ALEOS 4.2.1 Configuration

User Guide

20080616
Rev 2.1

SIERRA WIRELESS

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 device are used in a normal manner with a well-constructed network, the Sierra Wireless AirLink device should not be used in situations where failure to transmit or receive data could result in personal hazard or risk to the user or any other party, including but not limited to 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 device, or for failure of the Sierra Wireless AirLink device to transmit or receive such data.

Safety and Hazards

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

Do not operate the Sierra Wireless AirLink device in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless AirLink device **MUST BE POWERED OFF**. When operating, the Sierra Wireless 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 devices may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless 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 offense.

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 may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM® 3G. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates 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:	sales@sierrawireless.com
Mail:	Sierra Wireless America 39677 Eureka Drive Newark, CA 94560 USA Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4	
Fax:	1-510-624-4299 1-604-231-1109	
Website:	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	Q3: 2010	ALEOS 4.2 Configuration User Guide created and edited.
1.0 D	March 2011	ALEOS 4.2 Configuration User Guide released.
2.0 A	April 2011	ALEOS 4.2 Configuration User Guide updated.
2.1	June 2011	ALEOS 4.2 Configuration User guide updated and released as version 4.2.1.

Contents

1: Introduction

Overview

ACEmanager™ is the free utility used to manage and configure the 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.

ACEmanager enables the user to:

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

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

A template can be created, after a single device 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.

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 descriptions in ACEmanager
- Relevant configuration details
- User scenarios for certain sections in the guide.

The following table lists the order and topic of each chapter in this user guide.

No.	Chapter Name
1	Introduction
2	Configuring the AirLink Device
3	Status
4	WAN/Cellular Configuration
5	LAN Configuration
6	VPN Configuration
7	Security Configuration
8	Services Configuration
9	GPS Configuration
10	Events Reporting
11	Serial Configuration
12	Application Configuration
13	I/O Configuration
14	Admin

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

Document	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 which is used to monitor the connection state of a Sierra Wireless AirLink device and GPS or power status as applicable.
AceNet 3.0 User Guide	This document explains the use of AceNet services for remote management of Sierra Wireless AirLink devices.
AMS User Guide	This document explains the use of AMS services for remote management of Sierra Wireless AirLink devices.

2: Configuring the AirLink Device

After powering on the AirLink device, and ensuring that you have an IP-based connection set up (Ethernet or USB/net), you can log on to ACEmanager. In your browser, either enter http://192.168.13.31:9191 or another IP address depending on the interface you select. (See table below.)

Note: The connected device for Ethernet is not always .100. It can be anything between 100 - 150.

Interface	AirLink device	Connected Device
Ethernet	192.168.13.31	192.168.13.100
USB/NET	192.168.14.31	192.168.14.100

The login defaults are:

- User Name: user (or viewer)
- Password: 12345

The “user” login is used for configuring or monitoring. The “viewer” login can only view the configuration and connection state but not change the configuration in any way.

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

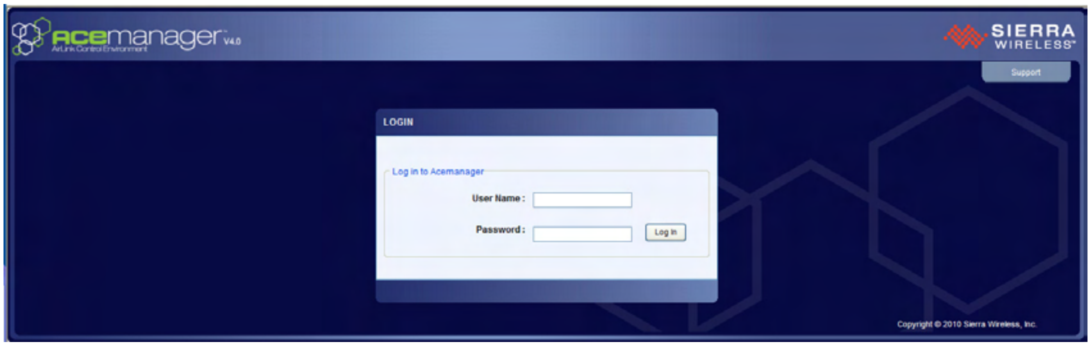


Figure 2-1: ACEmanager: Main Login screen

Main Menu Tabs

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

- Firmware: Upgrades the firmware
- 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

There are two options for configuring the AirLink device:

1. Use the browser based ACEmanager (as detailed in this guide); or
2. Use a terminal emulator application (e.g., HyperTerminal, PuTTY, etc.) 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 and from the connected device to the cellular network.

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

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.
- **Radio Bypass**: Direct connection to internal hardware (OEM Radio Module) of the AirLink device.
- **Telnet/SSH**: 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.*

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 a carriage return **<CR>** (ASCII character 0x0D), i.e., 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.

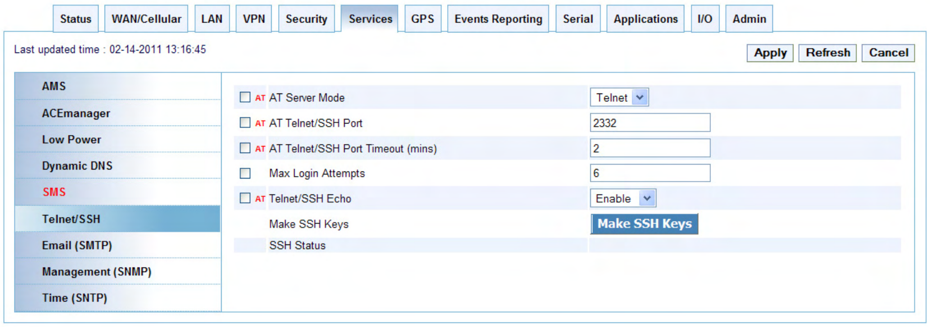
Refer to Appendix E for a list of and details on AT Commands.

Telnet/SSH 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 timeout is 2 minutes. This is the internal telnet on the modem to pass AT commands and not TCP pad.

To switch to SSH operation, select SSH from the drop-down menu in the AT Server Mode field.



Last updated time : 02-14-2011 13:16:45

□ AT AT Server Mode	Telnet
□ AT AT Telnet/SSH Port	2332
□ AT AT Telnet/SSH Port Timeout (mins)	2
□ Max Login Attempts	6
□ AT Telnet/SSH Echo	Enable
Make SSH Keys	Make SSH Keys
SSH Status	

Figure 2-2: ACEmanager: Services - Telnet/SSH

Creating a Template

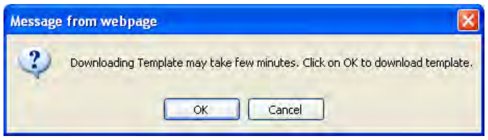
If you have a device configuration that works well for your needs, you can use ACEmanager to save that device's configuration as a template and then apply it to other Sierra Wireless AirLink devices.

Templates can be created as either feature-specific or for all configurable features. Feature-specific templates are quicker and more reliable to apply from one device to another. Because only specific feature fields are included in the template, all other configuration elements are not altered. This allows for different configurations for particular features not to be overwritten. Feature-specific templates are also more reliable since they are less likely to include configuration fields for features not present in the target device.

