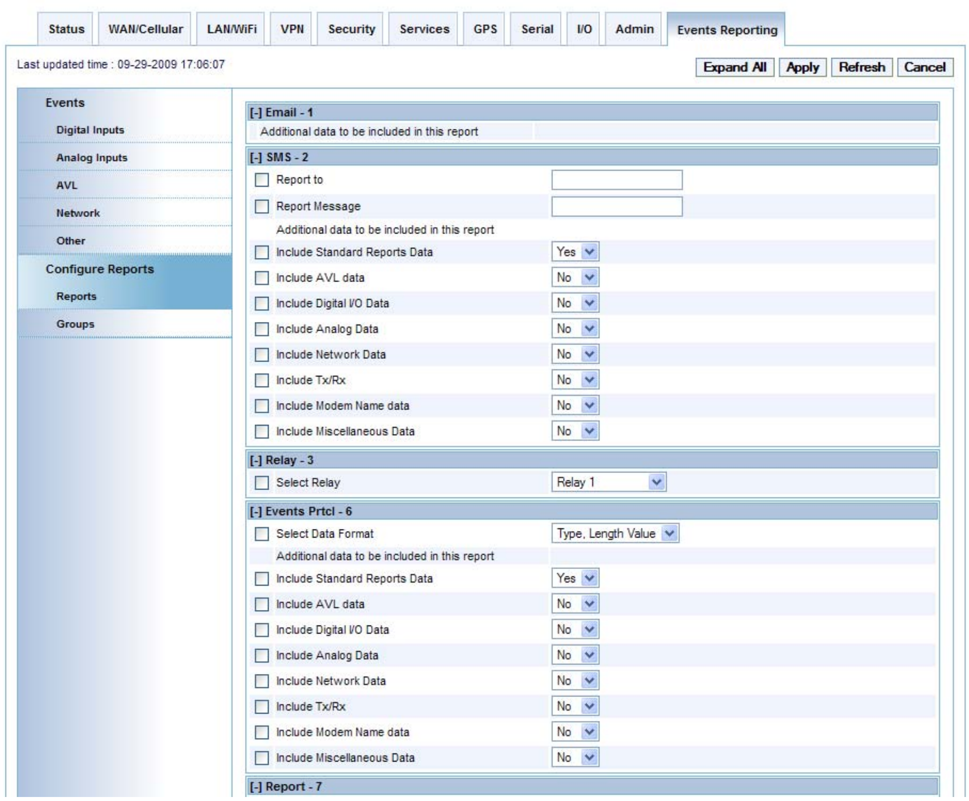


Figure 15-7: ACEmanager: Events Reporting - Configure Reports

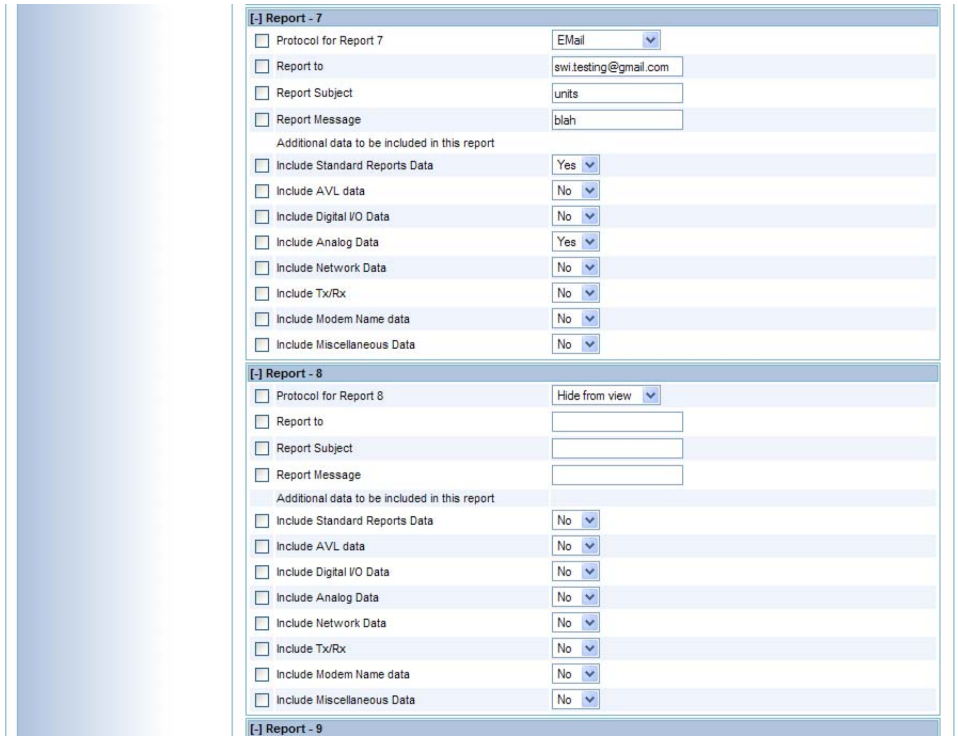


Figure 15-8: ACEmanager: Events Reporting - Configure Reports - Reports 7 and 8

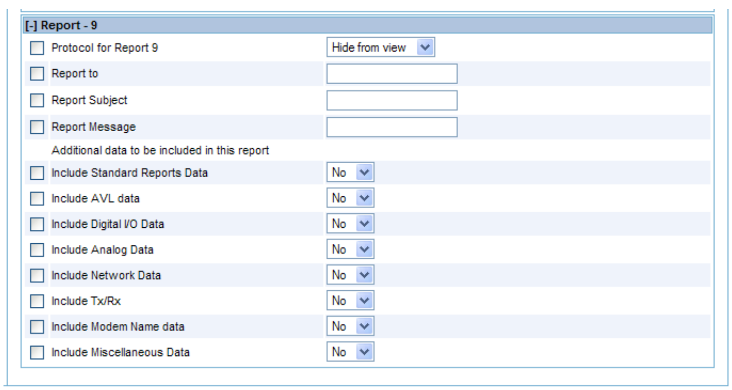


Figure 15-9: ACEmanager: Events Reporting - Configure Reports - Report 9

When you allow an additional report type on the *Setup* page, the sub-group configuration page will be made available. For example, to allow *Report 8* and display its configuration page, on the *Setup* page you would select *Allow this Report*. To conceal the report configuration and not make it available for events, select *Remove this Report*.

- **Email** - The AirLink device will send out an email to a specific destination using the SMTP settings.
- **SMS** -An SMS will be sent to a specific cellular destination, such as your cell phone.
- **Relay** - The AirLink device will change the state of the specified output relay.
- **RAP** - Using the configuration from the PinPoint group, a GPS Report type will be used.

- **SNMP** - Using the SNMP settings in Common > Other, the report will be included in the SNMP Trap.
- **Events Protocol** - The AirLink device will send out a report to the Reports Server to allow an interface with a wider variety of applications.
- **Report 7, Report 8, Report 9** - An additional destination for Email, SMS, Relay, or Events Protocol.

For the message report types, Email, SMS, and Events Protocol, you will need to select which data you would like included in the report.

Email

- **Report To** - The email address where the report should be sent.
- **Report Subject** - The subject that should be displayed.
- **Report Message** - The message you want included with each report.

Note: You cannot send an Email with your AirLink device unless the Email server you have configured allows your AirLink device as a relay host. Talk to your network administrator to ensure you can send email through the email server using your AirLink device.

SMS

- **Report To** - The cellular phone number where the report should be sent.
- **Report Message** - The message you want included with each report.

Note: You can only send SMS from your AirLink device if your cellular account allows SMS. You may need to have SMS added to the account. SMS from data accounts is blocked on some cellular networks.

Relay

The relay outputs on the AirLink device I/O port can be used to cause an external action.

- **1 - Relay 1** - Open
- **2 - Relay 1, Inverted** - Closed
- **3 - Relay 2** - Open
- **4 - Relay 2, Inverted** - Closed

Tip: *The relays are capable of switching small loads. If you need a stronger signal, such as to open some door locks, you can connect the AirLink device's relay to a stronger solenoid relay which has enough power to cause the desired effect.*

Events Protocol

The Events Reporting protocol is a collection of messaging formats. The messages are sent to the Reports Server.

The Events Protocol includes four message types.

- **1 - Type, Length, Value** - The TLV consists of the MSCI ID as the type, the length of the data, and the actual data.
- **2 - Binary** - A binary condensed form of the TLV message will be sent.
- **3 - ASCII** - An ASCII condensed and comma deliminated form of the TLV message will be sent.
- **4 - XML** - An XML form of the data will be sent.

Tip: *Because of its flexibility and robustness, the TLV message type is recommended for most reports using the Events Protocol. The Binary and ASCII forms do not contain "A type field" which can result in misinterpretation of data. Since the TLV and XML forms always includes the type as well as the data, an unintentional type can be identified much easier.*

Additional Reports

The last three report types allow an additional report of the defined types sent to a separate destination.

Select the Protocol, or report type desired and fill in the appropriate fields. The configuration needed for the report will depend on the protocol chosen. Use the previous report types as the guide for what fields are required.

- For an additional **Email** report, you would fill in the Report To, Report Subject, and Report Message the same way as the Email report. The Report To can be the same email address as the Email report or a different one. The Report Subject and Report Message can also be different.
- For an additional **SMS** report, you would specify the phone number in the Report To field and fill in the Report Message.
- For an additional **Relay** report, you would specify the relay value by number in the Report To field.
  - **1** - Relay 1
  - **2** - Relay 1, Inverted
  - **3** - Relay 2
  - **4** - Relay 2, Inverted
- For an additional **Events Protocol** report, you would use the Report To field to indicate the protocol, by number, to be used.
  - **1** - Type, Length, Value
  - **2** - Binary
  - **3** - ASCII
  - **4** - XML

Groups

The data in the device has been put in groups of similar data. For each report, you can specify which groups to included.

The groups are:

- Standard
- AVL
- Digital I/O
- Analog Input
- Network Data
- Network Traffic
- Device Name
- Misc Data

For each group you can enable individual fields. The complete list of fields is given in Appendix .

Note: Each data item included in a report will add to the size of the report. Disabling data not required will allow the report to be more compact. By default, all data is included.

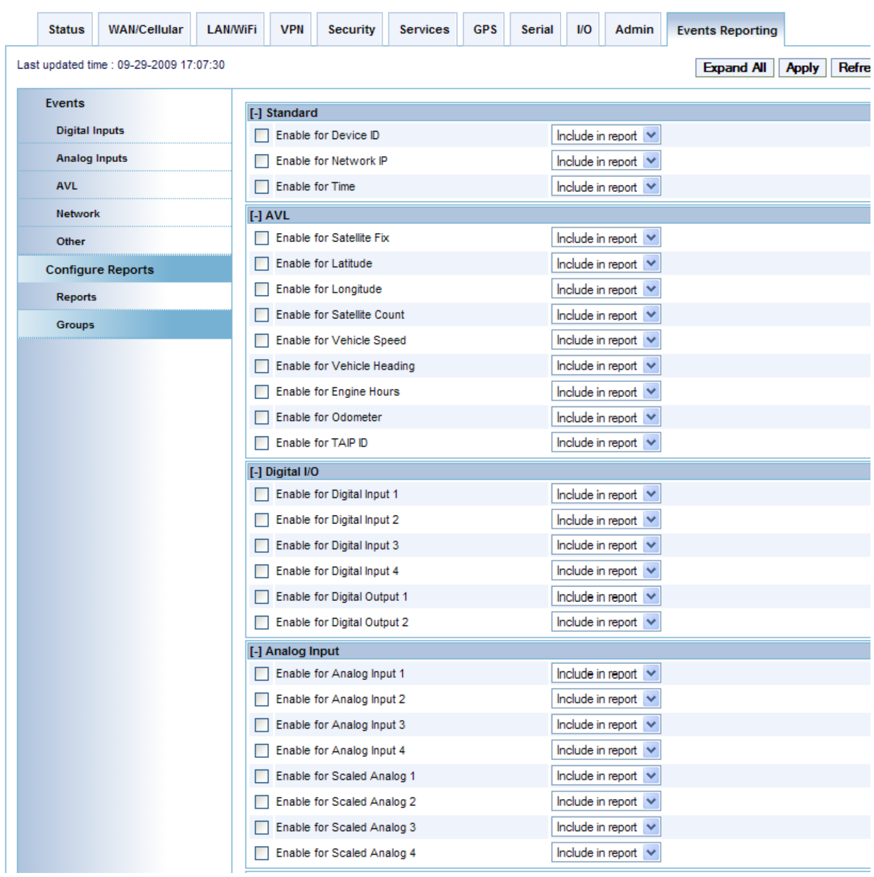


Figure 15-10: ACEmanager: Groups - Standard to Analog Input

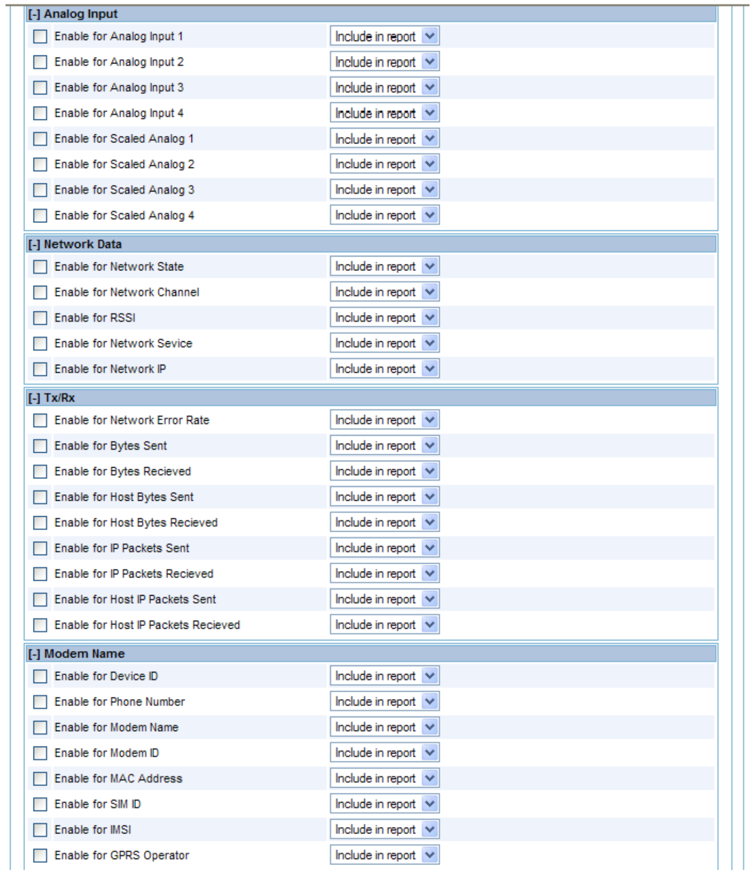


Figure 15-11: ACEmanager: Groups - Analog Input to device Name

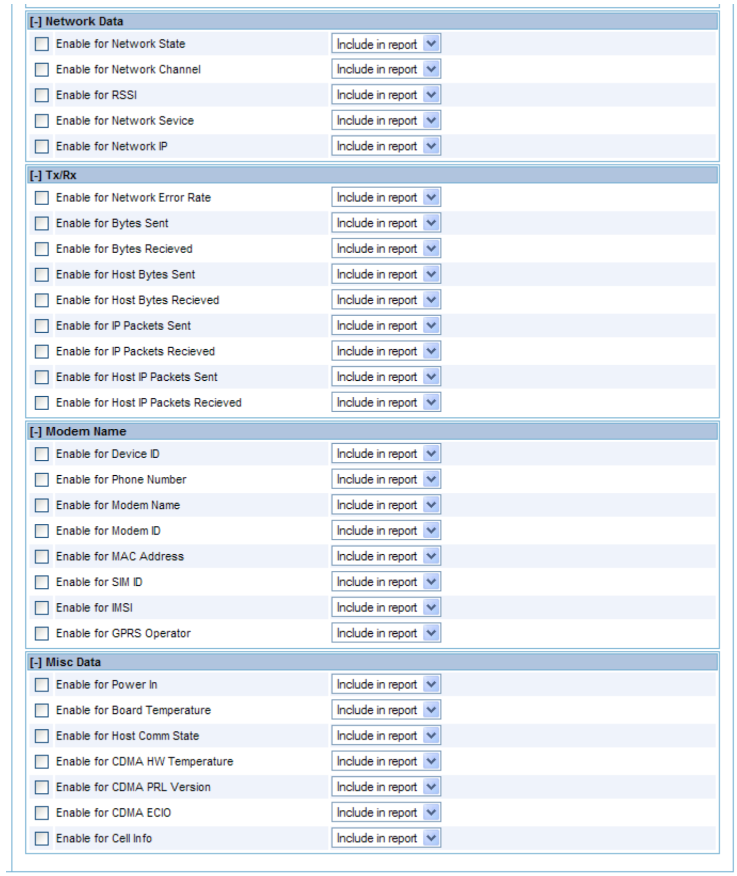


Figure 15-12: ACEmanager: Groups - Network Data to Misc Data

Each report type has its own configuration page. If a data group type is not set to be allowed on the Setup page, its configuration page will be hidden.

For each data element, select to *Include in Report* or *Don't Include*. The default is for all data to be included.

Tip: *Excluding data elements can reduce the size of the reports.*

Configuring Data

Standard Group

These elements in the Standard group are general identifiers for the AirLink device and the event occurrence. The elements of the Standard group will appear on all reports.

- **Enable for Device ID** - The device ID of the AirLink device. This should be enabled for a cellular account with a dynamic IP address.
- **Enable for Network IP** - The IP address given by the cellular network.

- **Enable for Time** - The time the report was generated. This will be the same time that is displayed with *DATE. The date will be sent as UTC: month, day, year, hour, minute, seconds.

AVL Group

GPS data is included in the Automatic Vehicle Location (AVL) data group.

- **Enable for Satellite Fix** - If there is a usable fix with the GPS satellites.
- **Enable for Latitude** - The latitude reported by the GPS.
- **Enable for Longitude** - The longitude reported by the GPS.
- **Enable for Satellite Count** - The number of satellites the GPS is able to ‘see’.
- **Enable for Vehicle Speed** - The speed of the vehicle reported by GPS.
- **Enable for Engine Hours** - The number of hours the engine has been on based on either Power In or Ignition Sense.
- **Enable for Odometer** - The number of miles reported by GPS.
- **Enable for TAIP ID** - The TAIP ID for the PinPoint X, configured in the PinPoint group.

Digital I/O Group

The Digital I/O group includes the status both the digital inputs and the relay outputs as well as the pulse count on the digital inputs.

- **Enable for Digital Input 1, 2, 3, or 4** - The status of the specific digital input.
- **Enable for Digital Output 1 or 2** - The status of the specific relay output.
- **Enable for Pulse Accumulator 1, 2, 3, or 4** - The pulse count of the specific digital input.

Analog Input Group

The Analog Input group includes the raw input data and the transformed input data, based on the configuration settings of the I/O group.

- **Enable for Analog Input 1, 2, 3, or 4** - The status of the specific analog input.
- **Enable for Scaled Analog 1, 2, 3, or 4** - The scaled analog input.

Network Data Group

The Network Data in this group relates to the cellular network and the connection state of the AirLink device.

- **Enable for Network State** - The network state for the AirLink device.
- **Enable for Network Channel** - The network channel to which AirLink device is connected.
- **Enable for RSSI** - The network state for the AirLink device.
- **Enable for Network Service** - The network channel to which AirLink device.

- **Enable for Network IP** - The IP address given by the cellular network.

Network Traffic Group

The Network Traffic in this group relates to the cellular network and the network between the AirLink device and any directly connected device(s).

- **Enable for Network Error Rate** - The error rate reported by the cellular network.
- **Enable for Bytes Sent** - The number of bytes sent on the cellular network since last reset.
- **Enable for Bytes Received** - The number of bytes received from the cellular network since last reset.
- **Enable for Host Bytes Sent** - The number of bytes sent from the network between the AirLink device and the connected device(s) since last reset.
- **Enable for Host Bytes Received** - The number of bytes received from the network between the AirLink device and the connected device(s) since last reset.
- **Enable for IP Packets Sent** - The number of IP packets sent on the cellular network since last reset.
- **Enable for IP Packets Receive (MSCI**- The number of IP packets received from the cellular network since last reset.
- **Enable for Host IP Packets Sent** - The number of IP packets sent from the network between the AirLink device and the connected device(s) since last reset.
- **Enable for Host IP Packets Receive (MSCI**- The number of IP packets received from the network between the AirLink device and the connected device(s) since last reset.

Device Name Group

These elements in the device Name group are general identifiers for the AirLink device and its cellular account.

- **Enable for Device ID** - The device ID of the AirLink device. This should be enabled for a cellular account with a dynamic IP address.
- **Enable for Phone Number** - The phone number of the AirLink device.
- **Enable for device Name** - The device Name of the AirLink device.
- **Enable for device ID** - The ESN or EID/IMEI of the AirLink device.
- **Enable for MAC Address** - The MAC Address of the Ethernet port of the AirLink device.
- **Enable for SIM ID** - The SIM ID of the AirLink device.
- **Enable for IMSI** - The IMSI of the SIM installed in the AirLink device.
- **Enable for GPRS Operator** - The operator of the SIM installed in the AirLink device.