Templates which are to include every configurable field in the device are more useful for troubleshooting purposes than for transferring feature configurations from one device to another.

To create a template with ACEmanager:

1. Configure your AirLink device in ACEmanager.
2. Click on Apply (in the upper right hand corner of the ACEmanager screen) so that the configuration settings write to the device.
    a. For feature-specific templates, check the boxes in front of the specific fields to be saved to the template. This allows you to have a template covering only the configuration items you want imported into another device. For tables, click the box at the top of the table to include the entire table.
    b. For templates with all configurable fields, **do not** check any of the boxes.
3. Click on Download to save the template. A confirmation dialog box displays.

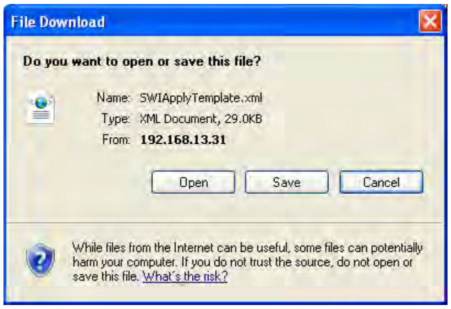


Downloading Template may take few minutes. Click on OK to download template.

Figure 2-3: ACEmanager: Download Template Message

Note: There will be a time delay as the template downloads. A yellow-lit text message of the downloading process displays.

4. Click on OK. The File Download box displays.



File Download

Do you want to open or save this file?

Name: SWIApplyTemplate.xml
Type: XML Document, 29.0KB
From: 192.168.13.31

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 2-4: ACEmanager: File Download Box

5. Click on Save (or OK depending on your system browser).

Note: Some of the configuration settings are specific to individual devices. Avoid having those settings in your saved template as the devices you configure with the template could cease to work with the cellular or local network. A feature specific template allows you to omit configuration elements which need to be specific to a device.

6. Type in a file name that is descriptive of the template (to easily find it 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.

Applying a Template

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

To apply the template to a device:

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

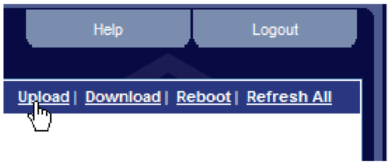
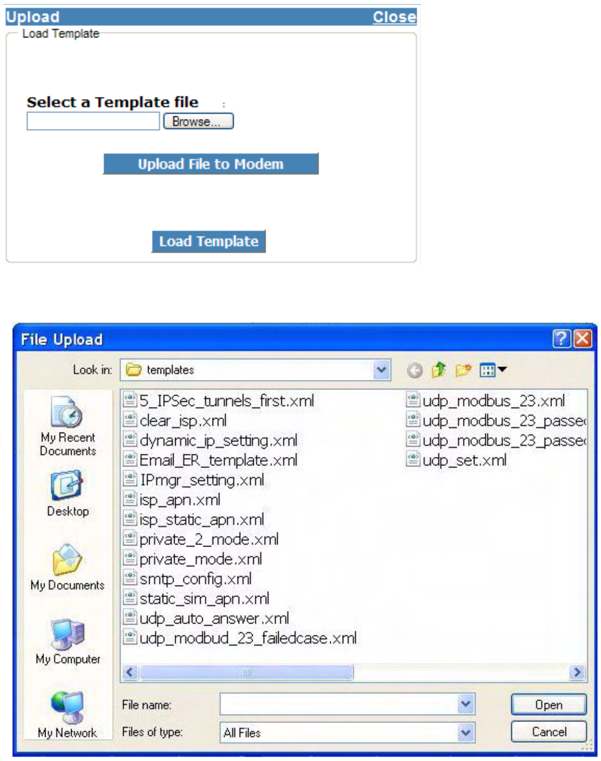


Figure 2-5: ACEmanager: Load

3. At the Upload window, click Browse, and select the template you have saved. You may need to change folders if you saved it to a different location.



Look in: templates

Files of type: All Files

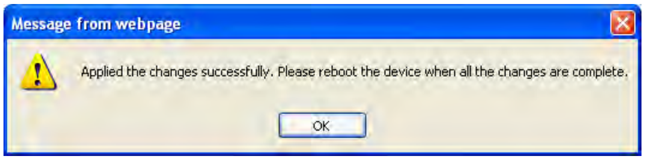
Figure 2-6: ACEmanager: Select and Upload Template

4. Click on Upload File to Modem.

5. Click on Load Template. As in the template creation process, there will be a time delay as the template downloads.

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. Red asterisks (*) will display on the tabs that have been changed. Make any adjustments to the settings as needed.*

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



Applied the changes successfully. Please reboot the device when all the changes are complete.

Figure 2-7: ACEmanager: Apply Changes Dialog Box

7. Click 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: *Use the common settings on one device to configure those same settings on another device. For example, use the serial settings of one device to configure the serial settings of another device.*

3: Status

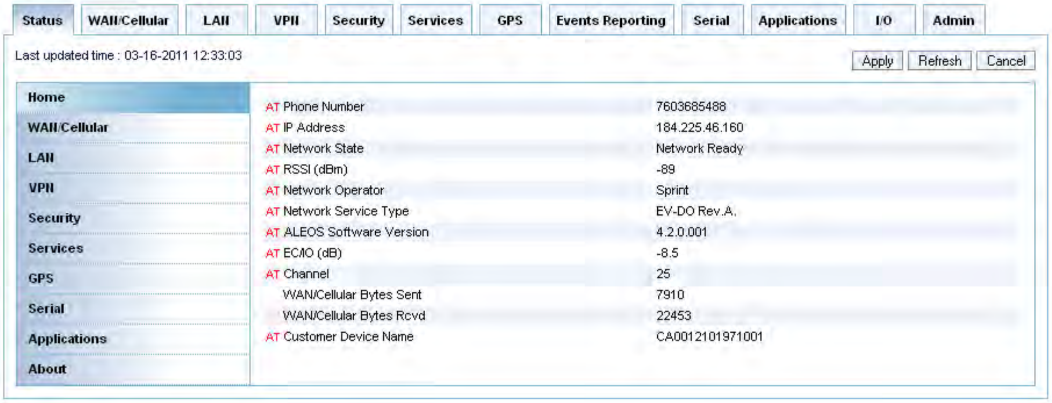
The Status tab that displays in ACEmanager is applicable to Sierra Wireless AirLink GX400 devices.

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 ACEmanager. It shows basic information about the cellular network connection and important information about the device you would most likely want to see first.

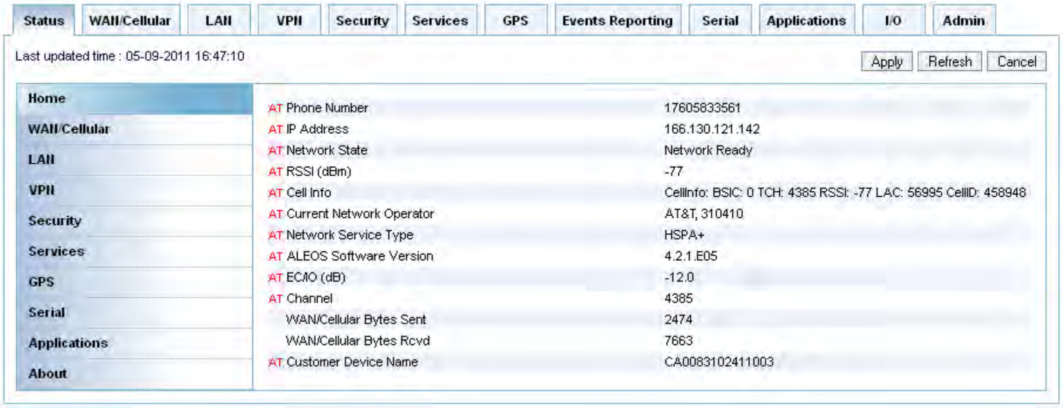
Tip: *Refer to the WAN/Cellular chapter of this guide for information about configuring the cellular settings.*



Last updated time : 03-16-2011 12:33:03

AT Phone Number	7603685488
AT IP Address	184.225.46.160
AT Network State	Network Ready
AT RSSI (dBm)	-89
AT Network Operator	Sprint
AT Network Service Type	EV-DO Rev.A.
AT ALEOS Software Version	4.2.0.001
AT EC/IO (dB)	-8.5
AT Channel	25
WAN/Cellular Bytes Sent	7910
WAN/Cellular Bytes Rcvd	22453
AT Customer Device Name	CA0012101971001

Figure 3-1: ACEmanager: Status - Home - CDMA



Last updated time : 05-09-2011 16:47:10

AT Phone Number	17605833561
AT IP Address	166.130.121.142
AT Network State	Network Ready
AT RSSI (dBm)	-77
AT Cell Info	CellInfo: BSIC: 0 TCH: 4385 RSSI: -77 LAC: 56995 CellID: 458948
AT Current Network Operator	AT&T, 310410
AT Network Service Type	HSPA+
AT ALEOS Software Version	4.2.1.E05
AT EC/IO (dB)	-12.0
AT Channel	4385
WAN/Cellular Bytes Sent	2474
WAN/Cellular Bytes Rcvd	7663
AT Customer Device Name	CA0083102411003

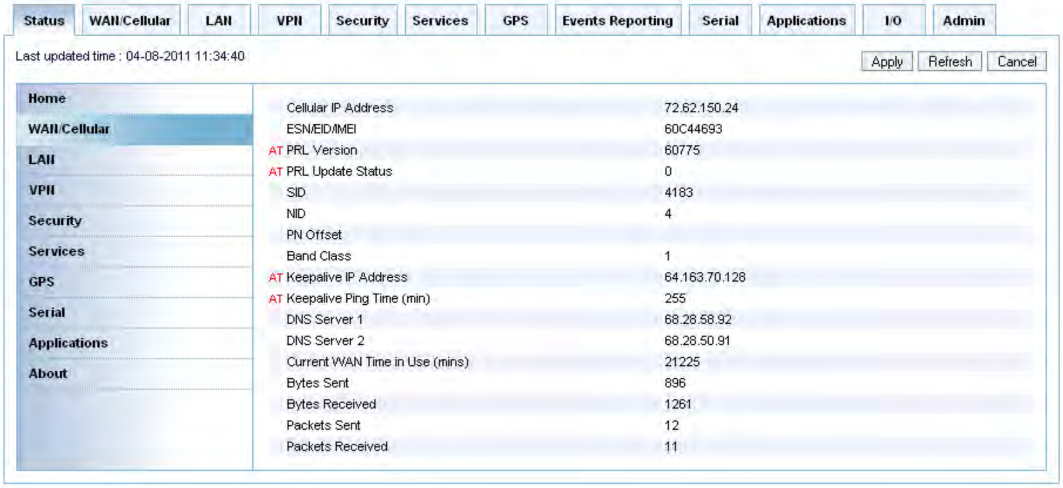
Figure 3-2: ACEmanager: Status - Home - GSM

Status Field	Description
Phone Number	The phone number (programmed into the device) associated with the 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 use to contact the AirLink device from the Internet if you have a mobile terminated or Internet accessible account.
Network State	Current state of the cellular radio network connection.
RSSI (dBm)	The current RSSI (Receive Signal Strength Indicator) of the AirLink device as a negative dBm value. Signal strength of the cellular signal. The higher 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.
Cell Info	For GSM/HSPA only. Provides such cell information as the base station identity code (BSIC), TCH, received signal strength indicator (RSSI), LAC, and the cell ID.
(Current) Network Operator	Provides the name of the cellular carrier being used.

Network Service Type	The type of service being used by the device, e.g., EV-DO Rev A or HSPA+.
ALEOS Software Version	Version of ALEOS software currently installed in the device.
EC/IO (dB)	Indicates the EC/IO signal quality measured in decibels.
Channel	The current active CDMA/GSM channel number.
WAN/Cellular Bytes Sent	Number of bytes sent to the network since system startup or reboot.
WAN/Cellular Bytes Rcvd	Number of bytes received from the network since system startup.
Device Name	Name of the device as it is configured with the Dynamic DNS IP Manager settings.

WAN/Cellular

WAN/Cellular status provides specific information about the cellular connection including IP address and how much data has been transmitted or received. Some of the information on this page is repeated on the Home page for quick reference.



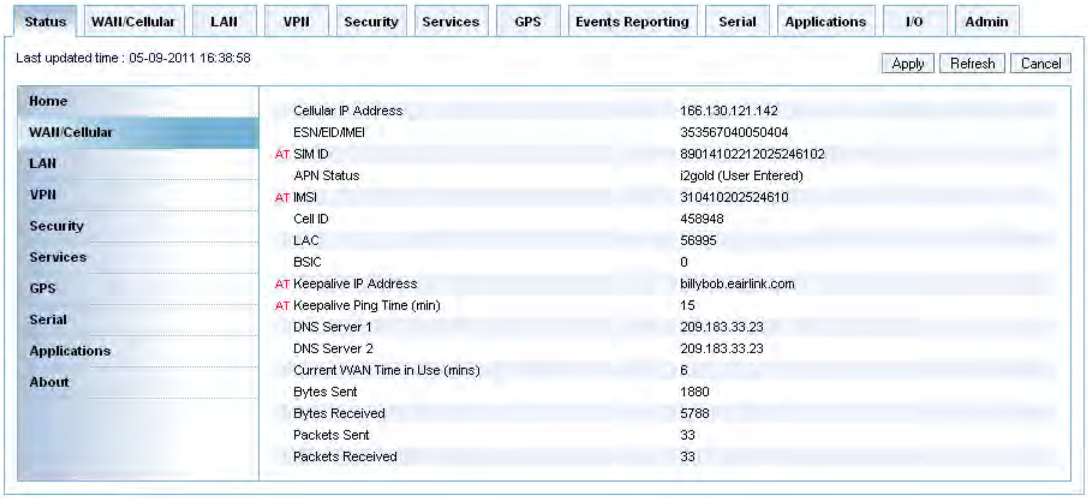
Last updated time : 04-08-2011 11:34:40

	Cellular IP Address	72.62.150.24
	ESN/EID/IMEI	60C44693
AT	PRL Version	60775
AT	PRL Update Status	0
	SID	4183
	NID	4
	PN Offset	
	Band Class	1
AT	Keepalive IP Address	64.163.70.128
AT	Keepalive Ping Time (min)	255
	DNS Server 1	68.28.58.92
	DNS Server 2	68.28.50.91
	Current WAN Time in Use (mins)	21225
	Bytes Sent	896
	Bytes Received	1261
	Packets Sent	12
	Packets Received	11

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

Status Field	Description
Cellular IP Address	Cellular WAN IP Address.
ESN/EID/IMEI	Electronic Serial Number for the internal radio.
PRL Version	Version of the Preferred Roaming List installed in the device.
PRL Update Status	Status of the last PRL update. 0 is there has been none.
SID	Configuration parameter for the cellular account.