Miscellaneous (Misc) Data Group

The Miscellaneous Data includes temperature rates and other information that does not fit in the other categories.

- **Enable for Power In** - The voltage level of the power coming in to the AirLink device at the time of the report.
- **Enable for Board Temperature** - The temperature of the internal hardware of the AirLink device at the time of the report.
- **Enable for Host Comm State** - The signal level between the AirLink device and the connected device(s).
- **Enable for CDMA HW Temperature** - The temperature of the internal radio module.
- **Enable for CDMA PRL Version** - The PRL version in use by the AirLink device.
- **Enable for CDMA ECIO** - The energy level of the signal from the cellular network.
- **Enable for Cell Info** - The GPRS cell information for the AirLink device.

A: Windows Dial-up Networking (DUN)

A

Dial-up Networking (DUN) allows a computer or other device to use the serial port or ethernet port or USB virtual serial port on your AirLink device to connect to the Internet or private network using PPP just like an analog modem using a standard phone line.

Caution: *To install any driver on your computer, you may need to be logged in as Administrator or have Administrator privileges for your login.*

Microsoft Windows XP is used in the examples below. The modem driver installation and DUN setup and configuration is similar in Microsoft Windows products. Examples are not provided here for installing the driver or configuring DUN for any other operating system.

Installing a device driver for AirLink device

Standard installations of Microsoft Windows XP and 2000 include a generic device driver which will work with your AirLink device.

1. Connect the AirLink device.
   a. Connect the device to the computer with a DB-9 cable or the USB port in serial mode.
   b. Plug in the AC adapter, connect the antenna(s) and power on the device.
2. Install the driver.
   a. Select *Start > Control Panel > Phone and device Options* (in Classic View).

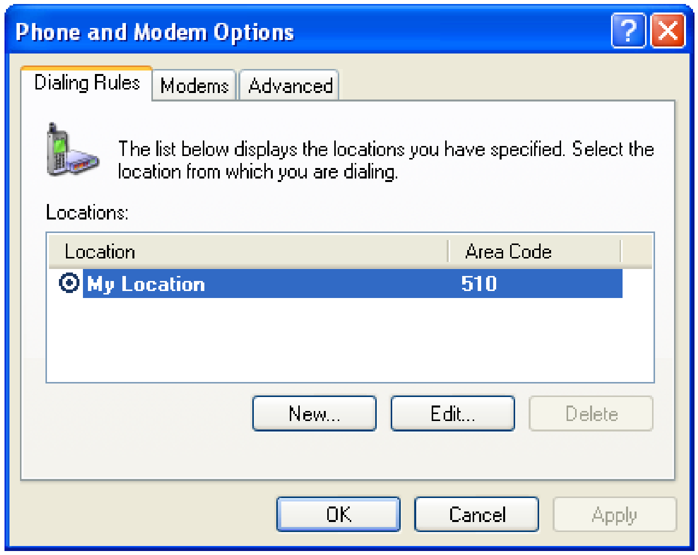


Figure 1-1: Phone and device Options

b. Select the *devices* tab.

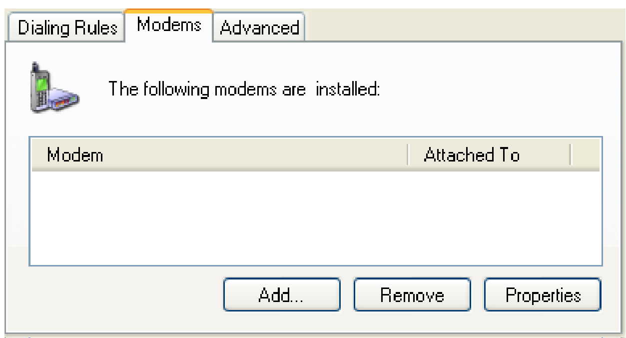


Figure 1-2: Phone and device Options: devices

c. Select *Add*.

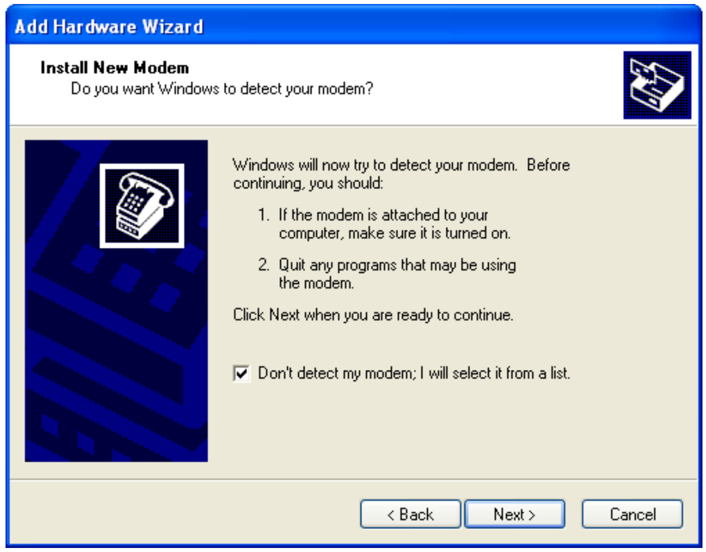


Figure 1-3: Add Hardware Wizard

d. Check *Don't detect my device; I will select it from a list.*

e. Select *Next.*

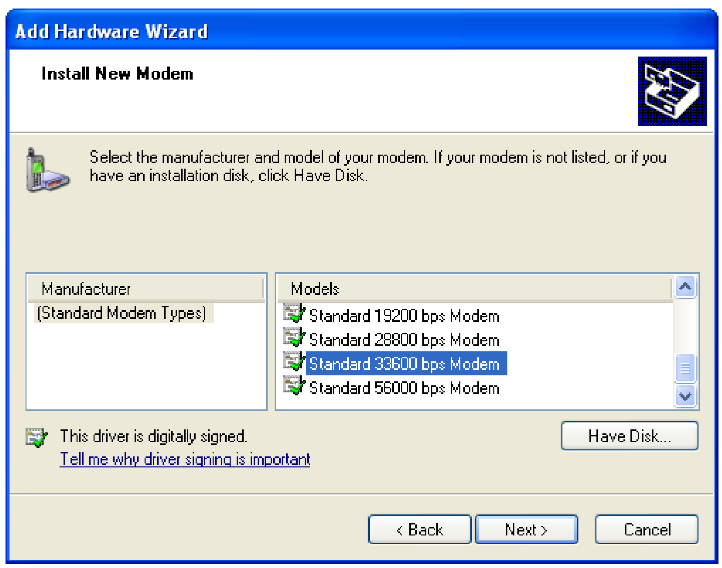


Figure 1-4: Add Hardware Wizard: Install New device

f. Select *(Standard device Types)* from the Manufacturers column.

g. Select *Standard 33600 bps device* from the Models column.

Tip: *If you have the speed for your device configured as something other than the default, use the Standard device that matches the speed you configured.*

h. Select *Next.*

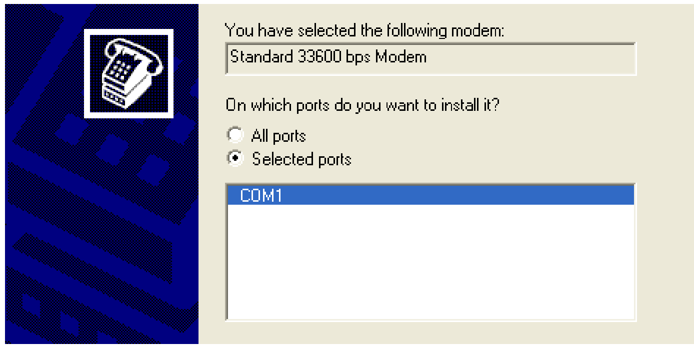


Figure 1-5: Add Hardware Wizard: Select Ports

i. Check *Selected Ports.*

j. Select the COM port the device is connected to (commonly COM1).

k. Select *Next.*

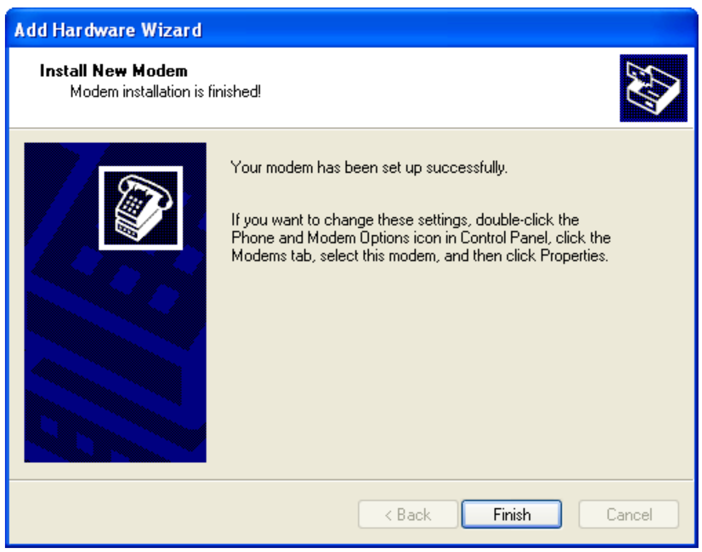


Figure 1-6: Add Hardware Wizard: Finish

l. Once the device driver is installed, select *Finish.*

When you return to the *Phone and device Options* window, you should see the newly installed device “attached to” the correct COM port.

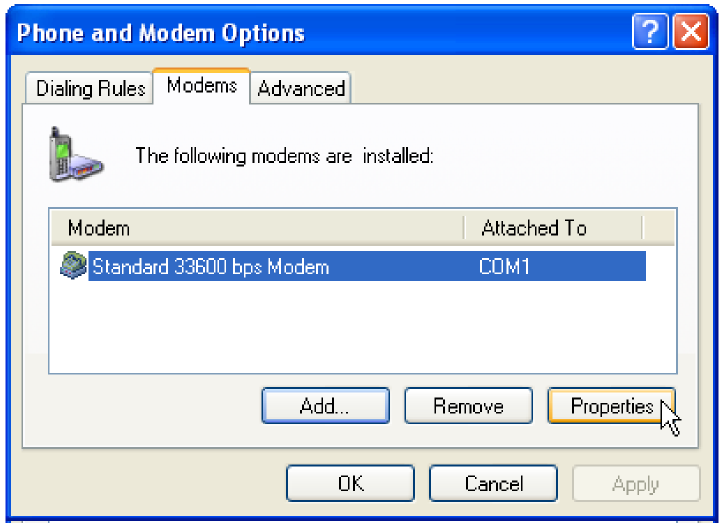


Figure 1-7: Phone and device Options: devices

a. Highlight the device and select *Properties*.

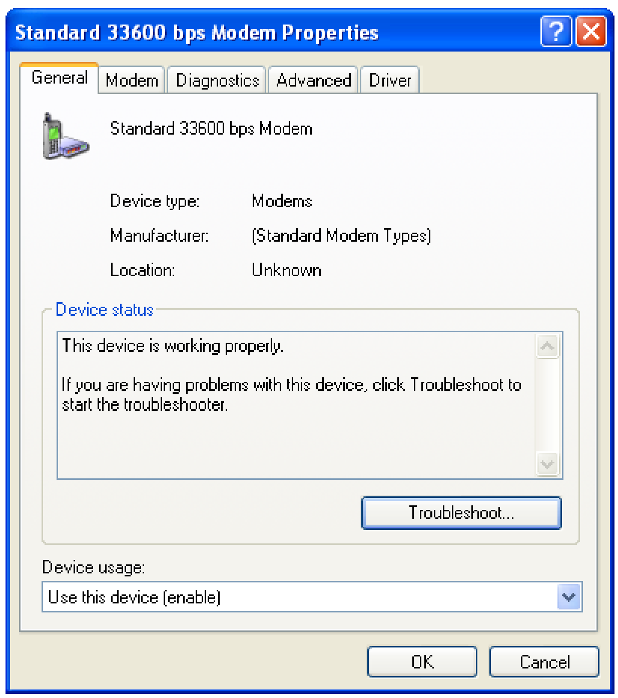


Figure 1-8: device Properties

b. Select the *device* tab.

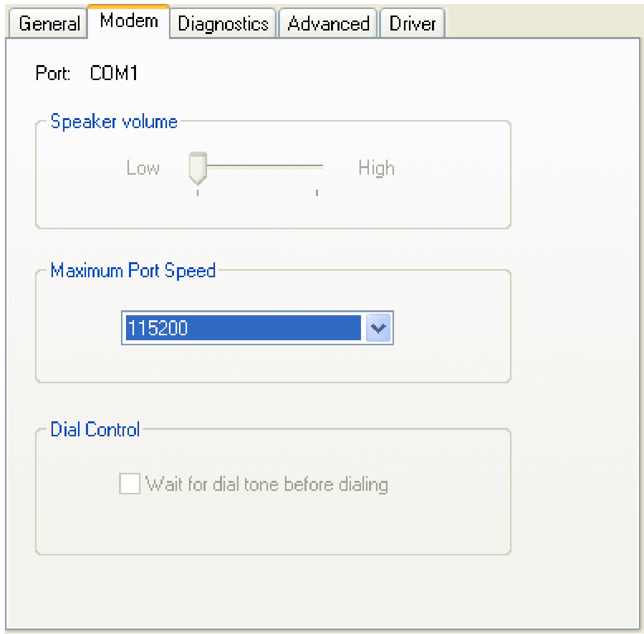


Figure 1-9: device Properties: device

c. Maximum Port Speed should be set to *115200* (default).

d. Select *OK* to exit.

e. Select *OK* again to exit out of the Phone and device Options.

Creating a Dial-Up Networking (PPP) Connection

Once you have the driver for the modem installed on your computer, you can set up and configure Dial Up Networking (DUN) to use the modem as your connection to the Internet using PPP.

Note: No other device or program can be using the same COM port (serial port) configured for the modem driver.

Caution: *If you have an existing LAN connection, installing DUN for the modem may interfere with the LAN connection. It's recommended to disconnect your LAN connection before using a PPP connection with your AirLink device.*

Once the DUN connection is initiated, by default, it will take over as the “default route” for network communication and specifically for Internet access. If you want the two connections to co-exist, you will need to de-select “Use default gateway on remote network” (described later) and use the route command in Windows to setup routing through the modem properly. This guide does not provide information on the route command. You may need to consult with your network administrator to properly configure routing.

1. Create a new network connection.
   a. Select *Start > Connect To > Show All Connections* to open the Network Connections window.

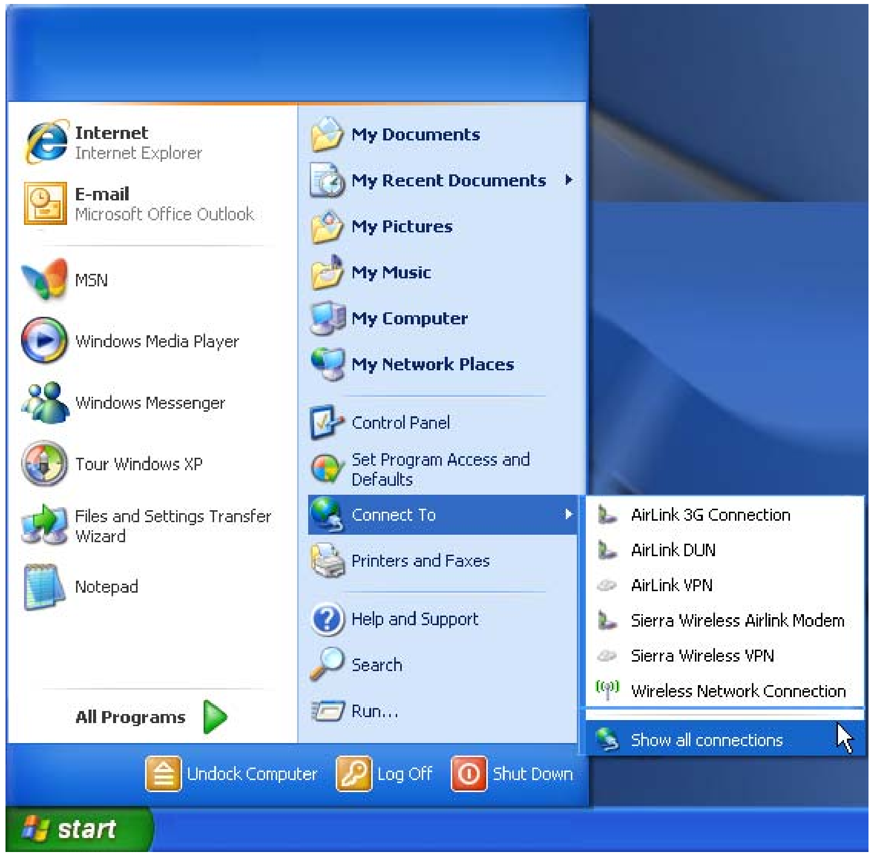


Figure 1-10: Windows : Start menu

   b. Select *Create a New Connection* under Network Tasks in the menu area on the left.

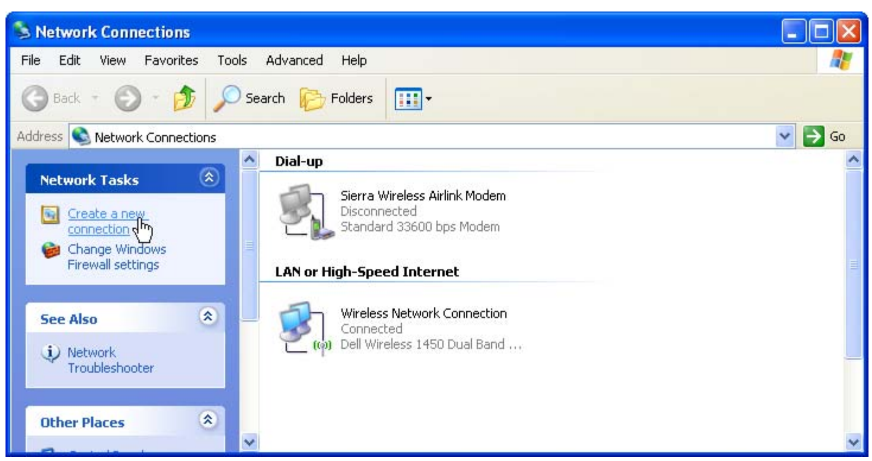


Figure 1-11: Create New Connection

   c. Select *Next* to start installing and configuring the DUN connection.

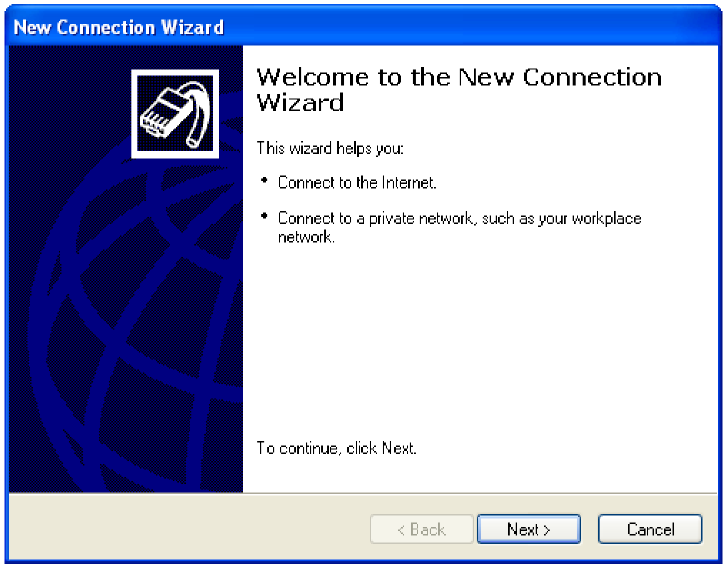


Figure 1-12: New Connection Wizard

d. Select *Connect to the Internet.*

e. Select *Next.*

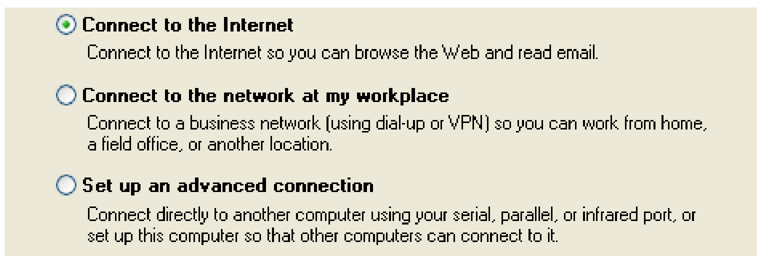


Figure 1-13: New Connection: Type

f. Select *Set up my connection manually.*

g. Select *Next.*

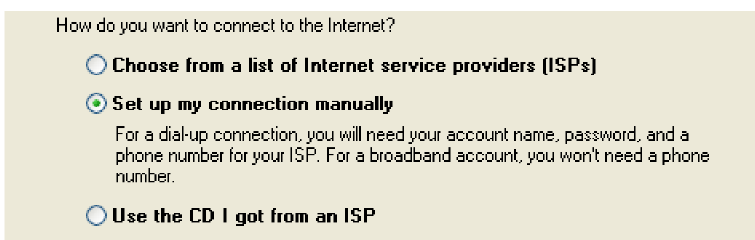


Figure 1-14: New Connection: How do you want to connect?

h. Select *Connect using a dial-up modem.*

i. Select *Next.*

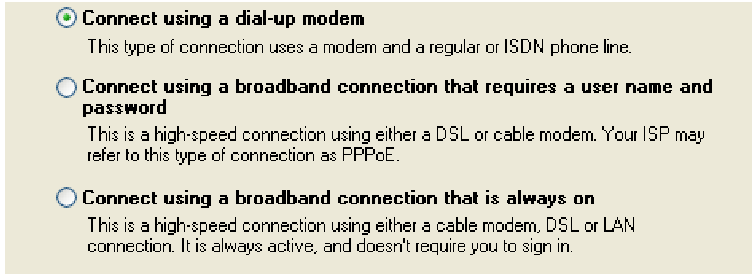


Figure 1-15: New Connection: Connect using...

j. *Optional:* If you have multiple modems installed on your computer, you may be prompted to select the modem to be used. If you only have one modem installed, this option will be omitted.

k. Check *Standard 33600 bps Modem*.

l. Select *Next*.