Status Field	Description
NID	Configuration parameter for the cellular account.
PN Offset	Configuration parameter for the cellular account.
Band Class	Configuration parameter for the cellular account.
Keepalive IP Address	The IP address that WAN Keep Alive uses to test cellular connectivity (if enabled).
Keepalive Ping Time (min)	The amount of time between Keep Alive pings in minutes.
DNS Server 1	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses.
DNS Server 2	2nd DNS server IP address.
Current WAN Time in Use (mins)	Provides the time (in minutes) that the WAN has been in use.
Bytes Sent	Number of bytes sent to the cellular network, since the system startup or reboot.
Bytes Received	Number of bytes received from the network, since system startup or reboot.
Packets Sent	Number of packets sent to the network, since system startup or reboot.
Packets Received	Number of packets received from the network, since system startup or reboot.



Last updated time : 05-09-2011 16:38:58

	Cellular IP Address	166.130.121.142
	ESN/EID/IMEI	353567040050404
AT	SIM ID	89014102212025246102
	APN Status	i2gold (User Entered)
AT	IMSI	310410202524610
	Cell ID	458948
	LAC	56995
	BSIC	0
AT	Keepalive IP Address	billybob.eairlink.com
AT	Keepalive Ping Time (min)	15
	DNS Server 1	209.183.33.23
	DNS Server 2	209.183.33.23
	Current WAN Time in Use (mins)	6
	Bytes Sent	1880
	Bytes Received	5788
	Packets Sent	33
	Packets Received	33

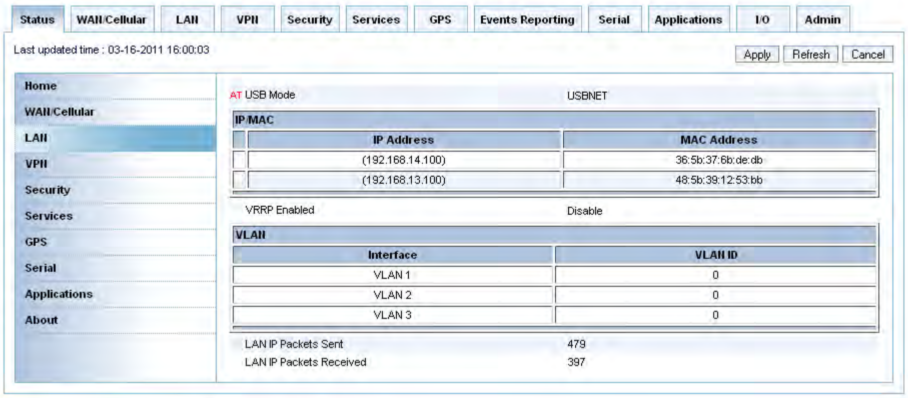
Figure 3-4: ACEmanager: Status - WAN/Cellular - GSM

Status Field	Description
Cellular IP Address	Provides the cellular WAN IP Address.
ESN/EID/IMEI	Provides the Electronic Serial Number for the internal radio.
SIM ID	Provides the identification number for the current SIM card in use.

Status Field	Description
APN Status	Identifies the current APN in use by the network connection. • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN configuration tab.*
IMSI	Identifies the International Mobile Subscriber Identity number.
Cell ID	A unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC.
LAC	The Location Area Code.
BSIC	The Base Station Identity Code.
Keepalive IP Address	The IP address that WAN Keep Alive uses to test cellular connectivity (if enabled).
Keepalive Ping Time (min)	The amount of time between Keep Alive pings in minutes.
DNS Server 1	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses.
DNS Server 2	2nd DNS server IP address.
Current WAN Time in Use (mins)	Provides the time (in minutes) that the WAN has been in use.
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

This is the status of the local network. It lists information about the network and connected clients.



Last updated time : 03-16-2011 16:00:03

AT USB Mode USBNET

IP/MAC

IP Address	MAC Address
(192.168.14.100)	36:5b:37:6b:de:db
(192.168.13.100)	48:5b:39:12:53:bb

VRRP Enabled Disable

VLAN

Interface	VLAN ID
VLAN 1	0
VLAN 2	0
VLAN 3	0

LAN IP Packets Sent 479

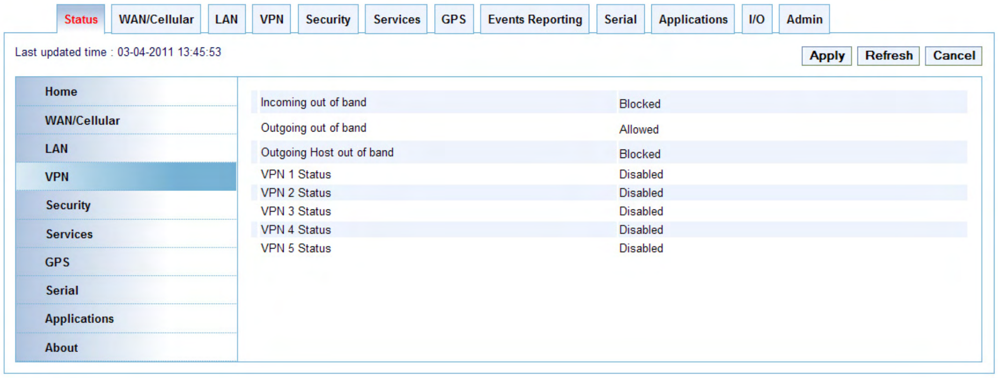
LAN IP Packets Received 397

Figure 3-5: ACEmanager: Status - LAN

Status Field	Description
USB Mode	Indicates which mode of the USB port is set: USBnet or USB serial.
IP/MAC table	Displays the local IP Address and the MAC Address of connected hosts.
VRRP Enabled	Indicates the configuration of the VRRP feature.
VLAN table	Provides the identities (name and ID) of the configured VLANs.
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.