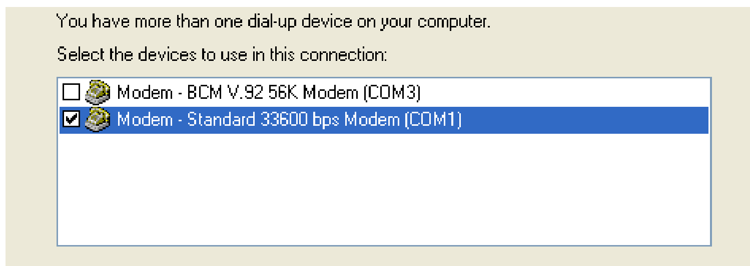


Figure 1-16: New Connection: Select Modem

m. Type in a name for the connection, such as *Sierra Wireless AirLink Modem*.

n. Select *Next*.

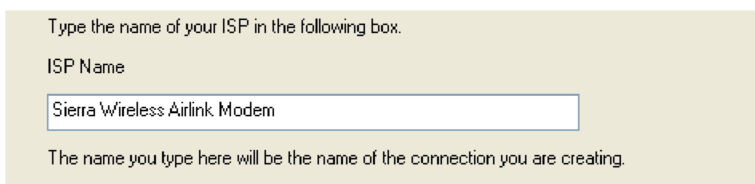


Figure 1-17: New Connection: Connection Name

Tip: *The name provided here will not effect the connection in any way. It is only a label for the icon. It can be the name of your wireless service provider (Provider), your modem (AirLink device), or any other designation for the connection.*

o. Type in *10001* as the phone number for the modem to dial.

p. Select *Next.*

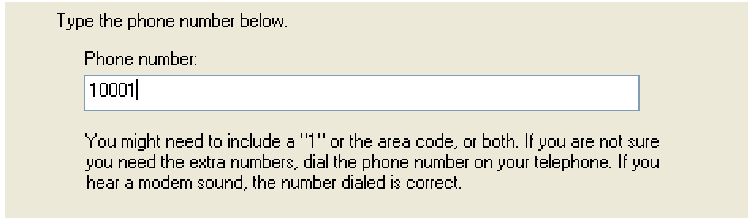


Figure 1-18: New Connection: Phone Number

q. *Optional:* If you have multiple users configured for your computer, you may be prompted for Connection Availability. If you select *My use only*, the account currently logged on will be the only one able to use this DUN connection.

r. Select *Next.*

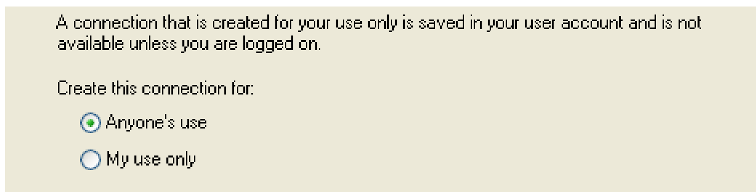


Figure 1-19: New Connection: Permissions

Generally the modem takes care of the Account Information, User name and Password, for the connection, so you can leave the fields blank (unless otherwise instructed by Support).

s. If you want to allow others to use the same login for the modem, select *Use this account name and password...*.

t. Select *Next.*

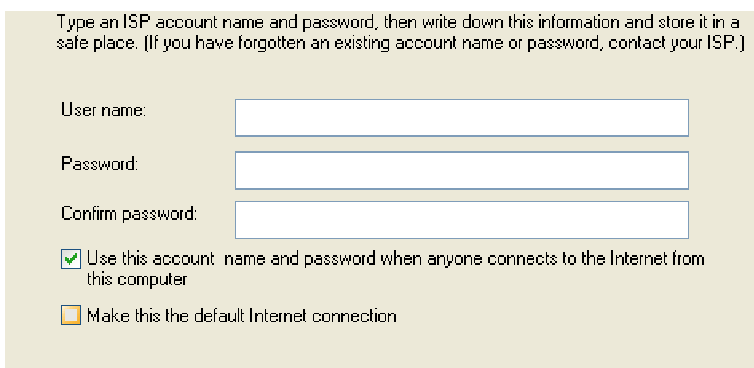


Figure 1-20: New Connection: Connection Information

Caution: *If you have a LAN connection to the Internet and select Make this the default Internet Connection for the DUN configuration, you will not be able to use the LAN to connect to the Internet and may also affect the network connection on your computer to the rest of the LAN. Select this option ONLY if the AirLink device will be your sole network connection.*

---

u. If you want to add a shortcut for this DUN connection to your desktop, check *Add a shortcut*.

v. Select *Finish* to exit the Network Connection Wizard.

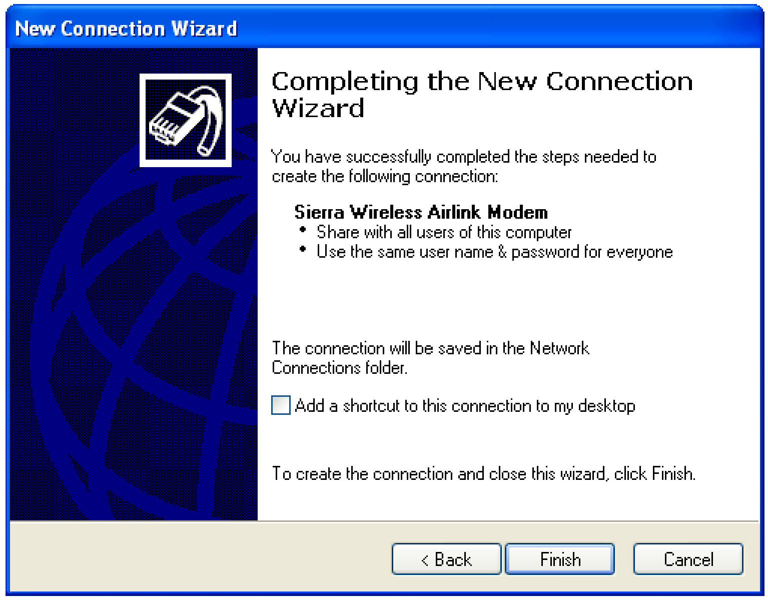


Figure 1-21: New Connection: Finish

2. Configure the DUN connection

After you complete the New Connection Wizard, there are a few more things you will want to configure in the connection.

a. Select *Properties*.

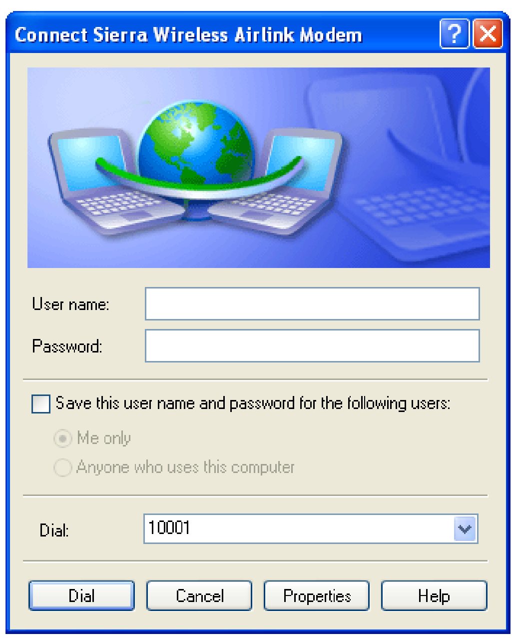


Figure 1-22: DUN Connection

b. Uncheck *Use dialing rules*.

c. Check *Show icon...when connected*.

d. Select *Configure*, below the Connect using line.

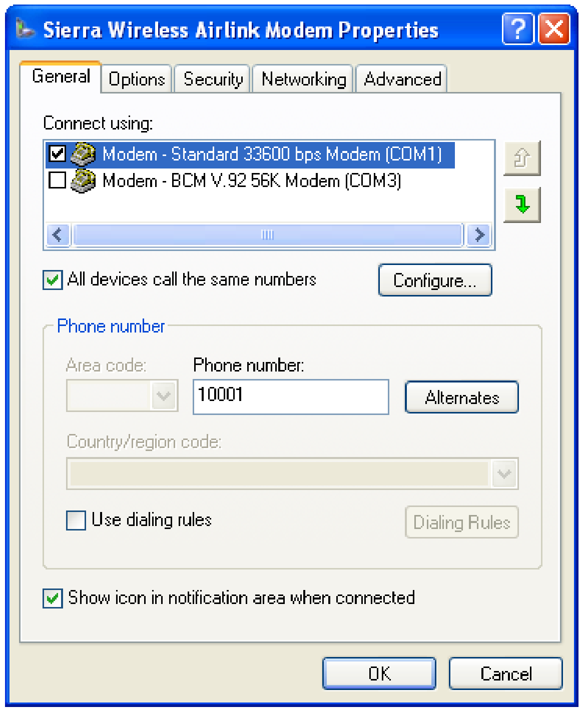


Figure 1-23: DUN Properties

e. Select *115200* as the Maximum speed.

f. Check *Enable hardware flow control*.

g. Do not check any other option.

h. Select *OK*.

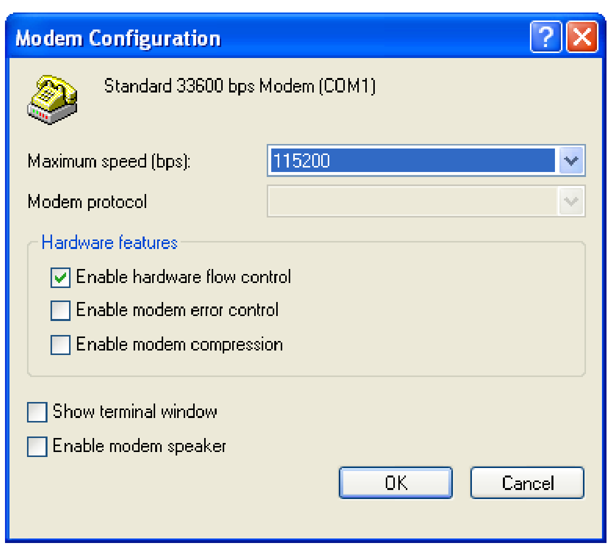


Figure 1-24: Modem Configuration

i. Back at the main properties screen, select the *Networking* tab.

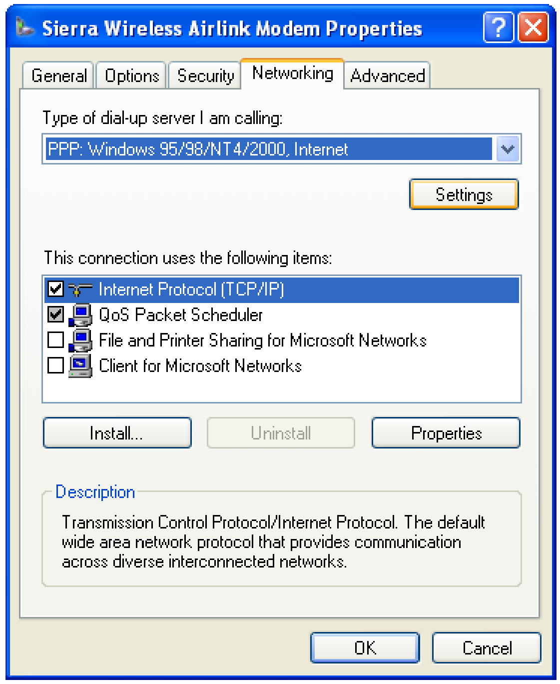


Figure 1-25: Networking

j. Select *Settings*.

k. Remove the checks from all three PPP settings.

l. Select *OK*.

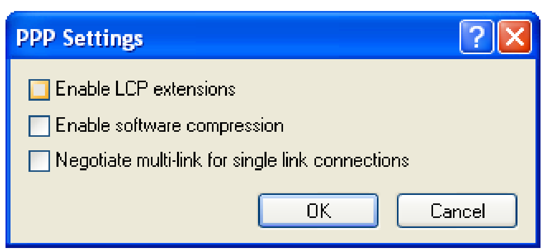


Figure 1-26: PPP Settings

m. Select (highlight) Internet Protocol (TCP/IP) and then select *Properties*.

Tip: *For most configurations, you will be obtaining the IP address and the DNS server address automatically.*

n. Select *Advanced*.

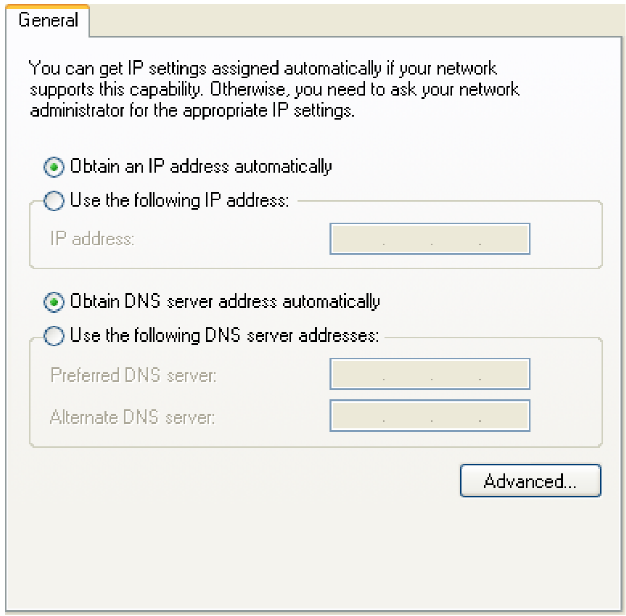


Figure 1-27: TCP/IP Properties

o. Uncheck *Use IP header compression*.

p. Check *Use default gateway on remote network.*

q. Select *OK*.

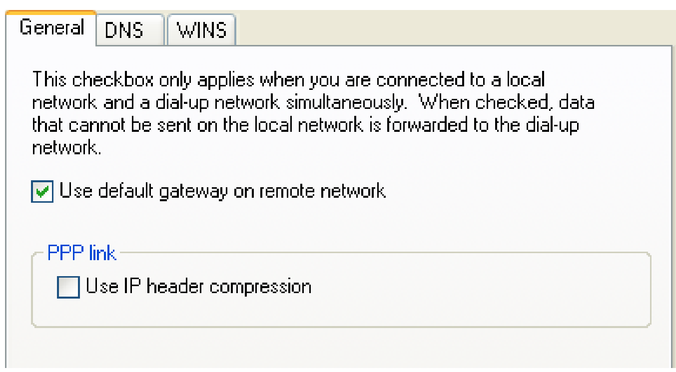


Figure 1-28: Advanced TCP/IP

Tip: *You may want to check the Options tab and change the settings for applications you might be using. The default options are generally applicable for most uses.*

Caution: *Unless specifically directed to do so by Support or your network administrator, you do not need to make any changes to the options on the Security tab.*

r. Select *OK* until you return to the *Connect* window.

Connecting to the Internet Using DUN

There are two methods you can use to connect with AirLink device to the Internet using DUN, AceView and the Windows DUN connection directly.

ACEview

ACEview is a small utility which can maintain your DUN connection and monitor the connection of your AirLink device to Provider. If you have not already installed ACEview you can obtain the most recent version from the Sierra Wireless AirLink website.

Note: The direct DUN connection features of ACEview are not available in Windows 98 or Windows NT.

This guide assumes you have a default installation of ACEview.

1. Start ACEview.

Start > All Programs > AirLink Communications > ACEview

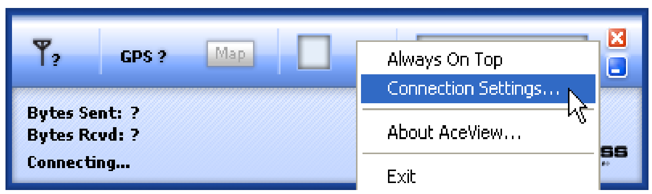


Figure 1-29: ACEview: Menu

a. Right-click on the ACEview window to open the menu.

b. Select *Connection Settings*.

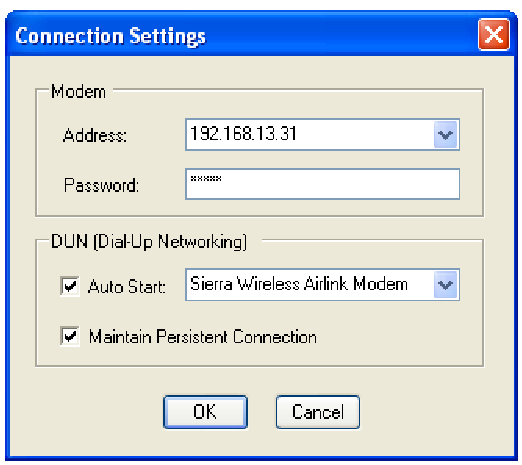


Figure 1-30: ACEview: Connection Settings

c. Select *Auto Start* in the DUN section.

d. Select *Maintain Persistent Connection*.

When checked, ACEview will continually check the DUN connection to ensure it is not down. If so, ACEview will attempt to connect again.

Tip: *When using the DUN connection, make sure the IP Address is set to the local IP address of the modem, 192.168.13.31 by default.*

e. Select *OK*.

f. *OK*.

Windows DUN

You can directly use the Dial-up link for the DUN connection.

1. Start the DUN session.

Start > Connect To > Prosoft Technology RadioLinx Modem

If you named the connection differently, use the name of the PPP connection you made earlier.

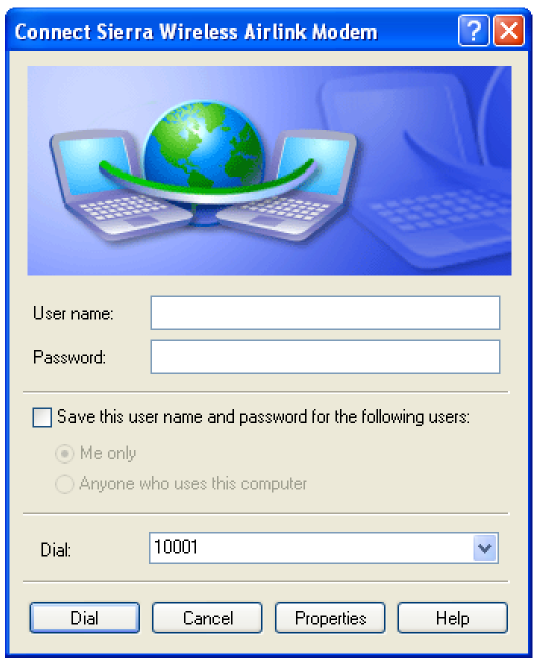


Figure 1-31: DUN Connection

Tip: *Generally you will not need to enter a Username or Password. If you do need to enter either, you can enter these parameters beforehand using *NETUID and *NETPW.*

Note: Select Dial to connect to the modem and the cellular network. *The speed shown in the connection is the speed between the modem and your computer, it is not the speed of the modem's connection to Provider or the Internet.*

When you're connected, an icon should appear in the system tray showing the connection status.

Figure 1-32: Connection indicator

Caution: *For DUN connections on a Windows Mobility or other non-personal computer, the DNS settings may not be configured with the DUN connection. You may need to go into the network settings and add DNS servers manually.*

B: Configuring Modbus/BSAP

B

The AirLink device supports Modbus ASCII, Modbus RTU, BSAP, and can also emulate other protocols like DF1 or others using its Modbus Variable feature.

Modbus Overview

The Modbus Protocol, developed by Modicon in 1979, provides for client-server (also referred to as master-slave) communications between intelligent devices. As a de facto standard, it is the most widely used network protocol in the industrial manufacturing environment to transfer discrete/analog I/O and register data between control devices. Modbus, BSAP, and other Modbus variations are often used in conjunction with telemetry devices.

Tip: *This section is just a brief overview of Modbus. For more information, refer to your Modbus equipment distributor or manufacturer or http://www.modbus.org.*

Telemetry

Telemetry is an automated communications process by which data is collected from instruments located at remote or inaccessible points and transmitted to receiving equipment for measurement, monitoring, display, and recording. Transmission of the information may be over physical pairs of wires, telecommunication circuits, radios or satellite.

Remote Terminal Unit (RTU)

Modbus was originally designed to be used in a radio environment where packets are broadcast from a central station (also called master or host) to a group of remote units. Each remote unit, Remote Terminal Unit (RTU), has a hexidecimal identification number (ID). The first part of the broadcast packet contains an RTU ID which corresponds to the ID of one of the remote units. The Modbus host looks for the ID and sends to only the unit with the matching ID. The RTU would then reply back to the central station.

The RTU connects to physical equipment such as switches, pumps, and other devices and monitors and controls these devices. The RTU can be part of a network set up for Supervisory Control and Data Acquisition.

Supervisory Control and Data Acquisition (SCADA)

Supervisory Control and Data Acquisition (SCADA) describes solutions across a large variety of industries and is used in industrial and engineering applications to monitor and control distributed systems from a master location. SCADA encompasses multiple RTUs, a central control room with a host computer (or network), and some sort of communication infrastructure.

SCADA allows for “supervisory” control of remote devices as well as acquiring data from the remote locations. Programmable Logic Controllers allow for a higher degree of automated SCADA.

Programmable Logic Controller (PLC)

A Programmable Logic Controller (PLC) is a small industrial computer which generally monitors several connected sensor inputs and controls attached devices (motor starters, solenoids, pilot lights/displays, speed drives, valves, etc.) according to a user-created program stored in its memory. Containing inputs and outputs similar to an RTU, PLCs are frequently used for typical relay control, sophisticated motion control, process control, Distributed Control System and complex networking.

Modbus TCP/IP

Modbus TCP/IP simply takes the Modbus instruction set and wraps TCP/IP around it. Since TCP/IP is the communications standard for the Internet and most networked computers, this provides a simpler installation. Modbus TCP/IP uses standard Ethernet equipment.

Raven Modbus on UDP

When Sierra Wireless AirLink devices are used in place of radios, a AirLink device is connected to the central station (host) and aAirLink device is connected to each remote unit. When the AirLink device is configured for Modbus with UDP, the AirLink device connected to the host can store a list of IP addresses or names with matching IDs. When the host at the central station sends serial data as a poll request, the AirLink device at the host matches the RTU ID to a corresponding IP of a AirLink device at a remote unit. A UDP packet is assembled encapsulating the RTU ID and serial data transmitted from the host. The UDP packet is then transmitted to the specific AirLink device at the remote unit matching the RTU ID. The remote AirLink device then disassembles the packet before transmitting the RTU ID and serial data to the remote unit. The remote units operate in normal UDP mode and their data is sent to the host via the remote AirLink device and host AirLink device.

Configuring the AirLink device at the Polling Host for Modbus on UDP

This section covers a Polling Host with standard Modbus, variations may need additional AT commands.

In ACEmanager, select *Port Configuration* in the side menu.

The destination port for the modem at the host needs to match the device port (*DPORT) in use on all the modems at the remote sites. For example, if the remote modem’s device port (*DPORT) is “12345”, then the Modbus host modem's *S53* destination port should be set to “12345”.

Take note of (or set) the Device Port setting in *DPORT to configure the destination port on the remote modems.

In ACEmanager, select *UDP* in the side menu. Select the appropriate *MD* mode from the drop down menu.

- **MD13** : Modbus ASCII
- **MD23** : Modbus RTU (Binary)
- **MD33** : BSAP
- **MD63**: Variable Modbus - individual parameters are set up manually.

If you do not have a static IP, the host modem should be configured to report its current IP to a Dynamic DNS (DDNS) server with Dynamic DNS.

In the Host modem’s configuration, instead of IP address for the Addr List (ATMLIST or ATMLISTX), substitute a single unique name for each modem, i.e. remote1, remote2, etc.

When you configure Dynamic DNS for the host modem, make note of your modem name and domain setting in ACEmanager in the menu selection *Dynamic IP* to be used with the remote modems.

With names instead of IP addresses for the Address List, the host modem will query the DNS server for the current IP address assigned to the specific name of a remote modem to send a message corresponding to the ID.

When you use names instead of IP addresses, to ensure your modems are updated quickly with the correct IP addresses for the names, you will want to set the DNS settings as well. In ACEmanager, select *DNS*.

Configure *DNSUSER to the same IP address as the Dynamic DNS (*IPMANAGER1). If your modems have dynamic IP addresses and not static (the IP address can change when it is powered up), configure *DNSUPDATE to a low interval to allow frequent updates.

Configuring the Remote AirLink devices for Modbus with UDP

This section covers standard Modbus settings for the AirLink device at the remote unit, variations may need additional commands.

1. Configure the ports

In ACEmanager, select *Port Configuration* in the side menu.

The destination port for the device at the host needs to match the device port in use on all the devices at the remote sites. For example, if the remote device's device port (see below) is "12345", then the Modbus host device's *S53* destination port should be set to "12345".

Set the destination port (S53) to match the device port of the host device (*DPORT). Make sure the device port of the remote device (*DPORT) matches the destination port of the host device (S53).

Configure IP addresses for the host.

If the Host device has a static IP address, enter it in the Destination Address for S53.

Note: With a name instead of IPs for the host device, the remote devices will query the DNS server for the current IP assigned to the host device before sending data back to the host.

If the device at the host has a dynamic IP and is using Dynamic DNS, instead of an IP address for S53, specify the name of the host device (*deviceNAME). If the remote devices are using a different DDNS than the host device, you will need to specify the fully qualified domain name (*deviceNAME+*DOMAIN).

*Note: Setting the Host device IP address as the S53 Destination Address provides a low level security. The device will not forward UDP traffic unless the source IP/port matches what is in S53. However, if you set *AIP=1, the device will forward UDP traffic from any source IP address as long as it is accessing the device on the configured *DPORT.*

2. Configure the default mode for start-up.

Each device at the remote locations will need to be configured to communicate with the device at the host. In ACEmanager, select *UDP* in the side menu.

- **a.** Enable *S82*, UDP auto answer.
- **b.** Set *S83* to the idle time-out applicable to your application, commonly 20.

3. Configure other RTU settings.

Other parameters may need to be changed, but this is dependent on the RTU type being used. As a minimum, this typically involves setting the proper serial settings to match your RTU.

4. Optional: Dynamic IP Address

If you do not have a static IP, the host device should be configured to report its current IP to a Dynamic DNS (DDNS) server with Dynamic DNS.

You will need to match the name of the device to the names specified in the host device's MLIST or MLISTX for the connected RTU.

When you configure Dynamic DNS for the host device, make note of your device name and domain setting in ACEmanager in the menu selection *Dynamic IP* to be used with the remote devices.

When you use names instead of IP addresses, to ensure your devices are updated quickly with the correct IP addresses for the names, you will want to set the DNS settings as well.

Configure *DNSUSER to the same IP address as the Dynamic DNS (*IPMANAGER1). If your devices have dynamic IP addresses and not static (the IP address can change when it is powered up), configure *DNSUPDATE to a low interval to allow frequent updates.

C: PPP over Ethernet (PPPoE)

C

Configuring a PPPoE Connection in Windows

1. Create a new network connection
   a. Select *Start > Connect To > Show All Connections*. This will open the Network Connections window.

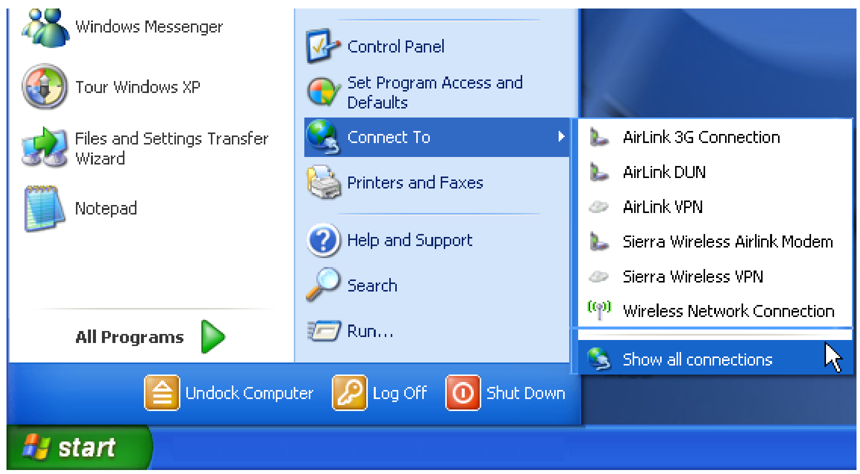


Figure 3-1: Windows : Start menu

   b. Select *Create a New Connection* under Network Tasks in the menu area on the left. Select Next to start installing and configuring the PPPoE connection.

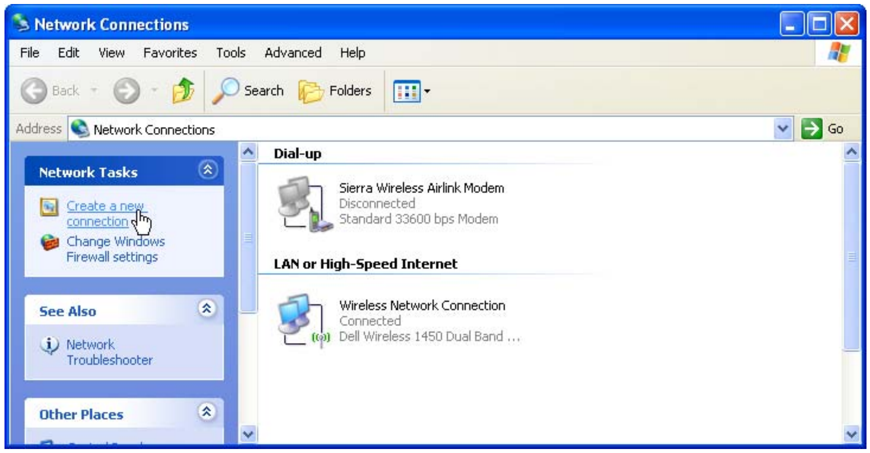


Figure 3-2: Windows : Network Connections

c. Click *Next* on the opening screen to begin creating a PPPoE connection.

d. *Next*.

Figure 3-3: New Connection Wizard

e. Select *Connect to the Internet*.

f. Select *Next*.

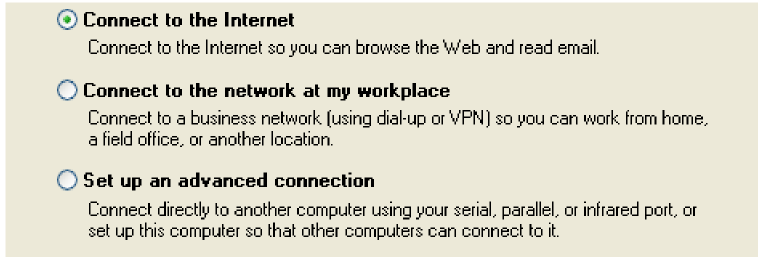


Figure 3-4: New Connection: Type

g. Select *Set up my connection manually.*

h. Select *Next*.

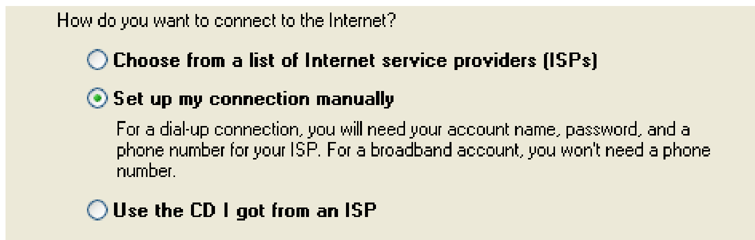


Figure 3-5: New Connection: How do you want to connect?

i. Select *Connect using a broadband connection*.

j. Select *Next*.

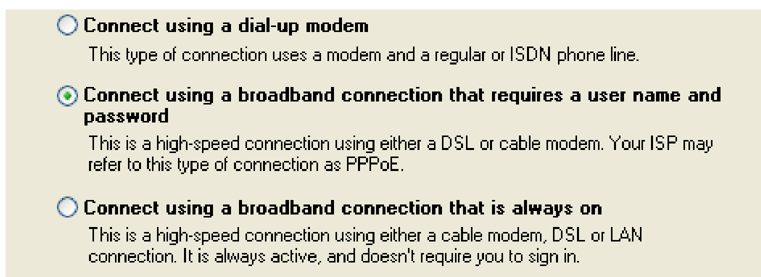


Figure 3-6: New Connection : Connect using broadband

k. Type in a name for the connection, such as *Sierra Wireless AirLink Modem*.

l. Select *Next*.

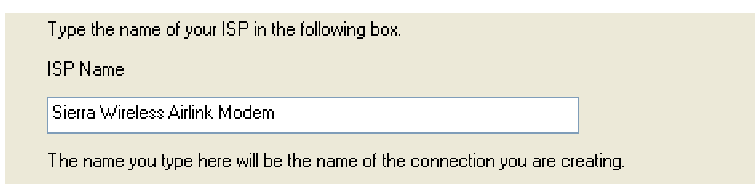


Figure 3-7: New Connection: Connection Name

Tip: *The name provided here will not effect the connection in any way. It is only a label for the icon. It can be the name of your wireless service provider (Provider), your modem (AirLink device), or any other designation for the connection.*

m. *Optional:* If you have multiple users configured for your computer, you may be prompted for Connection Availability. If you select *My use only*, the account currently logged on will be the only one able to use this connection.

n. Enter the user name and password you configured for *HOSTUID and *HOSTPW above.

Tip: *If you want to allow others to use the same login for the modem, select Use this account name and password... Select Next to continue.*

o. Select *Next.*

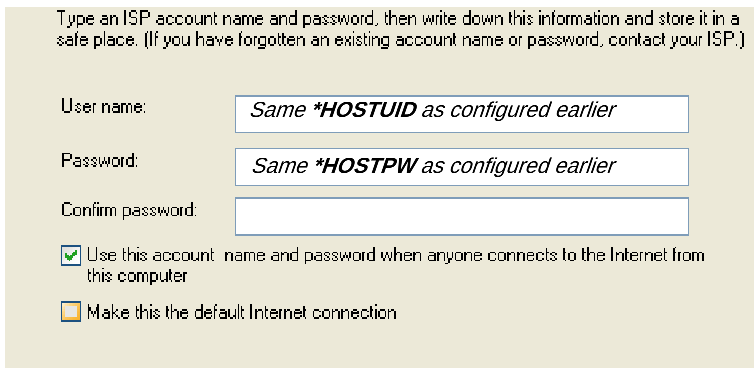


Figure 3-8: New Connection: Connection Information

Caution: *If you have a LAN connection to the Internet and select Make this the default Internet Connection for the PPPoE configuration, you will not be able to use the LAN to connect to the Internet and may also affect the network connection on your computer to the rest of the LAN. Select this option ONLY if the AirLink device will be your sole network connection.*

p. If you want to add a shortcut for this PPPoE connection to your desktop, check Add a shortcut...

q. Select *Finish* to exit the Network Connection Wizard.

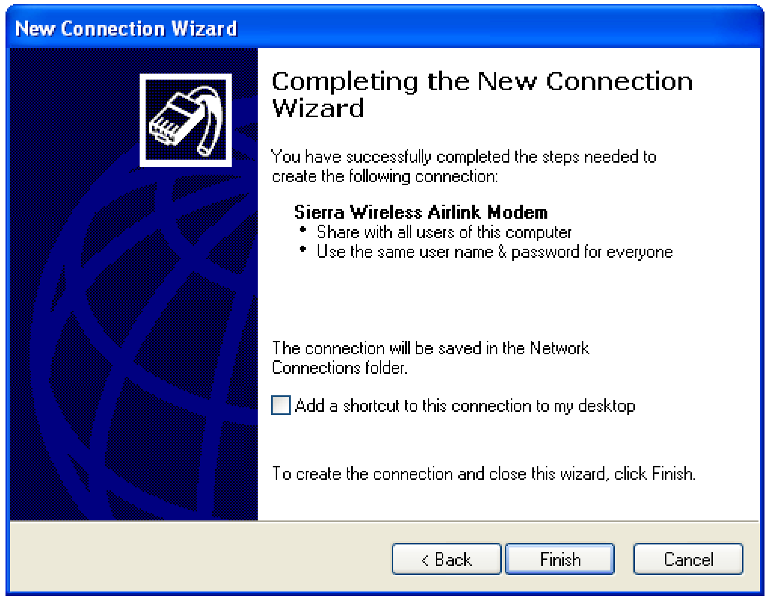


Figure 3-9: New Connection: Finish

2. Configure the PPPoE connection

After you complete the New Connection Wizard, there are a few more things you will want to configure in the connection.

a. Select *Properties*.

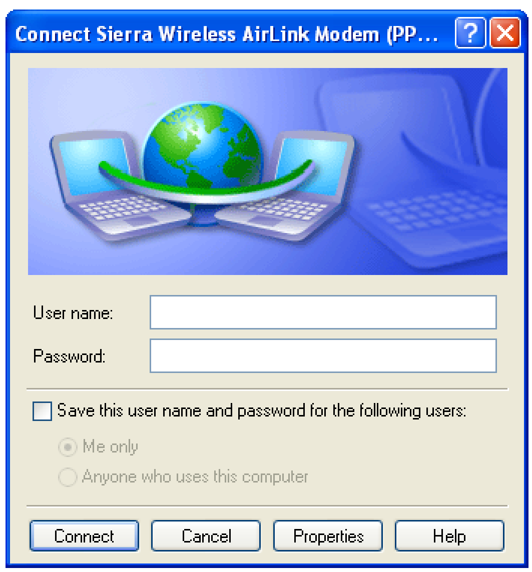


Figure 3-10: PPPoE Connection

b. *Optional:* On the General tab, if you gave the modem a name with *MODEMNAME above, you can type in that name as the Service Name.

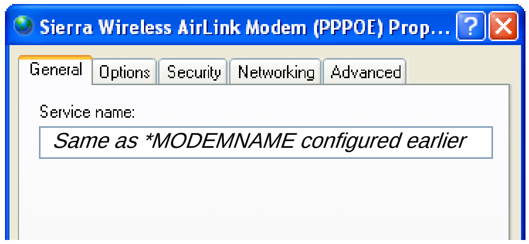


Figure 3-11: PPPoE Connection : Service Name

c. Select *Networking*.

d. Select *Settings*.

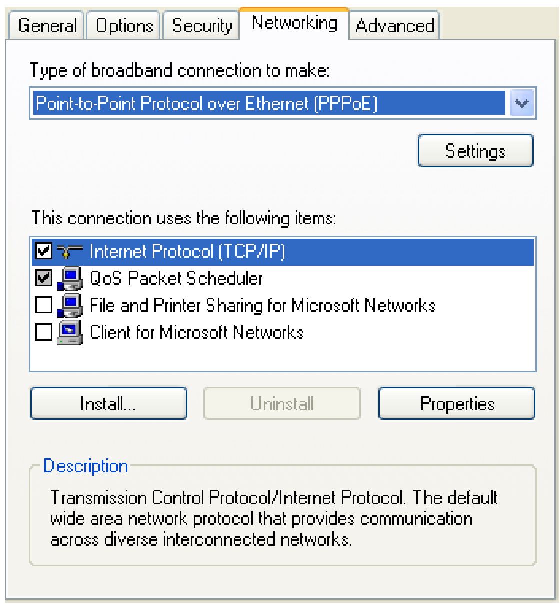


Figure 3-12: PPPoE : Networking

e. Remove the checks from all three PPP settings.

f. Select *OK*.

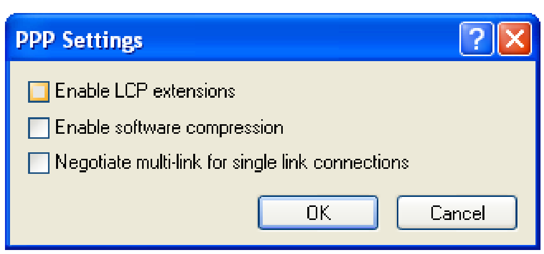


Figure 3-13: PPP Settings

Tip: *You may want to check the Options tab and change the settings for applications you might be using. The default options are generally applicable for most uses.*

Caution: *Unless specifically directed to do so by Support or your network administrator, you do not need to make any changes to the options on the Security tab.*

g. Select *OK* until you return to the *Connect* window.

Connecting to the Internet with PPPoE

Now the PPPoE connection can be run and a data connection can be established.

a. Connect your computer and the modem to the same local network using a hub or a switch.

Note: It is not recommended to connect your computer directly to the modem without a hub or switch.

b. Start the PPPoE by *Start* > *Connect To* > *Sierra Wireless AirLink Modem* (or whatever you named the connection). It will be listed on your Network Connections window under the heading Broadband.

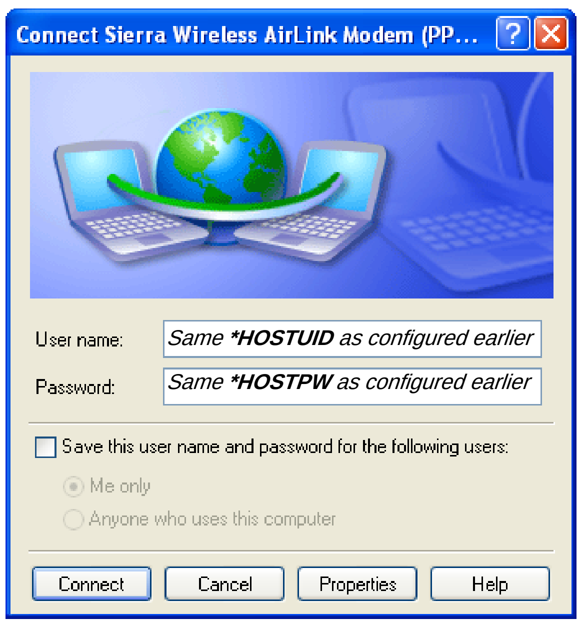


Figure 3-14: PPPoE Connection

c. Enter the User name and Password you configured for *HOSTUID and *HOSTPW earlier.

d. Select *Connect* to connect to the modem and the Internet.