Last updated time : 03-04-2011 13:45:53

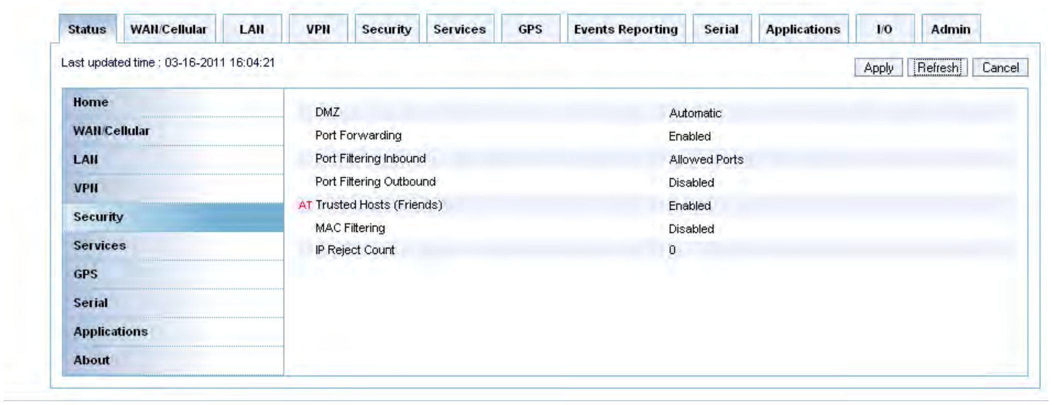
Incoming out of band	Blocked
Outgoing out of band	Allowed
Outgoing Host out of band	Blocked
VPN 1 Status	Disabled
VPN 2 Status	Disabled
VPN 3 Status	Disabled
VPN 4 Status	Disabled
VPN 5 Status	Disabled

Figure 3-6: ACEmanager: Status - VPN

Status Field	Description
Incoming out of band	Indicates whether incoming out of band traffic is allowed or blocked.
Outgoing out of band	Indicates whether outgoing ALEOS out of band traffic is allowed or blocked.
Outgoing Host out of band	Indicates whetherOutgoing Host out of band traffic is allowed or blocked.
VPN 1 to 5 Status	The status of each IPsec VPN client or GRE client: Disabled, Enabled, or Connected. VPN 1, however, can be configured for L2TP and SSL VPN.

Security

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



Last updated time : 03-16-2011 16:04:21

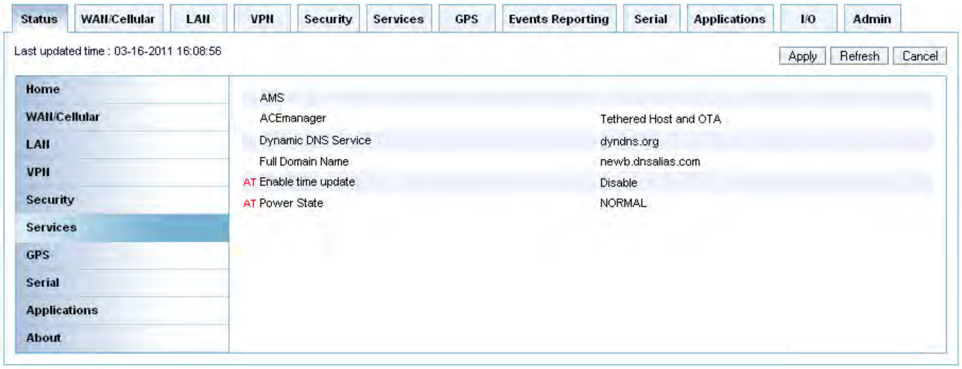
DMZ	Automatic
Port Forwarding	Enabled
Port Filtering Inbound	Allowed Ports
Port Filtering Outbound	Disabled
Trusted Hosts (Friends)	Enabled
MAC Filtering	Disabled
IP Reject Count	0

Figure 3-7: ACEmanager: Status - Security

Status Field	Description
DMZ	Options: Automatic, Manual, or Disabled. DMZ defines a single LAN connected device where all unsolicited data should be routed.
Port Forwarding	Options: Enabled or Disabled. Show status of port forwarding.
Port Filtering Inbound	Options: Allowed Ports, Blocked Ports, or Not Used. Show status of inbound port filtering.
Port Filtering Outbound	Options: Allowed Ports, Blocked Ports, or Not Used. Show status of outbound port filtering.
Trusted Hosts (Friends)	Options: Disabled or Enabled. Accepts connections from only trusted remote IP addresses.
MAC Filtering	Options: Enabled or Disabled. Show status of MAC filtering.
IP Reject Count	Rejected IP Count.

Services

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



Last updated time : 03-16-2011 16:08:56

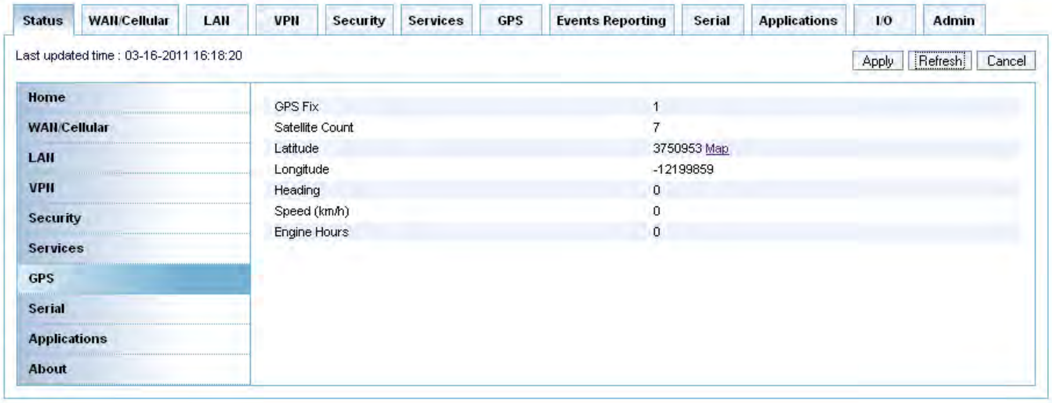
AMS	
ACEmanager	Tethered Host and OTA
Dynamic DNS Service	dyndns.org
Full Domain Name	newb.dnsalias.com
AT Enable time update	Disable
AT Power State	NORMAL

Figure 3-8: ACEmanager: Status - Services

Status Field	Description
AMS	Indicates the status of the connection to the AirLink Management System (or Service). This field is blank if the AMS configuration is disabled.
ACEmanager	The ACEmanager access mode. Options are Tethered Host and OTA or Tethered Host Only.
Dynamic DNS Service	Indicates the service in use for Dynamic DNS translation.
Full Domain Name	If the Dynamic DNS Service is configured to use a 3rd party host, the domain name configured will be displaced. If the Dynamic DNS Service is configured to use IP Manager, this field will not display.
Enable time update	Daily SNTP updates of the system time.
Power State	The current state of the Low Power feature.

GPS

The GPS (Global Positioning System) tab provides AirLink device location and movement information for use with tracking applications.



Last updated time : 03-16-2011 16:18:20

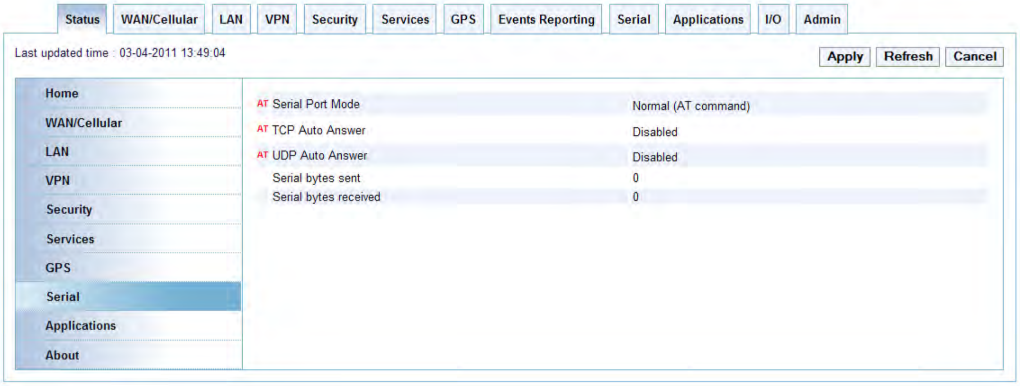
GPS Fix	1
Satellite Count	7
Latitude	3750953 Map
Longitude	-12199859
Heading	0
Speed (km/h)	0
Engine Hours	0

Figure 3-9: ACEmanager: Status - GPS

Status Field	Description
GPS Fix	0 = No Fix, 1 = GPS Fix, 2 = WAAS
Satellite Count	Displays how many satellites the GPS receiver detects.
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 (km/h)	Speed (in kilometers per hour).
Engine Hours	Measure of the number of hours the engine is on.