When you're connected, an icon should appear in the System Tray, near the time display, showing the connection status.

D

D: SNMP : Simple Network Management Protocol

Management Information Base (MIB)

The management information base (MIB) is a type of database used to compile the information from the various SNMP agents. Reports from various agents, such as the AirLink device, are sent as data in form designed to be parsed by the NMS into its MIB. The data is hierarchical with entries addressed through object identifiers.

SNMP Traps

SNMP traps are alerts that can be sent from the managed device to the Network Management Station when an event happens. Your AirLink device is capable of sending the linkUp trap when the network connection becomes available.

Listening Port

*SNMPPORT sets the port for the SNMP agent to listen on. If set to zero, default, SNMP is disabled.

Tip: *SNMP generally uses port 161, however most Internet providers (including cellular) block all ports below 1024 as a security measure. You should be able to use a higher numbered port such as 10161.*

Security Level

*SNMPSECLVL sets the security level and which version of SNMP communications are used.

- **0** - No security required. SNMPv2c and SMNPv3 communications are allowed.
- **1** - Authentication required. SNMPv3 is required to do authentication and SNMPv2c transmissions will be silently discarded. Authentication is equivalent to the authNoPriv setting in SNMPv3.
- **2** - Authentication required and messages are encrypted. SNMPv3 is required to do authentication. SNMPv2c and SNMPv3 authNoPriv transmissions will be silently discarded. Authentication and encryption is equivalent to the authPriv setting in SNMPv3.

User Name and Password

The user name is '***user***'. The user name cannot be changed. The AirLink device's password is used as the SNMP password (default is '***12345***').

Tip: *The eight-character password requirement for SMNPv3 is not enforced by the PinPoint X Agent to allow the default password to function. Your SNMP administrator or MIS may require you to change to a more secure and/or longer password.*

To change the password in the AirLink device, go to Admin and change your ACEmanager password.

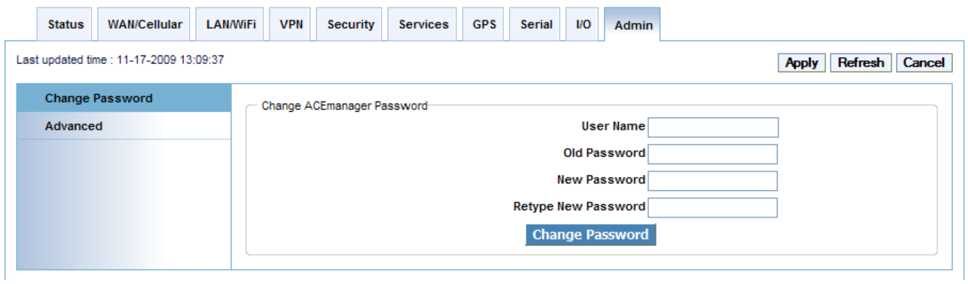


Figure 4-1: ACEmanager : Change Password menu option

For the password, you can use numbers, letters, and/or punctuation.

Caution: *The password is case sensitive. “drowssaP” is not the same as “drowssap”.*

Trap Destination

*SNMPTRAPDEST needs to be set with the destination IP and port. If either are set to zero or empty, SNMP traps are disabled.

Note: Traps are sent out according to the SNMP security level (i.e. if the security level is 2, traps will be authenticated and encrypted). Currently, the only trap supported is LinkUp.

Community String

The community string can be configured using *SNMPCOMMUNITY. The default is “public”.

SNMP MIB Definition Sample

```
AIRLINK-MIB DEFINITIONS ::= BEGIN

IMPORTS
ObjectName FROM SNMPv2-SMI
MODULE-COMPLIANCE FROM SNMPv2-CONF;
```

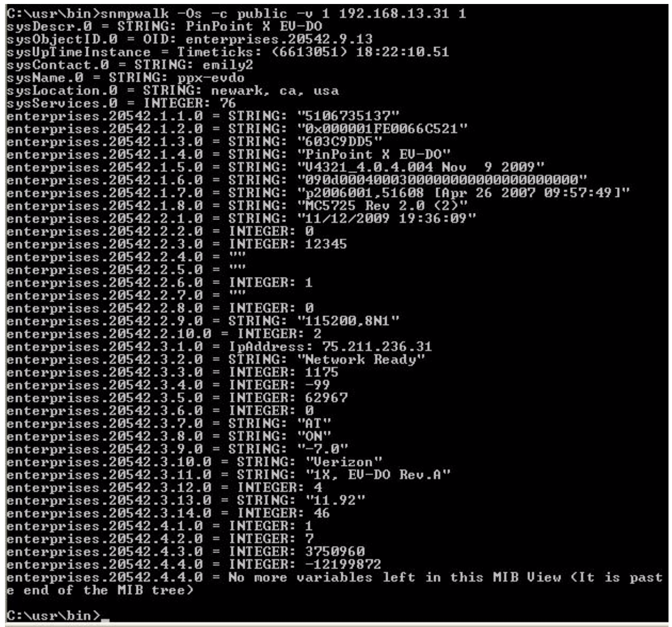
```
org OBJECT IDENTIFIER ::= { iso 3 }
dod OBJECT IDENTIFIER ::= { org 6 }
internet OBJECT IDENTIFIER ::= { dod 1 }
private OBJECT IDENTIFIER ::= { internet 4 }
enterprises OBJECT IDENTIFIER ::= { private 1 }

airlink OBJECT IDENTIFIER ::= { enterprises 20542 }
general OBJECT IDENTIFIER ::= { airlink 1 }
common OBJECT IDENTIFIER ::= { airlink 2 }
status OBJECT IDENTIFIER ::= { airlink 3 }
gps OBJECT IDENTIFIER ::= { airlink 4 }

-- GENERAL --
phoneNumber OBJECT-TYPE
SYNTAX DisplayString (SIZE (10))
MAX-ACCESS read-only
STATUS current
   ::= { general 1 }

deviceID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS  current
   ::= { general 2 }

electronicID OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS current
   ::= { general 3 }

modemType OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS read-only
STATUS current
   ::= { general 4 }

aleosSWVer OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS current
   ::= { general 5 }

aleosHWVer OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS  current
   ::= { general 6 }

modemSWVer OBJECT-TYPE
SYNTAX   DisplayString
```

```
MAX-ACCESS read-only
STATUS current
  ::= { general 7 }

modemHWVer OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS read-only
STATUS current
  ::= { general 8 }

-- COMMON --
date OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  ::= { common 1 }

otaProgrammingEnable OBJECT-TYPE
SYNTAX INTEGER {
disabled(0),
enabled(1) }
MAX-ACCESS read-only
STATUS current
  ::= { common 2 }

devicePort OBJECT-TYPE
SYNTAX INTEGER(0..65535)
MAX-ACCESS read-only
STATUS current
  ::= { common 3 }

netUID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS  current
  ::= { common 4 }

netPW OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  ::= { common 5 }

requestPAP OBJECT-TYPE
SYNTAX  INTEGER {
no(0),
yes(1) }
MAX-ACCESS read-only
STATUS current
  ::= { common 6 }

destinationAddress OBJECT-TYPE
```

```
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS  current
   ::= { common 7 }

destinationPort OBJECT-TYPE
SYNTAX   INTEGER(0..65535)
MAX-ACCESS  read-only
STATUS  current
   ::= { common 8 }

serialPortSettings OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS  current
   ::= { common 9 }

serialPortFlowControl OBJECT-TYPE
SYNTAX  INTEGER {
none(0),
hardware(2),
software(4) }
MAX-ACCESS  read-only
STATUS  current
   ::= { common 10 }

-- STATUS --
ipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS  read-only
STATUS  current
   ::= { status 1 }

netState OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS  read-only
STATUS  current
   ::= { status 2 }

netChannel OBJECT-TYPE
SYNTAX  INTEGER
MAX-ACCESS  read-only
STATUS  current
   ::= { status 3 }

rssi OBJECT-TYPE
SYNTAX   INTEGER(-125..-50)
MAX-ACCESS  read-only
STATUS current
    ::= { status 4 }

serialSent OBJECT-TYPE
```

```
SYNTAX  INTEGER
MAX-ACCESS  read-only
STATUS  current
   ::= { status 5 }

serialReceived OBJECT-TYPE
SYNTAX  INTEGER
MAX-ACCESS  read-only
STATUS   current
   ::= { status 6 }

hostMode OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS  current
   ::= { status 7 }

powerMode OBJECT-TYPE
SYNTAX   DisplayString
MAX-ACCESS  read-only
STATUS  current
   ::= { status 8 }

fixObtained OBJECT-TYPE
SYNTAX  INTEGER {
no(0),
yes(1) }
MAX-ACCESS  read-only
STATUS  current
   ::= { gps 1 }

satelliteCount OBJECT-TYPE
SYNTAX  INTEGER
MAX-ACCESS  read-only
STATUS current
::= { gps 2 }

latitude OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS  current
::= { gps 3 }

longitude OBJECT-TYPE
SYNTAX  DisplayString
MAX-ACCESS  read-only
STATUS  current
::= { gps 4 }

c:\usr\bin>snmpwalk -Os -c public -v 1 192.168.75.31 1
sysDescr.0 = STRING: PinPoint X HSUPA
sysObjectID.0 = OID: enterprises.20542.9.17
```

```
sysUpTimeInstance = Timeticks: (0) 0:00:00.00
enterprises.20542.1.1.0 = ""
enterprises.20542.1.2.0 = STRING: "0x01011A50FD74A5F1"
enterprises.20542.1.3.0 = STRING: "354220010245369"
enterprises.20542.1.4.0 = STRING: "PinPoint X HSUPA"
enterprises.20542.1.5.0 = STRING: "H4323_4.0.x.005 Oct  7 2009"
enterprises.20542.1.6.0 = STRING: "09110004000300000000000000000000"
enterprises.20542.1.7.0 = STRING: "F1_0_0_12AP C:/WS/FW/F1_0_0_12AP/
MSM7200R3/SR
C/AMSS 2008/01/01 14:18:44"
enterprises.20542.1.8.0 = STRING: "MC8781"
enterprises.20542.2.1.0 = STRING: "10/07/2009 20:55:33"
enterprises.20542.2.2.0 = INTEGER: 0
enterprises.20542.2.3.0 = INTEGER: 12345
enterprises.20542.2.4.0 = ""
enterprises.20542.2.5.0 = ""
enterprises.20542.2.6.0 = INTEGER: 1
enterprises.20542.2.7.0 = ""
enterprises.20542.2.8.0 = INTEGER: 0
enterprises.20542.2.9.0 = STRING: "115200,8N1"
enterprises.20542.2.10.0 = INTEGER: 2
enterprises.20542.3.1.0 = IpAddress: 0.0.0.0
enterprises.20542.3.2.0 = STRING: "Connecting To Network"
enterprises.20542.3.3.0 = INTEGER: 0
enterprises.20542.3.4.0 = INTEGER: -90
enterprises.20542.3.5.0 = INTEGER: 7708
enterprises.20542.3.6.0 = INTEGER: 0
enterprises.20542.3.7.0 = STRING: "AT"
enterprises.20542.3.8.0 = STRING: "INITIAL"
****  new ********
enterprises.20542.3.9.0 = STRING: "-10.0"
enterprises.20542.3.10.0 = STRING: "'AT&T', 310410"
enterprises.20542.3.11.0 = STRING: "HSPA"
enterprises.20542.3.12.0 = INTEGER: 151
enterprises.20542.3.13.0 = STRING: "14.94"
enterprises.20542.3.14.0 = INTEGER: 34
****  down to here  **********

enterprises.20542.4.1.0 = INTEGER: 0
enterprises.20542.4.2.0 = INTEGER: 0
enterprises.20542.4.3.0 = INTEGER: 0
enterprises.20542.4.4.0 = INTEGER: 0
enterprises.20542.4.4.0 = No more variables left in this MIB View (It is past th
e end of the MIB tree)

c:\usr\bin>


END
```



```
C:\usr\bin>snmpwalk -Os -c public -v 1 192.168.13.31 1
sysDescr.0 = STRING: PinPoint X EV-DO
sysObjectID.0 = OID: enterprises.20542.9.13
sysUpTimeInstance = Timeticks: (6613051) 18:22:10.51
sysContact.0 = STRING: emily2
sysName.0 = STRING: ppx-evdo
sysLocation.0 = STRING: newark, ca, usa
sysServices.0 = INTEGER: 76
enterprises.20542.1.1.0 = STRING: "5106735137"
enterprises.20542.1.2.0 = STRING: "0x000001FE0066C521"
enterprises.20542.1.3.0 = STRING: "603C9DD5"
enterprises.20542.1.4.0 = STRING: "PinPoint X EV-DO"
enterprises.20542.1.5.0 = STRING: "V4321_4.0.4.004 Nov  9 2009"
enterprises.20542.1.6.0 = STRING: "090d00040003000000000000000000000"
enterprises.20542.1.7.0 = STRING: "p2006001,51608 [Apr 26 2007 09:57:49]"
enterprises.20542.1.8.0 = STRING: "MC5725 Rev 2.0 (2)"
enterprises.20542.2.1.0 = STRING: "11/12/2009 19:36:09"
enterprises.20542.2.2.0 = INTEGER: 0
enterprises.20542.2.3.0 = INTEGER: 12345
enterprises.20542.2.4.0 = ""
enterprises.20542.2.5.0 = ""
enterprises.20542.2.6.0 = INTEGER: 1
enterprises.20542.2.7.0 = ""
enterprises.20542.2.8.0 = INTEGER: 0
enterprises.20542.2.9.0 = STRING: "115200,8N1"
enterprises.20542.2.10.0 = INTEGER: 2
enterprises.20542.3.1.0 = IpAddress: 75.211.236.31
enterprises.20542.3.2.0 = STRING: "Network Ready"
enterprises.20542.3.3.0 = INTEGER: 1175
enterprises.20542.3.4.0 = INTEGER: -99
enterprises.20542.3.5.0 = INTEGER: 62967
enterprises.20542.3.6.0 = INTEGER: 0
enterprises.20542.3.7.0 = STRING: "AT"
enterprises.20542.3.8.0 = STRING: "ON"
enterprises.20542.3.9.0 = STRING: "-7.0"
enterprises.20542.3.10.0 = STRING: "Verizon"
enterprises.20542.3.11.0 = STRING: "1X, EV-DO Rev.A"
enterprises.20542.3.12.0 = INTEGER: 4
enterprises.20542.3.13.0 = STRING: "11.92"
enterprises.20542.3.14.0 = INTEGER: 46
enterprises.20542.4.1.0 = INTEGER: 1
enterprises.20542.4.2.0 = INTEGER: 7
enterprises.20542.4.3.0 = INTEGER: 3750960
enterprises.20542.4.4.0 = INTEGER: -12199872
enterprises.20542.4.4.0 = No more variables left in this MIB View (It is past
e end of the MIB tree)

C:\usr\bin>_
```

Display Responses

The string that is displayed for these objects is the same display for the corresponding AT Command.

Object	AT Command
phoneNumber	*NETPHONE?
deviceID	*DEVICEID?
electronicID	I3
aleosSWVer	I1
aleosHWVer	I1
modemSWVer	I2
modemHWVer	I2
date	*DATE?
otaProgrammingEnable	OPRG?
devicePort	*DPORT?
netUID	*NETUID?
netPW	*NETPW?
requestPAP	*HOSTPAP?
destinationAddress	S53
destinationPort	S53

Object	AT Command
serialPortSettings	S23
serialPortFlowControl	\Q
ipAddress	*NETIP?
netState	*NETSTATE?
netChannel	*NETCHAN?
rssi	*NETRSSI?
hostMode	*HOSTMODE?
powerMode	*POWERMODE? *PinPoint line modems only*
fixObtained	*PinPoint line modems only*
satelliteCount	*PinPoint line modems only*
latitude	*PinPoint line modems only*
longitude	*PinPoint line modems only*
ecio	*+ECIO*
Operator	*+NETOP*
Network Service Type	*+NETSERV*
System Reboots	*Number of System Resets* *There is no corresponding AT command available. Check on ACEmanager - Admin - Advanced screen.*
Power In	**POWERIN*
Board Temp	**BOARDTEMP*

Product ID

Each modem type has a unique ID associated with it so you can more easily identify the modem from its type on your network.

E: Global Positioning System (GPS)

The AirLink device is equipped with a Global Positioning System receiver (GPS) to ascertain its position and track the movements of a vehicle or other devices which move. The AirLink device relays the information of its location as well as other data for use with tracking applications.

Tracking Applications used with Sierra Wireless PinPoint line modems:

- Air-Trak
- Track Your Truck
- Track Star
- DeLorme Street Atlas USA
- Microsoft Streets and Trips
- CompassCom
- Zoll Data
- and many more...

GPS Overview

The Global Positioning System (GPS) is a satellite navigation system used for determining a location and providing a highly accurate time reference almost anywhere on Earth. The US military refers to GPS as Navigation Signal Timing and Ranging Global Positioning System (NAVSTAR GPS).

GPS consists of a “constellation” of at least 24 satellites in 6 orbital planes. Each satellite circles the Earth twice every day at an altitude of 20,200 kilometers (12,600 miles). Each satellite is equipped with an atomic clock and constantly broadcasts the time, according to its own clock, along with administrative information including the orbital elements of its motion, as determined by ground-based observatories.

A GPS receiver, such as the AirLink device, requires signals from four or more satellites in order to determine its own latitude, longitude, and elevation. Using time synced to the satellite system, the receiver computes the distance to each satellite from the difference between local time and the time the satellite signals were sent (this distance is called psuedoorange). The locations of the satellites are decoded from their radio signals and a database internal to the receiver. This process yields the location of the receiver. Getting positioning information from fewer than four satellites, using imprecise time, using satellites too closely positioned together, or using satellites too close to the Earth's curve will yield inaccurate data.

The GPS data is then transmitted to a central location which uses a tracking application to compile information about location, movement rates, and other pertinent data.

Note: Depending on the location of the satellites in relation to the modem's location and how many signals are being received, the AirLink device may encounter "GPS drift". The AirLink device may report it is in a location a few feet from its actual location because it does not employ differential GPS.

AirLink device Supported Protocols

The AirLink device supports three different GPS reporting protocols.

Remote Access Protocol (RAP)

The Remote Access Protocol (RAP) is a proprietary binary message format developed by Sierra Wireless AirLink Solutions. RAP was originally designed to work specifically with AirLink Tracking System (ATS), but other 3rd party applications have been developed to take advantage of the RAP messaging format.

In the original RAP, a PinPoint line modem uses the UDP (User Datagram Protocol) to communicate with the host server.

In RAP-based AVL, each PinPoint line device sends its command status and responses to the Host server and the Host sends commands to one or more PinPoint line devices. For reliability, the Host expects each command to be acknowledged within a time-out period. If the acknowledgement packet (ACK) is not received within the time-out period, the Host will retransmit the command.

The RAP messages are in Hex and are referred to by their message ID. Reports can include GPS data alone, as well as GPS data with the date and time, radio frequency data, and state changes of I/O as well as sending reports based on power states.

Examples of tracking applications using RAP:

- Air-Trak
- TrackStar
- CompassCom
- Zoll Data
- HTE
- Spillman
- and others...

National Marine Electronics Association (NMEA)

National Marine Electronics Association (NMEA) is a protocol by which marine instruments and most GPS receivers can communicate with each other. NMEA defines the format of many different GPS message (sentence) types, which are intended for use by navigational equipment.

Example of a tracking application using NMEA:

- Microsoft Streets and Trips

Tip: *For more information on the AirLink device supported NMEA message formats, please refer to the Appendix.*

Trimble ASCII Interface Protocol (TAIP)

Trimble ASCII Interface Protocol (TAIP) is a digital communication interface based on printable ASCII characters over a serial data link. TAIP was designed specifically for vehicle tracking applications but has become common in a number of other applications, such as data terminals and portable computers, because of its ease of use.

Example of a tracking application using TAIP:

- DeLorme Street Atlas USA

Tip: *For more information on TAIP message formats, refer to the Appendix and to the Sierra Wireless MP 3G Modem TAIP Reference.*

Datum

The GPS datum is the method of ascertaining the position of the GPS device using a specific reference point location. The datum used can influence the accuracy of the GPS positioning.

In addition to different reporting protocols, the AirLink device supports the most widely used GPS datum:

- WGS84
- NAD83
- NAD27

Before you Configure GPS

To decide what configuration you need for your AirLink device, there are some fundamental considerations you should determine:

- **Protocol:** What is the GPS protocol used by your tracking application and what type of reports will you need?
- **Datum:** What is the datum supported by your tracking application?
- **Dynamic IP Address:** Will you need DNS support to handle a dynamic IP address account?

Configuring the AirLink device for GPS

This section covers general configuration. Configurations for specific protocols are covered in later sections.

To configure your modem's GPS settings, you can use either ACEmanager or a terminal connection to configure the modem using AT commands. The configuration examples in this chapter all use ACEmanager. Most of the settings are in the group: *PinPoint*.