Serial

Note: The Serial section that displays in ACEmanager is applicable to all Sierra Wireless AirLink devices.



Last updated time : 03-04-2011 13:49:04

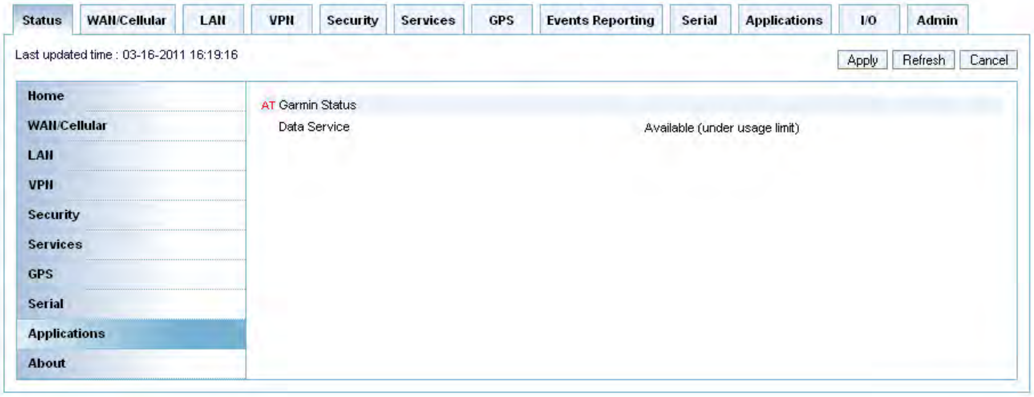
AT Serial Port Mode	Normal (AT command)
AT TCP Auto Answer	Disabled
AT UDP Auto Answer	Disabled
Serial bytes sent	0
Serial bytes received	0

Figure 3-10: ACEmanager: Status - Serial

Status Field	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 parameter 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 and allows 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 bytes sent	Number of bytes sent over serial port to host.
Serial bytes received	Number of bytes received over serial port from host.

Applications

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



Last updated time : 03-16-2011 16:19:16

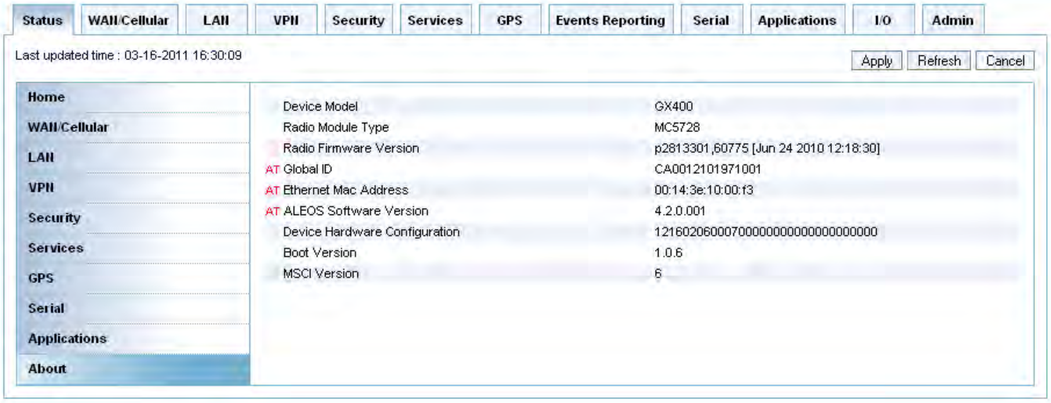
AT Garmin Status
Data Service Available (under usage limit)

Figure 3-11: ACEmanager: Status- Applications

Status Field	Description
Garmin Status	The state of the connection to the Garmin device when it is enabled. This field is blank when the Garmin device is disabled.
Data Service	The Data Service field displays “Available (under usage limit)” if the configured usage limit has not been exceeded.

About

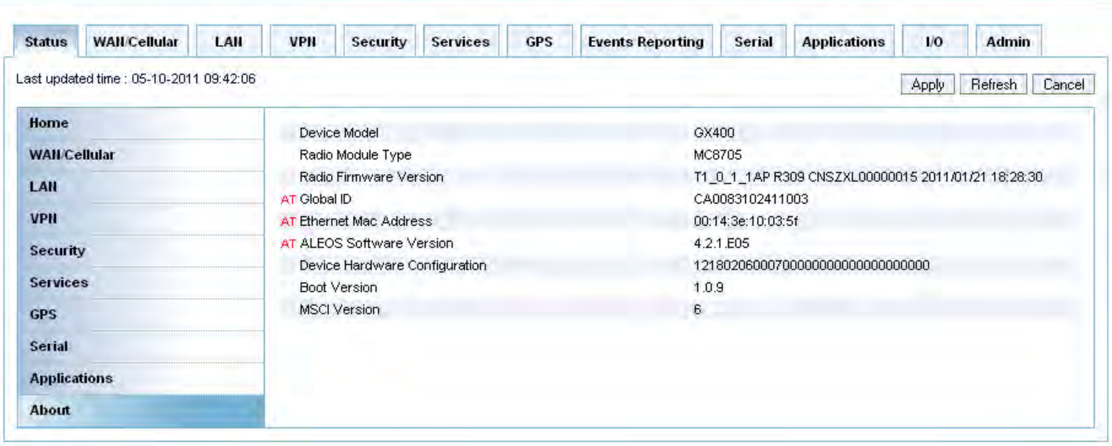
The About section of the Status group provides basic information about the cellular device. The fields for this section provide the same information for both CDMA and GSM.



Last updated time : 03-16-2011 16:30:09

Device Model	GX400
Radio Module Type	MC5728
Radio Firmware Version	p2813301,60775 [Jun 24 2010 12:18:30]
AT Global ID	CA0012101971001
AT Ethernet Mac Address	00:14:3e:10:00:f3
AT ALEOS Software Version	4.2.0.001
Device Hardware Configuration	1216020600070000000000000000000
Boot Version	1.0.6
MSCI Version	6

Figure 3-12: ACEmanager: Status - About - CDMA



Last updated time : 05-10-2011 09:42:06

Device Model	GX400
Radio Module Type	MC8705
Radio Firmware Version	T1_0_1_1AP R309 CNSZXL00000015 2011/01/21 18:28:30
AT Global ID	CA0083102411003
AT Ethernet Mac Address	00:14:3e:10:03:5f
AT ALEOS Software Version	4.2.1.E05
Device Hardware Configuration	12180206000700000000000000000000
Boot Version	1.0.9
MSCI Version	6

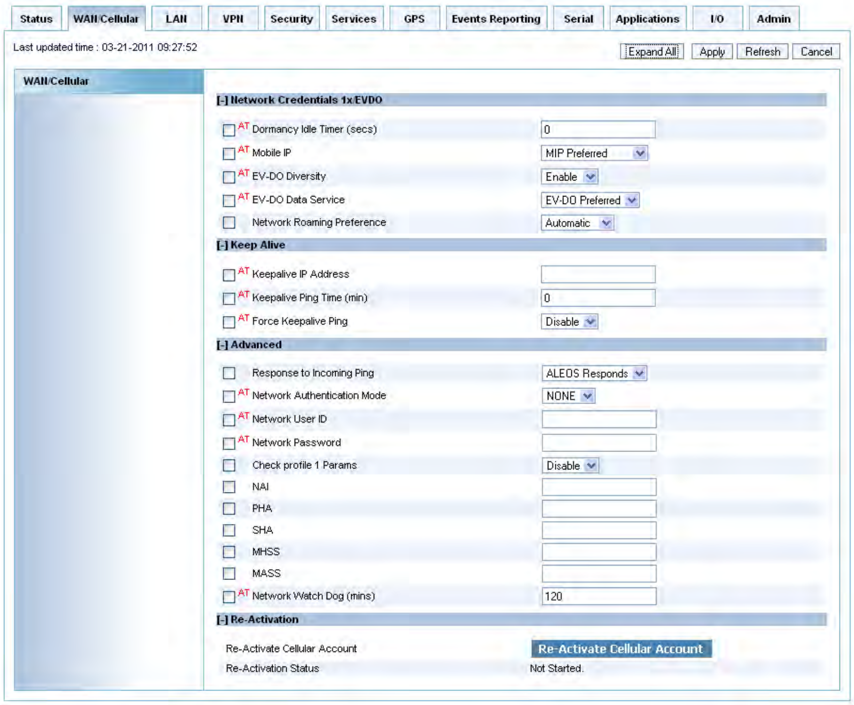
Figure 3-13: ACEmanager: Status - About - GSM

Status Field	Description
Device Model	The model of the device (e.g., GX400).
Radio Module Type	MC5728 or MC8705. The model number of the internal cellular radio module.
Radio Firmware Version	Firmware version in the radio module.
Global ID	The device ID used by ALEOS 4.2 to identify itself for various management applications.
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 device’s hardware configuration.
Boot Version	The version of boot code installed in the device.
MSCI Version	The MSCI version of the ALEOS internal configuration database.

4: WAN/Cellular Configuration

The WAN/Cellular tab that displays in ACEmanager is applicable across all Sierra Wireless AirLink GX400 devices.

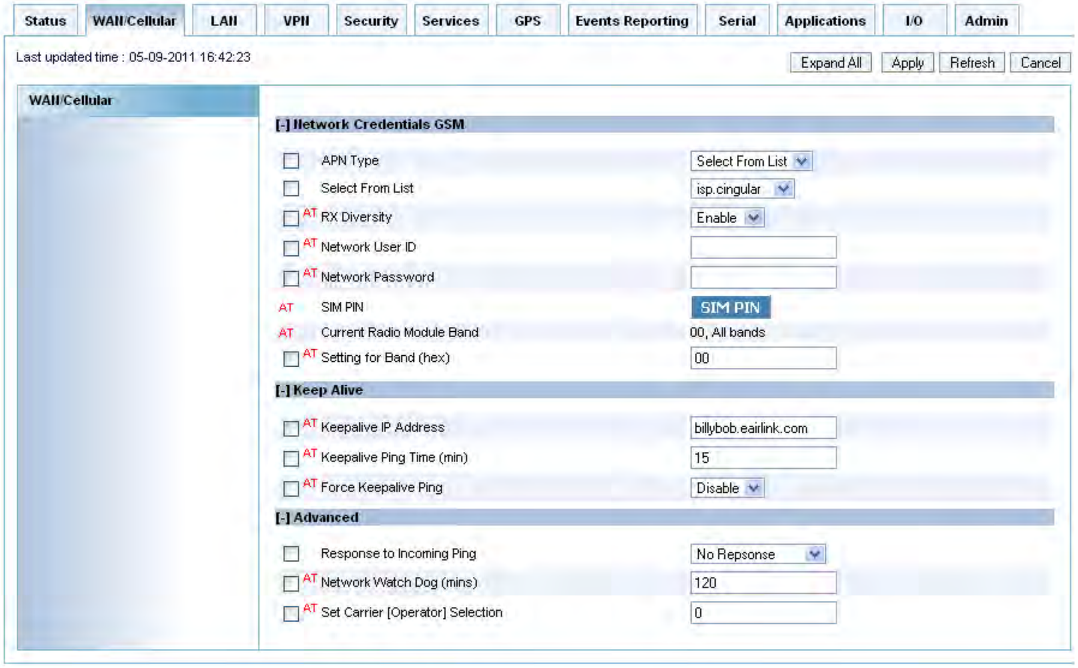
The WAN/Cellular section allows changes to the cellular connection and main operating mode of the AirLink device.



Last updated time : 03-21-2011 09:27:52

[-] Network Credentials 1x/EVDO	
□ AT Dormancy Idle Timer (secs)	0
□ AT Mobile IP	MIP Preferred
□ AT EV-DO Diversity	Enable
□ AT EV-DO Data Service	EV-DO Preferred
□ Network Roaming Preference	Automatic
[-] Keep Alive	
□ AT Keepalive IP Address	
□ AT Keepalive Ping Time (min)	0
□ AT Force Keepalive Ping	Disable
[-] Advanced	
□ Response to Incoming Ping	ALEOS Responds
□ AT Network Authentication Mode	NONE
□ AT Network User ID	
□ AT Network Password	
□ Check profile 1 Params	Disable
□ NAI	
□ PHA	
□ SHA	
□ MHSS	
□ MASS	
□ AT Network Watch Dog (mins)	120
[-] Re-Activation	
Re-Activate Cellular Account	Re-Activate Cellular Account
Re-Activation Status	Not Started.

Figure 4-1: ACEmanager: WAN/Cellular - Network Credentials 1x/EV-DO



Last updated time : 05-09-2011 16:42:23

[-] Network Credentials GSM

□	APN Type	Select From List
□	Select From List	isp.cingular
□ AT	RX Diversity	Enable
□ AT	Network User ID	
□ AT	Network Password	
AT	SIM PIN	SIM PIN
AT	Current Radio Module Band	00, All bands
□ AT	Setting for Band (hex)	00

[-] Keep Alive

□ AT	Keepalive IP Address	billybob.eairlink.com
□ AT	Keepalive Ping Time (min)	15
□ AT	Force Keepalive Ping	Disable

[-] Advanced

□	Response to Incoming Ping	No Repsonse
□ AT	Network Watch Dog (mins)	120
□ AT	Set Carrier [Operator] Selection	0

Figure 4-2: ACEmanager: WAN/Cellular - Network Credentials GSM

CarrierType	Command	Description
Network Credentials		
1x/EV-DO	**Dormancy Idle Timer (secs)**	Inactivity timer, in seconds. Typical network settings cause a link to go dormant after 10 to 20 seconds of inactivity with 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)
1x/EV-DO	**Mobile IP**	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 Default: MIP will be used when available with a fall back to SIP. *Note: Your account with your cellular carrier may not support all three of these options. check with lyour carrier as to which one should be used..*

CarrierType	Command	Description
1x/EV-DO	EV-DO Diversity	EV-DO Diversity allows two antennas to provide a more consistent connection. • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled.
1x/EV-DO	EV-DO Data Service	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
1x/EV-DO	Network Roaming Preference	Allows home or home preferred network preference.
HSPA/ GPRS	APN Type	Choose to use an APN based on the SIM in use or a custom APN manually entered. • Select From List - When selected, an entry field displays for typing in the APN that should be used. • User Entry
HSPA/ GPRS	Select From List	If the APN type is “Select from List,” a list of APNs based on the SIM in use will be available as a drop-down list.
HSPA/ GPRS	Rx Diversity	Allows two antennas to provide a more consistent connection. • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled.
HSPA/ GPRS	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.