Tip: *You can use a fully qualified domain name instead of an IP address for most configuration options calling for an IP address if your AirLink device is configured to use DNS. Refer to the IP Manager chapter for how to configure DNS and how to allow your AirLink device use a domain name even with a dynamic IP address account from your cellular provider.*

Real-Time Clock Synchronization

Every hour, the AirLink devicet will sync the internal Real Time Clock (RTC) with the Universal Time Coordinated (UTC) received from the GPS satellites.

Many tracking applications will translate the time reported by the AirLink device as part of the GPS message to the appropriate local time zone using the UTC offset (i.e. California is UTC-8 and New York is UTC-5).

Tip: *ACEmanager displays the current time (UTC) set in the AirLink device and does not translate it to the local time zone. If the AirLink device is in California and it is 8 a.m., the modem's time will be shown as 4 p.m, since UTC is 8 hours "ahead" of Pacific time (UTC-8).*

Configuring the Datum

You can change the Datum used by your AirLink device by configuring *PPGPSDATUM. Match the Datum to the Datum used by your tracking application.

Over-The-Air (Remote) Host

To set the AirLink device to report to an external or remote host, configure *PPIP (ATS Server IP) and *PPPORT (Server Port). *PPIP will work with any remote host.

Local Host

To set the AirLink device to report to a local host, one directly connected to the serial port, configure the port to be used with S53 - Destination Port. The local IP address will automatically be used for local reports. *S53*, in ACEmanager, is part of the *GPS* group.

If you need to send reports to additional local ports, you can specify other ports with **PPLATSEXTRA*. Local Reports can be sent to up to 7 additional ports consecutively following the S53 port. If S53=1000 and *PPLATSEXTRA=4, reports will be sent to 1000, 1001, 1002, 1003, and 1004. In PPLATSEXTRA, specify the number of ports where you want the reports sent, 0 to 7 (0 disables extra ports).

TCP GPS Report Polling

The AirLink device can easily and quickly be polled for location by opening a TCP connection to port 9494 (default). Once the connection is established, the AirLink device will send a report with the current position using the GPS report type the modem is configured to use.

You can change the port for the TCP GPS poll using **PPTCPPOLL*.

Note: Some Internet providers (including cellular) block ports below 1024.

Report Types

There are several report types available. For remote reports, set **PPGPSR*. For local reports, set **PPLATSR*.

- **0** - *MF, Legacy reports for use with ATS version 4 and older.
- **11** - Global Positioning System (GPS) data.
- **12** - GPS data with the UTC time and date.
- **13** - GPS with time and date and Radio Frequency data from the antenna.
- **D0** - Xora reports.
- **E0** - NMEA GGA and VTG sentences.
- **E1** - NMEA GGA, RMC, and VTG sentences.
- **F0** - TAIP data
- **F1** - TAIP compact data

Tip: *The AirLink device can be configured to supply one type of report to a remote host and a different report type locally through the serial port at same time. However, there may be conflicts due to the local and remote reporting being in different modes and not all features to both modes may be available.*

Sending Reports Automatically

Remote

You can configure the AirLink device to send reports based on a time interval and on the movement of a vehicle (based on it's position from one time to the next).

- ***PPTIME** - Location report sent every set time interval (seconds).
- ***PPDIST** - Location report sent only if the position is more than the set distance (x 100 meters).
- ***PPTSV** - Location report sent if the vehicle has been in one location (stationary) for more than a set time interval (minutes).
- ***PPMINTIME** - Location report sent be sent at no less than this time interval (seconds).

Note: If you're implementing both a time interval and distance interval for reports, the AirLink device will use the timer which expires first. The reporting interval can impact your data usage. If the interval is set frequently, you may want to have a high usage or unlimited data plan.

Tip: *One mile is approximately 1600 meters. 1000 meters is one kilometer.*

Local

If you are sending reports on the local serial port, and/or if you want them sent automatically, you will need to set **PPLATS*. The time interval, just as for *PPTIME, is in seconds.

Report Delay on Power-Up

The AirLink device can be configured to wait a specific amount of time after initialization before any reports are sent. Configure *#IG* for the desired wait in seconds.

Store and Forward

Store and Forward can provide seamless coverage even in areas with intermittent cellular coverage. If the AirLink device leaves coverage or has very low signal (an RSSI of -105 or lower), it will store the GPS messages in memory. When the modem re-enters cellular coverage, it will then forward the messages as configured. The AirLink device can also store messages and send them to the server in a packet rather than individually to conserve bandwidth.

Enable Store and Forward using **PPSNF*. You can also determine how you want the messages sent using **PPSNFB* and **PPSNFM*.

- **Normal** - Each report is sent immediately.
- **Polled** - Reports held until requested by the server.

- **Grouped** - Reports held until the total is equal or greater than **PPSNFM* which sets the packet size of grouped reports.

Store and Forward Reliable Mode

The Store and Forward Reliable Mode allows the AirLink device to ensure all messages are received by the server even if the connection between them goes down for a period of time (such when a vehicle passes through a location where the cellular signal is weak or non-existent).

With Reliable Mode, **PPSNFR*, enabled, the AirLink device will transmit a sequence number (1 to 127) as part of a packet of messages (may contain one or more reports). To reduce overhead, the server only acknowledges receipt of every eighth packet. The AirLink device considers that 8 a “window” of outstanding packets.

If the AirLink device doesn’t receive acknowledgement for a “window”, the modem will PING the server with a message containing the sequence numbers of the first and last packets that haven’t been acknowledged. The AirLink device will continue until the server acknowledges receipt. When the AirLink device receives the acknowledgement, it will advance its “window” to the next group.

When the AirLink device is first powered on (or reset), it will send a Set Window message to sync up with the server for the current “window”.

On the other side, if the server receives an out of sequence packet, it will send a message to the modem noting the missing sequence and the AirLink device will retransmit.

Simple Reliable Mode will ‘give up’ after a configured number, **PPMAXRETRIES*, of attempts and discard messages that cannot be transmitted or received after that number of tries.

Sending Reports Based on an Interval

You can configure the AirLink device to send reports based on a time interval and/or on the movement of a vehicle (based on it’s position from one time to the next).

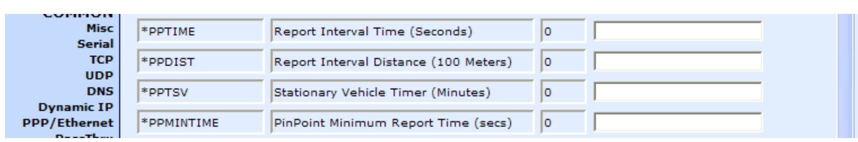


*Figure 5-1: ACEmanager : *PPTIME, *PPDIST, *PPTSV, *PPMINTIME*

- ***PPTIME** - Location report sent every set time interval (seconds).
- ***PPDIST** - Location report sent only if the position is more than the set distance (x 100 meters)
- ***PPTSV** - Location report sent if the vehicle has been in one location (stationary) for more than a set time interval (minutes).
- ***PPMINTIME** - Location report sent at no less than this time interval (seconds).

Flush on Event

If you have events enabled, with **PPFLUSHONEVT*, you can configure the AirLink device to flush the SnF buffer when an event occurs. This will immediately send all pending SnF messages to the host. This allows an event, such as a vehicle being powered on or a tow bar activated, to be immediately sent, so its cause can be acted on without delay.

Note: Outstanding packets can include messages already sent to the server that haven't been acknowledged (SnF Reliable Mode) whether they have been received by the server or not.

RAP Configuration

RAP has additional features which allow reports based on external physical events, input from a 3rd party devices, store and forward processing, etc.

In addition to being able to configure your AirLink device using ACEmanager or AT commands, most of the configuration settings for RAP can also be changed with the RAP configuration command message sent by the AVL host.

RAP Reports Over-The-Air (Remote)

To configure your AirLink device to send RAP reports to a remote AVL host server, you will need to set 3 commands: **PPIP*, **PPPORT*, and **PPGPSR*.

a. Set the IP address of the host with **PPIP* and desired port on the host with **PPPORT*.

b. Set the GPS Report Type, using **PPGPSR*, to your preferred RAP report type.

11 - GPS - Global Positioning System data

12 - GPS + Date - GPS data with the UTC time and date

13 - GPS + Date + RF - GPS data with the UTC time and date and Radio Frequency information from the antenna.

Tip: *If your AVL host server uses a dynamic IP address or needs to change its IP address for any reason, you can use the RAP configuration command to change the value for *PPIP.*

RAP Reports over a Local Connection

Local reports are sent to the local IP address of the computer or device connected directly to a port on the AirLink device. The reports are sent using PPP or SLIP for serial or USB virtual serial. To configure the modem to send reports to the local IP address, you will need to set 3 commands: *S53* in the GPS group and **PPLATS* and **PPLATSR* in the PinPoint group.

a. Set the *S53* port to the local port to which you want the reports sent. The local IP address will automatically be used.

b. Set the Local Report Type, using **PPLATSR*, to your preferred RAP report type.

11 - GPS - Global Positioning System data

12 - GPS + Date - GPS data with the UTC time and date

13 - GPS + Date + RF - GPS data with the UTC time and date and Radio Frequency information from the antenna.

c. Set Local Reporting Time Interval, using **PPLATS*, to the number of seconds you want as an interval between reports being sent.

Tip: *If *PPLATS is set to 0, reports will only be sent if a poll command is issued by the local client.*

Configuring Additional RAP Features

RAP allows additional information to be sent with the reports to enable a richer tracking feature set.

Device ID

By enabling **PPDEVID*, a device ID of the AirLink device is sent as part of the RAP message to make identification easier in a network or fleet of vehicles equipped with PinPoint line devices.

With *PPDEVID enabled, the AirLink device will use the value configured for **NETPHONE* for the device ID. If *NETPHONE is empty, the ESN of the modem will be used.

Tip: *If the AirLink device is using a dynamic IP, *PPDEVID needs to be enabled.*

Odometer Data in Reports

When the odometer report is enabled, the AirLink device will calculate distance between reports based on GPS data. The modem’s odometer calculations can be included in the RAP message.

- **PPODOM* enables the odometer reporting.
- **PPODOMVAL* is the current odometer reading in the AirLink device. You can set this to a number to offset the odometer calculation, such as one-time manual synchronization of the AirLink device odometer with the current vehicle odometer.

Note: The odometer calculations of the AirLink device may not match the odometer in the vehicle itself. The AirLink device odometer is not connected to the vehicle’s, it is entirely based on calculations of GPS readings.

I/O Event Reports

You can configure the AirLink device to send reports to the AVL Host based on the state of the digital inputs, analogue inputs, and relay outputs.

Tip: *Setting up the I/O port hardware is covered in the Inputs, Relay Outputs, and Power Status chapter.*

Enable *PPINPUTEVT to have events sent to the Host server.

COM 1000 support

Support for a COM1000 is enable with the command *PPCOM1000=1 or *PPREPORTINPUTS=1. Once enabled, ALEOS will receive the reports from a properly configured COM1000 and add the state of the extra inputs to RAP packets sent to the RAP Host.

If you are replacing an existing Pinpoint or PinPoint-E in a vehicle with a COM1000, simply replace earlier modem with the with the PinPoint. Turn on COM1000 reporting with the command *PPCOM1000=1 to allow a seamless transition with no need to change any commands to support the COM1000 in the same operation as the previous installation.

If you have a new vehicle installations for the PinPoint and have previously installed Pinpoints or PinPoint-E modems plus COMM1000 in other vehicles, connect the inputs directly to the PinPoint and turn on input reporting with the command *PPREPORTINPUTS=1. Since the PinPoint inputs report using the exact same bit fields as the COM1000, no changes to your software should be required.

Caution: *If both *PPCOM1000 and *PPREPORTINPUTS are enabled, the AirLink device digital inputs will be reported and the COM1000 inputs will be ignored.*

The report type will indicate the state of change in the inputs. The contents of the report will be the same as Report Type 0x12 (GPS data with date) or 0x13 (GPS data with date and RF data) with the addition of the event report.

Flush on Event

If you have Store and Forward configured and enabled, to receive event reports immediately when they occur, you will want to enable **PPFLUSHONEVT*. This will cause all pending reports, including the triggering event, to be sent immediately to the Host.

NMEA Configuration

Messages Over-The-Air (Remote)

To configure the AirLink device to send NMEA reports to a remote server, you will need to set 3 commands: *PPIP, *PPPORT, and *PPGPSR.

a. Set **PPIP* and **PPPORT* to the IP address and port of the server to which you want the reports sent.

b. Set the GPS Report Type (*PPGPSR) to your preferred NMEA sentence format.

- **E0** - NMEA GGA and VTG sentences.
- **E1** - NMEA GGA, RMC, and VTG sentences.

Local Host

Local reports are sent to the local IP address of the computer or device connected to the serial port or USB port of the AirLink device using PPP. To configure the modem to send to the local IP, you will need to set 3 commands: *S53, *PPLATS, and *PPLATSR.

a. Set the port (S53) to the local port to which you want the reports sent. The local IP address will automatically be used. *S53*, in ACEmanager, is part of the *GPS* group.

b. Set the Local Report Type, **PPLATSR*, to your preferred NMEA sentence format.

- **E0** - NMEA GGA and VTG sentences.
- **E1** - NMEA GGA, RMC, and VTG sentences.

c. Set Local Reporting Time Interval, using **PPLATS*, to the number of seconds you want as an interval between reports being sent.

Streaming Messages (Local)

The AirLink device can be configured to send standard NMEA messages (sentences) in ASCII over the serial port and/or USB port without a PPP connection to the local computer.

Send the command *ATGPS1* to the serial port, *ATGPS2* to the USB port, or *ATGPS3* for both to begin the NMEA stream. The example below shows the stream in HyperTerminal connecting directly to a AirLink device via the comport and/or USB port. To stop the stream, with either terminal connection, use the command *ATGPS0* (this can be entered even while data is streaming).

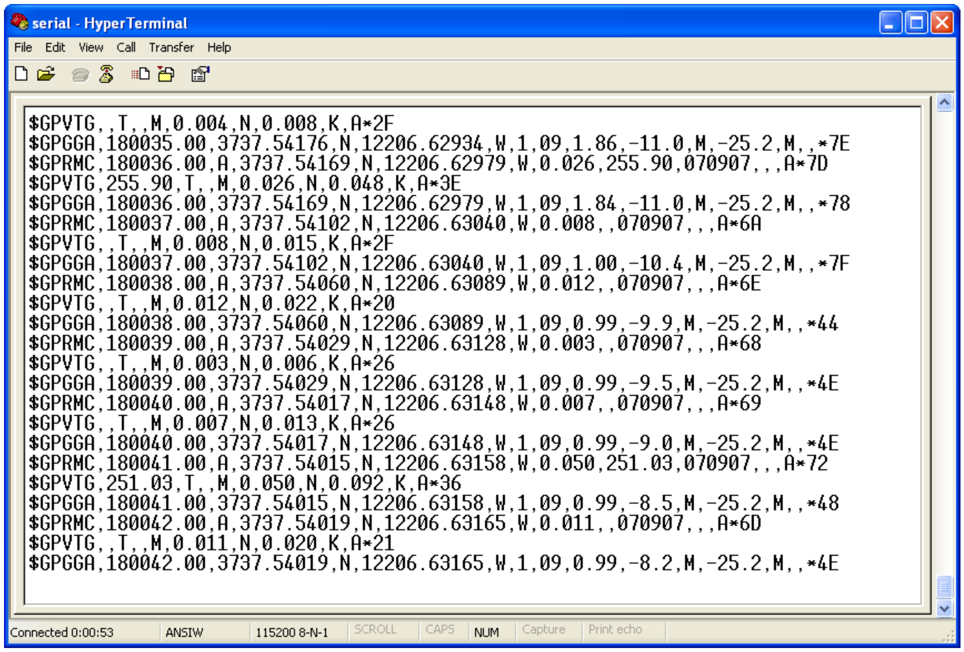


Figure 5-2: HyperTerminal : NMEA Streaming

Persistent Streaming

To have persistent streaming, allowing you to stream the data even after the modem is reset, configure **PGPS* and set **PGPSR* for NMEA.

- **0** - Disable NMEA streaming.
- **1** - Stream the NMEA strings out the serial port only.
- **2** - Stream the NMEA strings out the USB port only.
- **3** - Stream the NMEA strings out both the serial and the USB ports.
- **E1** - NMEA GGA, RMC, and VTG sentences.

TAIP Emulation Configuration

The TAIP emulation functionality allows the AirLink device to operate in a limited manner with clients which only understand the Trimble ASCII Interface Protocol (TAIP).This emulation is enabled by setting the GPS report format, directing the modem to listen for TAIP messages, and disabling RAP formatted messages to the same interface.

TAIP ID

TAIP messages can be configured to send the user specified identification number (ID). This greatly enhances the functional capability of the unit in a network environment. Set the ID using **PPTAIPID*.

TAIP Command Emulation

With TAIP emulation, the AirLink device will listen for TAIP messages on port 21000. Set the GPS Report Type, **PPGPSR*, to your preferred TAIP data format.

- **F0** - TAIP data (LN): latitude, longitude, altitude, the horizontal and vertical speed, and heading.
- **F1** - Compact TAIP data (PV): latitude/longitude, speed, and heading.

Caution: *When TAIP emulation is enabled, RAP will be disabled and no RAP messages or commands will be sent or received on that port.*

Supported TAIP Commands

The TAIP emulation will accept the following TAIP message types:

- **SRM** (Set Reporting Mode) allows the client to set the reporting mode configuration. The report mode configuration is not stored in non-volatile memory and such should be resent upon a unit reset. This behavior emulates that specified in TAIP specifications.
- **QRM** (Query Reporting Mode) reports the reporting mode configuration (returns an “RRM” message).
- **SID** (Set ID) allows the client to set the TAIP ID (AT*PPTAIPID can also be used to set the TAIP ID). The TAIP ID, when set with a “SID” message, will be written to non-volatile memory.
- **QID** (Query ID) reports the TAIP ID (returns an “RID” message).
- **DPV** configures automatic reporting of PV (Position/Velocity) reports based on distance traveled and a maximum time. The delta distance value specified in the message is converted to hundreds of meters and stored as *PPDIST. The maximum time interval is stored as *PPTIME. Currently the minimum time and epoch values are ignored.
- **FPV** configures periodic reporting of PV (Position/Velocity) reports. The time interval from the message is stored at *PPTIME. Currently the epoch value is ignored.

- **QPV** (Query Position Velocity) responds with a PV (Position/Velocity) report.

The TAIP emulation will generate the following reports corresponding to the appropriate event (either a query for it, echoed due to a set, or due to an automatic reporting event):

- **RRM** (Report Reporting Mode) reports the reporting mode configuration.
- **RID** (Report ID) reports the TAIP ID.
- **RPV** (Report Position/Velocity) reports Position/Velocity.

Messages Over-the-Air (Remote)

To configure the AirLink device to send NMEA reports to a remote server, you will need to set 3 commands: *PPIP, *PPPORT, and *PPGPSR.

a. Set **PPIP* and **PPPORT* to the IP address and port of the server to which you want the reports sent.

*Note: Unlike standard TAIP which simply sends to the last client to request automatic reports, the remote reports are sent to the destination address (*PPIP) and destination port (*PPPORT).*

b. Set the GPS Report Type, **PPGPSR*, to your preferred TAIP data format.

- **F0** - TAIP data (LN): latitude, longitude, altitude, the horizontal and vertical speed, and heading.
- **F1** - Compact TAIP data (PV): latitude/longitude, speed, and heading.

Local Connection

Some TAIP client applications can send TAIP requests and listen for reports using a local connection. Generally this is done over the serial port using PPP. This can also be done over the USB virtual serial port using PPP.

The AirLink device will listen for TAIP requests on the local IP address and port. Once a TAIP request command has been received, the AirLink devicet will begin issuing TAIP reports to the local IP address and port 21000. The client application should be listening for reports on this IP address and port. No unsolicited reports will be sent from the PinPoint to the local client application.

To configure this local TAIP reporting, you will need to set four commands: *PPIP, S53, *PPGPSR, and *PPLATS.

a. Set the port (S53) to the local port to which you want the reports sent, 21000 is the common setting. *S53*, in ACEmanager, is part of the *GPS* group.

b. Set **PPIP* to the local IP address of the AirLink device. The default IP address of the AirLink device 192.168.14.31.

c. Set Local Reporting Time Interval, using **PPLATS*, to the number of seconds you want as an interval between reports being sent.

d. Set the GPS Report Type, **PPGPSR*, to your preferred TAIP data format.

- **F0** - TAIP data (LN): latitude, longitude, altitude, the horizontal and vertical speed, and heading.

- **F1** - Compact TAIP data (PV): latitude/longitude, speed, and heading.

Sending Unsolicited TAIP Messages over the Local Connection

Standard TAIP requires a request before GPS reports are sent. The AirLink device, however, can be configured to allow TAIP formatted messages to be sent over any UDP Port without request commands. This is useful for those applications which can listen for TAIP messages but cannot send UDP request packets.

a. Set the *S53* port to **1000**. The local IP address will automatically be used.

b. Set **PPLATSR*, Local Report Type, to **F0** or **F1**.

c. Set **PPLATS,* Local Reporting Time Interval, to **5** to send reports every 5 seconds (can be adjusted as circumstances warrant).

d.

Streaming Messages (Local)

The Product Name can be configured to send standard TAIP messages (sentences) in ASCII over the serial port and/or USB port without a PPP connection to the local computer.

Send the command ATGPS1 to the serial port, ATGPS2 to the USB port, or ATGPS3 for both to begin the TAIP stream. The example below shows the stream in HyperTerminal connecting directly to a Product Name via the comport and/or USB port. To stop the stream, with either terminal connection, use the command ATGPS0 (this can be entered even while data is streaming).

Persistent Streaming

To have persistent streaming, allowing you to stream the data even after the modem is reset, configure *PGPS and set *PGPSR for TAIP.

Avoir couler persistant, te permettant de couler les données même après que le modem est remis à zéro, configurent le *PGPS et *PGPSR.

- *PGPS

0 - Disable TAIP streaming.

1 - Stream the TAIP strings out the serial port only.

2 - Stream the TAIP strings out the USB port only.

3 - Stream the TAIP strings out both the serial and the USB ports.

0 - Neutralisez couler de TAIP.

1 - Coulent les cordes de TAIP hors de la porte série seulement.

2 - Coulent les cordes de TAIP hors du port d’USB seulement.

3 - Coulent les cordes de TAIP hors de la porte série et du port d’USB.

E1 - TAIP GGA, RMC, and VTG sentences.

E1 - Phrases TAIP GGA, RMC et VTG.

F: AT Commands

- AT command set summary
- Reference tables
- Status registers
- Stored profile settings

AT command set summary

The reference tables are presented in strict ASCII alphabetical order (including prefixes). This format allows quick look-up of each command to verify syntax, parameters, and behaviors. It does *not* lend itself to finding whether or not the AirLink Device has a command to perform a particular service or setting.

The summary in this section organizes the commands into functional groups to allow you to more quickly locate a desired command when you know the operation but not the command.

Reference tables

Result codes are not shown in the command tables unless special conditions apply. Generally the result code OK is returned when the command has been executed. ERROR may be returned if parameters are out of range, and is returned if the command is not recognized or is not permitted in the current state or condition of the AirLink Device.

Info

The commands in the “Info” group have read-only parameters. They only provide information about the device. The commands displayed in ACEmanager and the results of those commands depends on the model of the device. The commands in the “Info” group have read-only parameters. They only provide information about the device.

Table 6-1: Info Commands

Command	Description
***ETHMAC?**	The MAC address of the Ethernet port.
***NETPHONE?**	The device's phone number, if applicable or obtainable.
***DEVICEID?**	The commands displayed in AceManager and the results of those commands depends on the model of the device. The 64-bit device ID the device uses to identify itself to the cellular network.

Table 6-1: Info Commands (Continued)

Command	Description
***ETHMAC?**	The MAC address of the Ethernet port.
***I1**	ALEOS Software Version

Status

Most of the commands in the “Status” group have read-only parameters and provide information about the device. Most of the commands in the “Status” group have read-only parameters and provide information about the device. The Status Group has more fields that can be displayed on most screens. You can either resize your window or use the scroll bar on the side to display the remainder.

Table 6-2: Status: Network

Command	Description
***NETIP?**	The current IP address of the device reported by the internal module, generally obtained from Carrier your cellular carrier. This is the address that can contact the device from the Internet. Use *NETALLOWZEROIP if you need to allow the display of an IP ending in a zero. *Note: If there is no current network IP address, 0.0.0.0 may be displayed.*
***NETRSSI?**	The current RSSI (Receive Signal Strength Indicator) of the AirLink device as a negative dBm value. **Tip:** *The same information is displayed with the command S202?.*

Table 6-2: Status: Network

Command	Description
*NETSTATE?	The current network state: • Connecting To Network: The device is in the process of trying to connect to the cellular network. • Network Authentication Fail: Authentication to the cellular network has failed. Verify settings to activate the device. Data Connection Failed: The device failed to connect, and it is now waiting a set time interval before it attempts to reconnect. Verify settings to activate the device. • Network Negotiation Fail: Network connection negotiation failed. This is usually temporary and often clears up during a subsequent attempt. • Network Ready: The device is connected to the 1x cellular network and ready to send data. • Network Dormant: The MP is connected to the 1x cellular network, but the link is dormant. It will be woken up when data is sent or received. • No Service: There is no cellular network detected. • Hardware Reset: The internal module is being reset. This is a temporary state.
*NETCHAN?	The current active CDMA/GSM channel number.
*HOSTMODE?	The current host mode (AT, PPP, UDP, etc.). If the device is not in AT mode, telnet into the device to execute this command.
*NETERR?	The EVDO or CDMA network frame error rate. The EDGE or GPRS network bit error rate. The network frame for CDMA or EV-DO or bit error rate for EDGE or GPRS.
*NETSERV?	The type of service being used by the device, for example Tech EV-DO Rev A or HSDPA.

GPRS Info

Table 6-3: Status: GPRS Info

Command	Description
*NETOP	The current cellular carrier from the device's firmware.
	Subscriber Identity Module ID. GPRS or EDGE Only.
+CIMI	Subscriber Identity Module ID.
	Current Cell Info Information. GPRS or EDGE Only.

CDMA Info

Table 6-4: Status: CDMA Info

Command	Description
+PRL	Preferred Roaming List (PRL) version. CDMA or EV-DO Only.
***PRLSTATUS**	The status of the most recent PRL Update. *CDMA or EV-DO Only.* • **0** : None • **1** : In Progress • **2** : Success • **Any other value** : Failure .
CDMA ECIO	Indicates the signal-to-noise ratio, essentially the quality of the signal.

CPU Status

Table 6-5: Status: CPU Status

Command	Description
***POWERIN**	The voltage input to the internal hardware.
***BoardTemp**	The temperature, in Celsius, of the internal hardware.
***POWERMODE**	Displays the current power state/mode. Possible values returned are: • Initial: The device is in the initial 5 minutes since power up, so power down event will be ignored. • On: Regular power on, a power down is not pending. • Low Cancellable: Power down is pending but still cancelable if the power down trigger goes away. • Low Pending 1 and Low Pending 2: Power down is pending, any device tasks are gracefully preparing for the power down. • Low Final: Power down is imminent. • Low: Power is down.

Common

The groups under the heading Common encompass those commands that are common to most Sierra Wireless AirLink devices. The Groups shown will depend entirely on the model of device.

Misc

Table 6-6: Common: Misc

Command	Description
General	
***DATE**	Sets and queries the internal clock. Either the date and time can be specified, or simply one of the two can be specified in which case the unspecified value will remain unchanged. The date and time are always specified 24-hour notation. mm/dd/yyyy=date in month/day/year notation hh:mm:ss=time in 24-hour notation *Note: In AirLink devices, the GPS will be used to set the time, in which case any date/time specified by this command will be ignored.*
***OPRG**	Enables/disables over-the-air firmware upgrading of the MP. When Sierra Wireless releases a new version of ALEOS, you can upgrade your remote devices with OPRG enabled. • n=0 : Disables • n=1 : Enables
***DPORT**	The device's Device Port which the device is listening on for inbound packets/data/polls. Can also be set with the command S110. • n=1-65535
***NETUID**	Network User ID The login that is used to login to the cellular network, when required. • uid=user id (up to 64 bytes)
***NETPW**	Network Password The password that is used to login to the cellular network, when required. • pw=password (30 characters maximum)

Table 6-6: Common: Misc

S53	This AT Command applies to: • Destination Address • Destination Port • Default Dial Code Destination IP address, port, and method. These are used as defaults for the D (Dial) AT command. • method= P : UDP • method=T : TCP • method=N : Telnet • d.d.d.d=IP address or domain name • ppppp=the port address Examples: **ATS53=T192.168.100.23/12345** **ATS53=foo.earlink.com** Telnet to the specified IP at port 12345. **ATS53=192.168.100.23/12345** Query the specified IP at port 12345. **ATS53=/12345** Query port 12345.
***NETALLOWZEROIP**	Allow Last Byte of net IP = Zero Allows the displayed IP address in *NETIP to end in zero (ex. 192.168.1.0). • n=0 : Do not allow. • n=1 : Allow.
***NETPHONE?**	Phone Number The device’s phone number, if applicable or obtainable.
***HOSTPAP**	Request PAP Use PAP to request the user login and password during PPP negotiation on the host connection. n=0 : Disable PAP request (Default). n=1 : Takes user login and password from Windows DUN connection and copies to *NETUID and *NETPW.

USB

Table 6-7: Common: USB

Command	Description
USB Device Mode	*USBDEVICE=n This parameter alters the default startup data mode.

Serial

Table 6-8: Common: Serial

Command	Description
***S23**	Configure Serial Port Format: [speed],[data bits][parity][stop bits] Valid speeds are 300-115200, data bits: 7 or 8, parity: O,E,N,M, stop bits: 1,1.5,2
\Q	Serial Port Flow Control Set or query the serial port flow control setting. • **n=0** : No flow control is being used. • **n=1** : RTS/CTS hardware flow control is being used. • **n=4** : Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@. Set or query the serial port flow control setting. • n=0 : No flow control is being used. • n=1 : RTS/CTS hardware flow control is being used. • n=4 : Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@.
V	Command Response Mode. • n=0 : Terse (numeric) command responses • n=1 : Verbose command responses (Default).
&D	Set DTR mode. n=0 : Ignore DTR, same effect as HW DTR always asserted (same as S211=1). n=2 : Use hardware DTR (same as S211=0).
S211	For applications or situations where hardware control of the DTR signal is not possible, the device can be configured to ignore DTR. When Ignore DTR is enabled, the device operates as if the DTR signal is always asserted. • n=0 : Use hardware DTR. (default). • n=1 : Ignore DTR. • n=3 : Ignore DTR and assert DSR. This value is deprecated, and it is recommended to use &S to control the DSR instead. When this value is set to 3, &S will automatically be set to 0. See also: &D and &S.
Q	The AT quiet-mode setting. If quiet mode is set, there will be no responses to AT commands except for data queried. • n=0 : Off (Default). • n=1 : Quiet-mode on.
S50	Data forwarding idle time-out. If set to 0, a forwarding time-out of 10ms is used. Used in UDP or TCP PAD mode. • n=tenths of a second

Table 6-8: Common: Serial

Command	Description
S51	PAD data forwarding character. ASCII code of character that will cause data to be forwarded. Used in UDP or TCP PAD mode. • n=0 : No forwarding character.
E	Toggle AT command echo mode. • n=0 : Echo Off. • n=1 : Echo On. With more than one connection types (serial, and Telnet, and USB) the echo command can be set differently on each interface.
&S	Set DSR mode. • n=0 : Always assert DSR (Default). • n=1 : Assert DSR when in a data mode (UDP, TCP, PPP, or SLIP) (Default). • n=2 : Assert DSR when the device has network coverage. S211 can also be used to request that DSR is always asserted. If S211 is set to 3 and &S is changed to a non-zero value, S211 will be changed to 1.
&C	Assert DCD
CTSE	Clear To Send Enable: This feature asserts CTS when there is a network connection. • n=0 : Disabled (Default). • n=1 : Enable assertion of CTS when there is network coverage. RS232 voltage levels: • *Positive = Network coverage.* • *Negative = No coverage.* Flow control (AT\Q) will override this indication, so if you want to use CTS to indicate network coverage, flow control has to be off (AT\Q0).
X	Extended Call Progress Result mode. • **n=0** : Turn off extended result codes (Default). • **n=1** : Turn on result codes. This adds the text 19200 to the CONNECT response.
***NUMTIOP**	Convert 12 digit number to IP. • **n=0** : Use as name. • **n=1** : Use as IP address.

TCP

Table 6-9: Common: TCP

Command	Description
General	
S0	This register determines how the device responds to an incoming TCP connection request. The device remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the device must be set for a successful TCP connection. The device will send a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgement of the connection request and the TCP session is established. • n=0 : Off (Default). • n=1 : On. • n=2 : Use Telnet server mode on TCP connections. • n=3 : With a Telnet connection, overrides the client's default echo, allowing the server on the host port to perform the echo. CRLF sequences from the telnet client will also be edited to simply pass CRs to the server on the host port.
S7	Specifies the number of seconds to wait for a TCP connection to be established when dialing out.
TCPT	Interval to terminate a TCP connection when no in or outbound traffic. This value affects only the TCP connection in TCP PAD mode. • n=interval
TCPS	TCP connection time-out (TCPS) units. Specifies a time interval upon which if there is no in or outbound traffic through a TCP connection, the connection will be terminated. • n=0 : minutes
S221	Connect Delay: Number of seconds to delay the “CONNECT' response upon establishing a TCP connection. OR Number of tenths of seconds to delay before outputting ENQ on the serial port after the CONNECT when the ENQ feature is enabled. • n=0 - 255
S60	Telnet Client Echo Mode. • n=0 : No Echo • n=1 : Local Echo (Default) • n=2 : Remote Echo
***ENQ**	Outputs an ENQ [0x05] after the TCP CONNECT delayed by the Delay Connect Response time (S221). • n=0 : Disabled (Default). • n=1 : Enable ENQ on CONNECT.

UDP

Table 6-10: Common: UDP

Command	Description
MD	Default power-up mode for the serial port: When the device is power-cycled, the serial port enters the mode specified by this command after 5 seconds. On startup, typing ATMD0 within 5 seconds changes the mode to normal (AT command) mode. See also S53 to set the port for UDP . • hh (hex byte)=00 : normal • hh=01 : SLIP • hh=02 : PPP • hh=03 : UDP • hh=04 : TCP • hh=07 : PassThru • hh=0F : MP MDT • hh=13 : Modbus ASCII • hh=23 : Modbus RTU (Binary) • hh=33 : BSAP • hh=63 : Variable Modbus • hh=73 : Reliable UDP • hh=83 : UDP Multicast
S82	Enables UDP auto answer (half-open) mode. • n=0 : Normal mode • n=2 : Enable UDP auto answer mode.
S83	Set or query UDP auto answer idle time-out. If no data is sent or received before the time-out occurs, the current UDP session will be terminated. While a session is active, packets from other IP addresses will be discarded (unless *UALL is set). • n=0 : No idle time-out (Default). • n=1 - 255 : Time-out in seconds.
UDPLAST	If enabled, sets S53 to the last accepted IP address through UDP auto answer. This can be used in conjunction with MD3 so that when there is no UDP session, new ethernet host data will cause a connection to be restored to the last IP accepted through UDP auto answer. • n=0 : Does not change S53 setting. (Default). • n=1 : Set S53 to the last accepted IP.
AIP	Allow IP address. • n=0 : Allow only the IP address specified in S53 to connect when UDP auto answer is enabled (S82=2). • n=1 : Allow any incoming IP address to connect when UDP auto answer is enabled (S82=2). Always subject to any Friends filters that may be defined.

Table 6-10: Common: UDP

Command	Description
UALL	Accepts UDP packets from any IP address when a UDP session is active. If there is no UDP session active, an incoming UDP packet will be treated according to the UDP auto answer and AIP settings. • n=0 : No effect (Default). • n=1 : Accept UDP data from all IP addresses when in a UDP session.
HOR	Half-Open Response - In UDP auto answer (half-open) mode. • n=0 : No response codes when UDP session is initiated. • n=1 : RING CONNECT response codes sent out serial link before the data from the first UDP packet. *Note: Quiet Mode must be Off.*
***DU**	The dial command always uses UDP, even when using ATDT. • n=0 : Dial using the means specified (default). • n=1 : Dial UDP always, even when using ATDT. *Note: When this parameter is set you cannot establish a TCP PAD connection.*
***USD**	Waits the specified delay before sending the first UDP packet and the subsequent UDP packets out to the port Ethernet. • n=0 : No UDP packet delay (Default). • n=1 - 255 : Delay in 100ms units, from 100 ms to 25.5 sec.

DNS

Table 6-11: Common: DNS

Command	Description
***DNS1** ***DNS2**	Queries the DNS addresses. Your cellular carrier provides the DNS addresses while your device is registering on their network. • n=1 or 2 : First and second DNS address. • d.d.d.d=IP address of domain server.

Table 6-11: Common: DNS

Command	Description
***DNSUSER**	Sets a user-provided DNS to query first when performing name resolutions in the device. • d.d.d.d=IP address of domain server *Note: You can set up a second DNS User, if you have two DNS users.*
***DNSUPDATE**	Indicates whether the device should send DNS updates to the DNS server specified by *DNSUSER. These updates are as per RFC2136. They are not secure and are recommended only for a private network. In a public network, the IP Logger services should be used instead. • n=0 : DNS updates disabled (Default). • n=1 : DNS updates enabled.

Dynamic IP

Table 6-12: Common: Dynamic IP

Command	Description
***DEVICENAME**	Name of the device (up to 20 characters long) to use when performing IP address change notifications to IP Manager. The value in *DOMAIN provides the domain zone to add to this name. name=device name (for example, mydevice) Example: if *deviceNAME=mydevice and *DOMAIN=eairlink.com, then the device's fully qualified domain name is mydevice.eairlink.com. Automatically Generated Names: • #I3 - The ESN/IMEI will be used as the name. • #CCID - The CCID will be used as the name. • #NETPHONE - The phone number will be used as the name. **Tip:** *Each device using IP Manager needs a unique name. Two devices cannot be called “mydevice”. One could be “mydevice1” with the other as “mydevice”.*
***DOMAIN**	Domain (or domain zone) of which the device is a part. This value is used during name resolutions if a fully qualified name is not provided and also for DNS updates. This value can be up to 20 characters long. • name=domain name (i.e. eairlink.com) If *DOMAIN=eairlink.com, then when ATDT@remote1 is entered, the fully qualified name remote1.eairlink.com will be used to perform a DNS query to resolve the name to an IP address. **Tip:** *Only letters, numbers, hyphens, and periods can be used in a domain name.*

Table 6-12: Common: Dynamic IP

Command	Description
*IPMANAGER1 *IPMANAGER2	Sets a domain name or IP address to send IP change notifications to. Up to two independent IP Manager servers can be set, using either AT*IPMANAGER1 or AT*IPMANAGER2. Updates to a server can be disabled by setting that entry to nothing (for example, “AT*IPMANAGER1=”). • n=1 : First IP Manager server. • n=2 : Second IP Manager server.
*IPMGRUPDATE1 *IPMGRUPDATE2	Sets the number of minutes to periodically send an IP update notification to the corresponding server. This will occur even if the IP address of the MP device doesn't change. *IPMGRUPDATE1 is used to set the refresh rate to *IPMANAGER1, while *IPMGRUPDATE2 is used with *IPMANAGER2. If the value is set to 0, then periodic updates will not be issued (i.e. IP change notifications will only be sent when the IP actually changes). • n=1 : First IP Manager server. • n=2 : Second IP Manager server. • **m=0, 5-255** : Number of minutes to send an update.
*IPMGRKEY1 *IPMGRKEY2	Sets the 128-bit key to use to authenticate the IP update notifications. If the key's value is all zeros, a default key will be used. If all the bytes in the key are set to FF, then no key will be used (i.e. the IP change notifications will not be authenticated). AT*IPMGRKEY1 is used to set the key to use with AT*IPMANAGER1, while AT*IPMGRKEY2 is used to the key with AT*IPMANAGER2. • n=1 : First IP Manager server. • n=2 : Second IP Manager server. • key=128-bit key in hexadecimal [32 hex characters]

PPP/Ethernet

Table 6-13: Common: PPP/Ethernet

Command	Description
*HOSTPRIVMODE	Set or query whether a private or public (network) IP is to be used when the Host initiates a 1x connection to the device. • n=0 : Public (network) IP Mode: When the Host initiates a PPP connection, the host will be given the network IP address that was obtained from the cellular carrier while registering on the network. If the network issues a new IP address, the cellular connection will be closed (since the IP address has changed) and has to be re-initiated. (default). • n=1 : Private IP Mode: When the Host initiates a 1x connection, the host will be given the IP address specified in *HOSTPRIVIP. The device will then perform 1 to 1 NAT-like address translation, which shields the Host from network IP changes.
*HOSTPRVIP	Set or query the private IP address that is to be negotiated by the 1x connection if *HOSTPRIVMODE =1. • d.d.d.d=IP Address

Table 6-13: Common: PPP/Ethernet

Command	Description
***HOSTPEERIP**	Set or query the IP address that can be used to directly contact the MP device once a cellular connection is established. If this value is not specified, 192.168.13.31 will be used. • d.d.d.d=local or peer IP address of the device. *Note: This is not normally used nor needed by user applications.*
***HOSTNETMASK**	Subnet mask for the host interface. Allows communication with a subnet behind the host interface. • n.n.n.n = subnet mask, example 255.255.255.0.
***HOSTAUTH**	Host Authentication Mode: Use PAP or CHAP to request the user login and password during PPP or CHAP negotiation on the host connection. The username and password set in *HOSTUID and *HOSTPW will be used. • n=0 : Disable PAP or CHAP request (Default). • n=1 : PAP and CHAP. • n=2 : CHAP
***HOSTUID**	Host User ID for PAP, or CHAP, or PPPoE. • string=user id (up to 64 bytes)
***HOSTPW**	Host Password for PAP, or CHAP, or PPPoE. • string=password
***DHCPSERVER**	DHCP Server Mode

PassThru

Table 6-14: Common: PassThru

Command	Description
***PTINIT**	Any AT Command string to be passed to the OEM module before entering PASSTHRU mode, e.g. AT&S1V1, etc. • string=AT command(s)
***PTREFRESH**	Number of minutes of inactivity in PASSTHRU mode to resend the *PTINIT string to the hardware module. • n=0 : Disabled • n=1-255 minutes

Table 6-14: Common: PassThru

Command	Description
***RESETPERIOD**	In PASSTHRU mode, device will be reset after this period if no data has been sent or received. Value is in hours. • n=0 : Disabled • n=1-255 hours
***CSX1**	PassThru Echo : Echo data to the host. • n=0 : Data will be passed to the host. • n=1 : PASSTHRU mode will echo all host received data and will not pass the data to the device while the device is not asserting DCD. *Note: If the device is asserting DCD, data will be passed from the host to the device as it normally is when *CSX1=0.*

SMTP

Table 6-15: Common: SMTP

Command	Description
***SMTPRADDR**	Specify the IP address or Fully Qualified Domain Name (FQDN) of the SMTP server to use. • d.d.d.d=IP Address • name=domain name (maximum: 40 characters).
***SMTPFROM**	Sets the email address from which the SMTP message is being sent. • email=email address (maximum: 30 characters).
***SMTPUSER**	The email account username to authenticate with the SMTP server (*SMTPADDR) for sending email. • user=username (maximum: 40 characters). *Note: Not required to use SMTP settings but may be required by your cellular carrier.*
***SMTPPW**	Sets the password to use when authenticating the email account (*SMTPFROM) with the server (*SMTPADDR). • pw= password *Note: Not required to use SMTP settings but may be required by your cellular carrier.*
***SMTPSUBJ**	Allows configuration of the default Subject to use if one isn't specified in the message by providing a “Subject: xxx” line as the initial message line. • subject=message subject

Other

Table 6-16: Common: Other

Command	Description
***IPPING**	Set the period to ping (if no valid packets have been received) a specified address (*IPPINGADDR) to keep the device alive (online). • n=0 : Disable pinging (default) • n=15-255 minutes *Note: 15 minutes is the minimum interval which can be set for Keepalive. If you set *IPPING for a value between 0 and 15, the minimum value of 15 will be set.*
***IPPINGADDR**	Set the IP address or valid internet domain name for the device to ping to keep itself alive (online). *IPPING must to be set to a value other than 0 to enable pinging. • d.d.d.d=IP address • name=domain name
***IPPINGFORCE**	Force Keepalive Ping
***TPPORT**	Sets or queries the port used for the AT Telnet server. If 0 is specified, the AT Telnet server will be disabled. The default value is 2332. • n=0 : Disabled. • n=1-65535 Many networks have the ports below 1024 blocked. It is recommended to use a higher numbered port.
***TELNETTIMEOUT**	Telnet port inactivity time out. By default, this value is set to close the AT telnet connection if no data is received for 2 minutes. • n=minutes
***SNTP**	Enables daily SNTP update of the system time. • n=0 : Off • n=1 : On
***SNTPADDR**	SNTP Server IP address, or fully-qualified domain name, to use if *SNTP=1. If blank, time.nist.gov is used. • d.d.d.d=IP address • name=domain name
***NETWDOG**	Network connection watchdog: The number of minutes to wait for a network connection. If no connection is established within the set number of minutes, the device resets. • n=0 : Disabled. • n=minutes : Default = 120 min.
***MSCIUPADDR**	Device Status Update Address - where Name/Port is the domain name and port of the machine where the device status updates will be sent. The status parameters of the device are sent in an XML format. • name=domain name • port=port

Table 6-16: Common: Other

Command	Description
***MSCIUPDPERIOD**	Device Status Update Period - where n defines the update period in seconds. • n=0 : Disabled • n=1-255 seconds
DAE	AT Escape Sequence detection. • n=0 : Enable • n=1 : Disable
***DATZ**	Enables or disables reset on ATZ. • n=0 : Normal Reset (Default). • n=1 : Disable Reset on ATZ.
***SNMPPORT**	This controls which port the SNMP Agent listens on. • n=0 : SNMP is disabled • n=1-65535
***SNMPSECLVL**	Selects the security level requirements for SNMP communications. • n=0 : No security required. SNMPv2c and SNMPv3 communications are allowed. • n=1 : Authentication equivalent to “authNoPriv” setting in SNMPv3. SNMPv3 is required to do authentication, SNMPv2c transmissions will be silently discarded. • n=2 : Authentication and encryption, equivalent to “authPriv”' setting in SNMPv3. SNMPv3 is required to do authentication and encryption, SNMPv2c and SNMPv3 authNoPriv transmissions will be silently discarded. Messages are both authenticated and encrypted to prevent a hacker from viewing its contents.
***SNMPTRAPDEST**	Controls destination for SNMP Trap messages. If port is 0 or host is empty, traps are disabled. Traps are sent out according to the SNMP security level (i.e. if the security level is 2, traps will be authenticated and encrypted). Currently, the only trap that can be generated is linkup. • host=IP address • port=TCP port
***SNMPCOMMUNITY**	The SNMP Community String acts like a password to limit access to the device’s SNMP data. • string =string of no more than 20 characters (default = public).

Low Power

Table 6-17: Common: Low Power

Command	Description
VLTG	Set or query the voltage level at which the device goes into low power mode. • n=0 : Ignore voltage for power control. • n=threshhold in tenths of volts Example: ATVLTG=130 would place the device in a low power use, standby state if the voltage goes below 13.0V.
PTMR	Number of minutes after one of the power down events (VTLG or DTRP) happens until the device enters the low power mode. If DTRP and VLTG are both 0 (zero), this setting does nothing. • n=0-255 minutes *Note: There is always a minimum of 1 minute between power down event and actual shutdown (to give the device time to prepare); entering zero will not power down the device immediately, but after one minute.In the first 5 minutes after device powers up, power down events are ignored to give the user time to change configurations.*
SISE	Standby Ignition Sense Enable: the device will monitor the ignition sense on the power connector and enter the low power consumption stand-by mode when the ignition is turned-off. • n=0 : Disable • n=1 : Enable

Firewall

Table 6-18: Common: Firewall

Command	Description
FM	Firewall mode - Only allow specified IPs to access the device. • n=0 : Disable Firewall mode • n=1 : Enable Firewall mode - Only packets from friends will be accepted, packets from other IP addresses are ignored.

Table 6-18: Common: Firewall

Command	Description
FO	Friends List IP address. • n=0-9 Friends list index • d.d.d.d = IP address Using 255 in the IP address will allow any number. Example: 166.129.2.255 allows access by all IPs in the range 166.129.2.0-166.129.2.255.
F1	
F2	
F3	
F4	
F5	
F6	
F7	
F8	
F9	

Logging

This group includes commands specific to the internal log.

Table 6-19: Logging

Command	Description
***DBGPPPLVL**	Sets the logging level for the PPP stack. • n=0 : No logging • n=1 : Log client events (default) • n=2 : Log server events • n=3 : Log client and Server events
***DBGIPLVL**	Sets the logging level for the IP subsystem. • n=0 : No logging • n=1 : Log errors (i.e. invalid/corrupt packets, etc.). • n=2 : Log the header of all received packets. Note that this can quickly exhaust available space for the event log. • n=3 : Log the header of all received and sent packets. Note that this can quickly exhaust available space for the event log.
***DBGCOMMLVL**	Set the logging level for the host or module COM port. • n=0 : No logging • n=1 : Host COM Port • n=2 : Module COM Port

Table 6-19: Logging

Command	Description
***DBGETHLVL**	Sets the logging level for the Ethernet port. • n=0 : No logging • n=1 : Log errors: invalid/corrupt packets, etc. • n=2 : Log the header of all received packets. Note that this can quickly exhaust available space for the event log.
***DBGDHCPLVL**	Enable or disable internal DHCP logging. • n=0 : No logging • n=1 : Log DHCP events.

Caution: *Logging is intended for diagnostic purposes only. Extensive use of logging features can cause degraded device performance.*

GPS

This group includes commands specific to GPS features and the device line.

Table 6-20: GPS: Server 1

Command	Description
***PPIP**	IP address where GPS reports are sent (ATS Server IP). Also see *PPPORT. • d.d.d.d=IP address Example: AT*PPIP=192.100.100.100
***PPPORT**	Port where GPS reports are sent. • n=1-65535
***PPTIME**	GPS Report Time Interval. See also *PPMINTIME, *PPTSV, +CTA. n=seconds (1 - 65535) *Note: Your cellular carrier may impose a minimum transmit time.* **Caution:** *A report time of less than 30 seconds can possibly keep an RF link up continuously. This will eventually cause the MP to overheat and shutdown. An RF resource may continue be tied up to transfer small amounts of data. Generally the RF channel will be released and go dormant in 10-20 seconds of no data sent or received.*
***PPDIST**	GPS Report Distance Interval in 100 Meter Units (kilometer). 1 mile is approximately 1600 kilometers. • n=0 : Disabled • n=1-65535

Table 6-20: GPS: Server 1

Command	Description
***PPTSV**	Timer for Stationary Vehicles. Time interval in minutes that the device will send in reports when it is stationary. • n=0 : Disabled • n=1-255 minutes For example, if *PPTIME=10, the MP will send in reports at least every 10 seconds while it is moving; however, once it stops moving, it will slow the reports down to this *PPTSV value. *Note: In order for the PPTSV (Stationary Vehicle timer) to take effect, the PPTIME value must be set to a value greater than 0 and less than the PPTSV value. The PPTSV timer checks for vehicle movement at the PPTIME interval, so if PPTIME is disabled, then PPTSV will also be disabled.*
***PPGPSR**	GPS report type. • n=0 : Use legacy reports specified in *MF value. Note: Must also have *PPDEVID=0. • n=0x11 : Standard GPS Report • n=0x12 : Standard GPS Report + UTC Date • n=0x13 : Standard GPS Report + UTC Date + RF data • n=0xD0 : Xora reports. • n=0xE0 : GGA and VTG NMEA reports • n=0xE1 : GGA, VTG and RMC NMEA reports • n=0xF0 : TAIP reports • n=0xF1 : Compact TAIP data
***PPSNF**	Store and Forward will cause GPS reports to be stored up if the MP goes out of network coverage. Once the vehicle is in coverage the GPS reports will be sent en masse to the server. • n=0 : Disabled • n=1 : Enabled (default)
***PPDEVID**	Whether or not the MP should include the 64-bit device ID in its GPS reports. *PPDEVID MUST be 1 if the device uses a Dynamic IP. n=0 : Disable ID. n=1 : Enable/display ID.
***PPSNFR**	Store and Forward Reliability: GPS reports will be retransmitted if not acknowledged by the server. • n=0 : Disabled • n=1 : Reliable mode enabled for RAP messages • n=2 : Simple reliable mode

Table 6-20: GPS: Server 1

Command	Description
*PPSNFB	Store and Forward Behavior. When *PPSNF=1, the type of Store and Forward behavior is defined by: • n=0 : Normal Store and Forward. Data is stored when the MP is out of cellular coverage; when the MP is in coverage, data is sent to server as soon as possible. This is the default form devices with RAP version 1.3 or lower. • n=1 : Data sent only when polled. Data is stored until polled using the Poll command sent by a server. • n=2 : Grouped Reports. Data is stored until the desired minimum number of reports (see *PPSNFM) has been stored. The data is then sent to the server in groups with at least the specified number of reports.
*PPSNFM	Store and Forward Minimum Reports. Specifies the minimum number of reports that must be stored before they are forwarded to the server. The data is then sent to the server in packets that contain at least this number of reports. • n=0-255
*PPMAXRETRIES	Maximum number retries when in Simple Reliable Mode. • n=0 : Disabled • n=1-255 retries

Misc

Table 6-21: GPS: Misc

Command	Description
*PPMINTIME	Specifies the minimum amount of time between reports generated due to either the time interval (*PPTIME) or the distance interval (*PPDIST). This is useful to limit network traffic and make more efficient use of bandwidth. This can be used in conjunction with store and forward. The minimum value which this setting can take depends on the policies of the carrier. • n=0 : Disabled • n=1-65535 seconds
*PPINPUTEVT	Enable sending input changes as events (different report types). • n=0 : Disable • n=1 : Enable
*PPODOM	Enable odometer reporting. • n=0 : Disabled (default) • n=1 : Enabled
*PPODOMVAL	The current odometer value of the MP. The value is in meters. Maximum value is approximately 4.3 billion meters (2.5 million miles). 1 mile is approximately 1600 meters. • n=meters

Table 6-21: GPS: Misc

Command	Description
***PPTAIPID**	Sets/queries the TAIP ID. This ID is returned in TAIP reports if it has been negotiated with the TAIP client. This value is only used in conjunction with TAIP emulation mode (*PPGPSR=F0). • nnnn=TAIP ID (4 characters)
***PPFLUSHONEVT**	Flushes store and forward buffer when an input event (DTR/RTS) occurs. • n=0 : Disable • n=1 : Enable
***PPREPORTINPUTS**	Enable input reporting. • n=0 : Disabled • n=1 : Enabled *Note: If both AT*PPCOM1000=1 and AT*PPREPORTINPUTS=1 are enabled, the AirLink Device digital inputs will be reported and the COM1000 inputs will be ignored.*
***PPGPSDATUM**	Specifies the GPS datum to use for position reports. For accurate results, this value should match the datum used by receiving mapping application. • n=0 : WGS84 • n=92 : NAD27 • n=115 : NAD83
***PPTCPPOLL**	Specifies the port to listen on for TCP GPS report polling. The request to this port needs to come from the same IP address in *PPIP. • n=0 : Disabled • n=1-65535 (default 9494)
***UDPRGPS**	Set or query GPS stamping of UDP Reliable packets. When set, data received on the host serial port will be encapsulated with the GPS date and time. • n=0 : Disabled (default) • n=1 : Enabled
***PPIGNOREIP**	When enabled, ignore ATS Server IP (*PPIP) updates in RAP. • n=0 : Use ATS Server IP updates. • n=1 : Ignore ATS Server IP updates.
***PPCOM1000**	Enables support for extra inputs from a COM1000. • n=0 : Disable • n=1 : Enable **Tip:** *If both AT*PPCOM1000=1 and AT*PPREPORTINPUTS=1 are enabled, the AirLink Device's digital inputs will be reported and the COM1000 inputs will be ignored.*

Serial Port

Table 6-22: GPS: Serial Port

Command	Description
***PPLATS**	Local ATS - Causes GPS reports to also be sent out the serial or Ethernet link every n seconds, when there is a PPP connection to the serial host or a connection to the Ethernet port is established. • n=0 : Disable • n=1-255 seconds **Tip:** *Sends to the PPP peer IP S110 with the Destination Port number S53.*
***PPLATSR**	Indicates the type of GPS report to send to the local client (PPP/SLIP peer). See *PPGPSR. • n=0x11 : Standard GPS Report • n=0x12 : Standard GPS Report + UTC Date • n=0x13 : Standard GPS Report + UTC Date + RF data • n=0xD0 : Xora reports. • n=0xE0 : GGA and VTG NMEA reports • n=0xE1 : GGA, VTG and RMC NMEA reports • n=0xF0 : TAIP reports • n=0xF1 : Compact TAIP data
***PPLATSEXTRA**	Have local ATS reporting (LATS) send up to 7 extra copies of a GPS report to the subsequent ports. • n=0 : Just the original report is sent (default). • n=1-7 : Send GPS report copies to that number of ports. Example: If AT*PPLATSEXTRA=7 and the port in S53 is 1000, then GPS reports will be sent to ports 1000-1008.
***PGPS**	Send NMEA GPS strings out serial link. Similar to ATGPS except that the *PGPS value can be saved to NVRAM so that it will continue to operate after resets. • n=0 : Disabled • n=1 : Send NMEA GPS strings out serial link. • n=2 : Send NMEA GPS strings out the USB port. • n=3 : Send NMEA GPS strings out both the serial and the USB port.
***PGPSC**	Allows a PP to be configured to send GPS sentences out of the serial port when the PP loses cellular coverage. This feature is configured by 2 fields. This command controls the status of the sentences. • n=0: Always sent • n=1: Sent when out of cellular coverage When set to 1, no reports are saved in SnF.

Table 6-22: GPS: Serial Port

Command	Description
***PGPSD**	PGPSD is a 16-bit value that is the number of seconds to wait when "Out of Coverage" occurs before switching to, sending the messages out the serial port and not into SnF. • Any messages put into SnF during this switchover delay period will be sent OTA, when coverage is re-acquired. *Note: The two persistent GPS report parameters, *PGPSR and *PGPSF, will control the report type and frequency of the messages sent out the serial port, when out of coverage.*
***PGPSR**	
***PGPSF**	Persistant GPS frequency • n= number of seconds per report Max Value: 65535 up to 18 hours

Cellular

This group includes commands specific to HSDPA, EDGE and GPRS. If you are not connecting to a which uses HSDPA, EDGE, or GPRS, you will not see this group in the menu.

Table 6-23: Cellular

Command	Description
***NETAPN**	Easy entry of the APN. If left blank, the device will attempt to use the default subscriber value as defined by the account. • apn=access point name 1 and “IP”, are required and not variable. Quotes need to be placed around the APN. **Tip:** *When *NETAPN has been configured, +CGDONT will be pre-populated in ACEmanager .*
***RXDIVERSITY**	This is the diversity setting, It is Disabled by default.
+COPS	Manually specify an operator. Refer also to *NETOP. • mode=0 : Automatic - any affiliated carrier [default]. • mode=1 : Manual - use only the operator <oper> specified. • mode=4 : Manual/Automatic - if manual selection fails, goes to automatic mode. • format=0 : Alphanumeric ("name") (G3x10 must use this format). • format=2 : Numeric • oper=”name”
+CGQREQ	Set Quality of Service Profile. Change should be at carrier's request. Normally not required to be changed.
+CGQMIN	Minimum Acceptable Quality of Service Profile. Change should be at carrier's request. Normally not required to be changed.

CDMA

This group includes commands specific to 1x and EV-DO. If you are not connecting to a device which uses EV-DO or 1x, you will not see this group in AceWeb.

Table 6-24: CDMA

Command	Description
+CTA	Inactivity timer, in seconds. Typical network settings cause a link to go dormant after 10 to 20 seconds of inactivity, no packets transmitted or received. This time can be shortened to release the physical RF link sooner when the application only transmits short bursts. • n=0 : Allows the cellular network to determine the inactivity timer. • n= seconds (maximum 20 seconds)
$QCMIP	Mobile IP (MIP) Preferences. On a Mobile IP network, a device connects to the network using PPP. During the negotiation process the device is NOT required to present a username and password to authenticate because the authentication parameters are stored in the device itself. • n=0 : Disabled, SIP only • n=1 : MIP preferred • n=2 : MIP only *Note: Your account with your cellular carrier may not support Mobile IP.*
~NAMLCK	The NAMLCK is the device's 6-digit OTSL (One Time Subsidy Lock), MSL (Master Subsidy Lock), or SPC (Service Provisioning Code). Your cellular carrier will provide the unlock code. • nnnnnn=6 digit unlock code *Note: If the number is accepted by the device, the OK result code is returned. If the number is rejected, the ERROR result is returned. If three successive Errors are returned, the device must be reset by Sierra Wireless AirLink Solutions to allow any further attempts. The device permits 99 failures of this command during its lifetime. After that, the device becomes permanently disabled.*

Table 6-24: CDMA

Command	Description
***EVDODIVERSITY**	EV-DO Diversity allows two antennas to provide more consistent connection. • n=0 : Disabled. • n=1 : Allow *Note: If you are not using a diversity antenna, *EVDODIVERSITY should be disabled.*
***EVDODATASERV**	*PROVISION=MSL,MDN/MIN[,SID][,NID] **Tip:** *It is recommended to use the Setup Wizard for your carrier to provision the device.* Provision the device with the lock code and phone number. Cannot be configured in AceManager. • **MSL=master lockcode** • **MDN/MIN=phone number** • **SID=system ID** • **NID=network ID**

I/O

This group includes configuration commands for the digital and analog inputs and relay outputs. Some of the values shown as a part of this group are not changeable but reflect the current status. Only those devices with available inputs and outputs will display this group.

Table 6-25: I/O

Command	Description
***DIGITALIN1**	Query individual digital inputs. The digital inputs report either a 0 (open) or 1 (closed). • n=1-4 Input number
***DIGITALIN2**	
***DIGITALIN2**	
***DIGITALIN4**	
***ANALOGIN1**	Query individual analog inputs. The analog inputs report the voltage in volts. • n=1-4 Input number
***ANALOGIN2**	
***ANALOGIN3**	
***ANALOGIN4**	

Table 6-25: I/O

Command	Description
*RELAYOUT1 *RELAYOUT2	Set or query the relay outputs. • n=1-2 Input number • s=OPEN or CLOSED

SMS

Command	Description
AT*securemode	This AT command to enables/disables Services. "AT*securemode=value" 0 - Will be the default, and leave the modem in its normal open state. 1 - Will disable the Aleos Ports for OTA and Wifi access 2 - Will disable the Aleos Ports for OTA and Local Access+ WiFi (All) 3+ - all values larger than 2 will receive an error response. The DHCP and the Telnet ports will not be blocked. Responses to outgoing Aleos message that are sent OTA will be allowed into Aleos, so GPS and DNS will work.
AT*SMSM2M	at*smsm2m_8 = for 8 bit data mode at*smsm2m_u = for unicode For example: at*smsm2m_8="17604053757 5448495320495320412054455354" sends the message "THIS IS A TEST" but the message is 8 bit data. Likewise at*smsm2m_8="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f" will send the bytes: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f

SIERRA
WIRELESS