CarrierType	Command	Description
HSPA/ GPRS	**Setting for Band (hex)**	Desired band to set by ALEOS in the radio module. Allows you to select GSM bands - All, 3G only, Enter the desired hex value: • 00 = All bands (default for the radio) • 02 = 3G 850/1900 • 04 = 2G 850/1900 • 05 = 2G all • 08 = 3G all
Keep Alive		
1x/EV-DO and HSPA/ GPRS	**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.
1x/EV-DO and HSPA/ GPRS	**Keepalive Ping Time (min)**	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.
1x/EV-DO and HSPA/ GPRS	**Force Keepalive Ping**	Determines if the ping should occur even if the device is not idle.
Advanced		
1x/EV-DO and HSPA/ GPRS	**Response to Incoming Ping**	When a Ping is received by the device from a remote location, the Response to Incoming Ping will redirect it to the selected location. • No response: the incoming Ping will be completely ignored • ALEOS Responds (default): ALEOS will return to the Ping response. • Pass to Host: The Ping will be forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there will be no Ping response. *Note: Some carriers may block all ICMP traffic on their network. A Ping sent to the device from a remote location will not be received.*

CarrierType	Command	Description
1x/EV-DO	Network Authentica-tion Mode	Specifies the authentication method to be used in the network PPP session. • PAP and CHAP are two options.
1x/EV-DO	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)
1x/EV-DO	Network Password	Network Password. The password that is used to login to the cellular network, when required. pw=password (30 characters maximum).
1x/EV-DO	Check profile 1 Params	Enables checking and updating the Profile 1 Parameters. *Not all carriers or account types support this featur*
1x/EV-DO	NAI	Sets the Network Access ID. *Not all carriers or account types support this feature.*
1x/EV-DO	PHA	Sets the IP address of the primary home agent. *Not all carriers or account types support this feature.*
1x/EV-DO	SHA	Sets the IP address of the secondary home agent. *Not all carriers or account types support this feature.*
1x/EV-DO	MHSS	Sets the home agent shared secret key. *Not all carriers or account types support this feature.*
1x/EV-DO	MASS	Sets the AAA shared secret key. *Not all carriers or account types support this feature.*
1x/EV-DO and HSPA/ GPRS	Network Watch Dog (mins)	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.
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”
Re-Activation		
1x/EV-DO	Re-Activate Cellular Account	Refer to the Re-Activation section of this chapter.
1x/EV-DO	Re-Activation Status	Refer to the Re-Activation section of this chapter.

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:

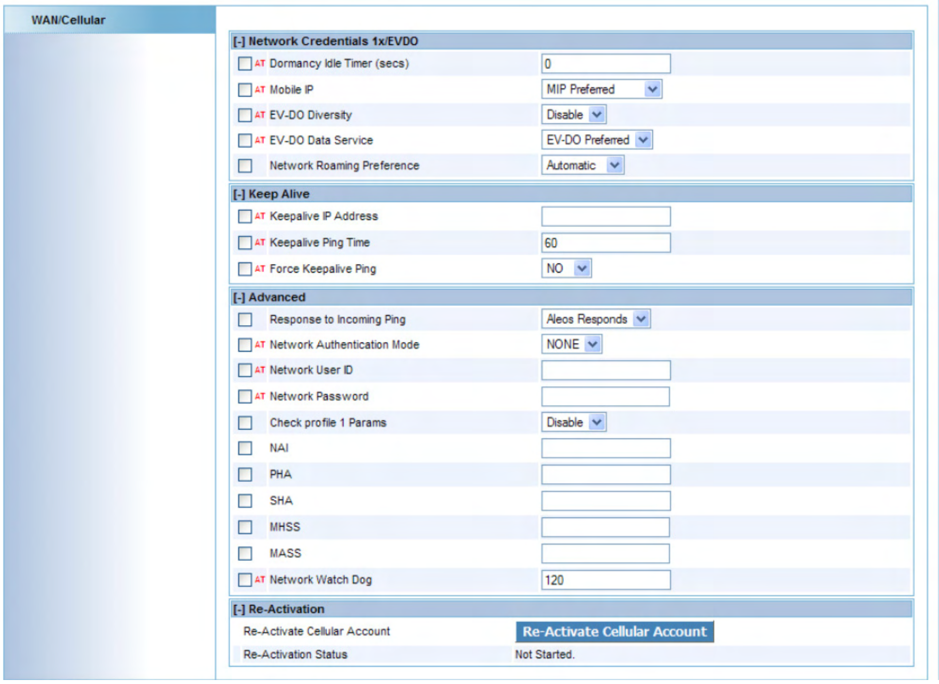
*IPPING	Estimated Usage
15 minutes	400k / month
30 minutes	200k / month
60 minutes	100k / month
120 minutes	50k / month

Re-Activation

The Re-Activation section of the WAN/Cellular tab only appears for EV-DO/1X devices. The Re-Activation feature can only be used when a particular device that has already been activated needs re-activation. If your device needs to be reactivated, click on the button labeled "Re-Activate Cellular Account". When you click on this button, the status will show the progress of the re-activation.

Note: If the provision fails, an error message will display.

After the provision process finishes, the system will then restart, as a reset is necessary to initiate the new account information.



[-] Network Credentials 1x/EVDO

□ AT Dormancy Idle Timer (secs)	0
□ AT Mobile IP	MIP Preferred
□ AT EV-DO Diversity	Disable
□ AT EV-DO Data Service	EV-DO Preferred
□ Network Roaming Preference	Automatic

[-] Keep Alive

□ AT Keepalive IP Address	
□ AT Keepalive Ping Time	60
□ AT Force Keepalive Ping	NO

[-] Advanced

□ Response to Incoming Ping	Aleos Responds
□ AT Network Authentication Mode	NONE
□ AT Network User ID	
□ AT Network Password	
□ Check profile 1 Params	Disable
□ NAI	
□ PHA	
□ SHA	
□ MHSS	
□ MASS	
□ AT Network Watch Dog	120

[-] Re-Activation

Re-Activate Cellular Account	Re-Activate Cellular Account
Re-Activation Status	Not Started.

Figure 4-3: ACEmanager: WAN/Cellular - ReActivation

5: LAN Configuration

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 can 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.

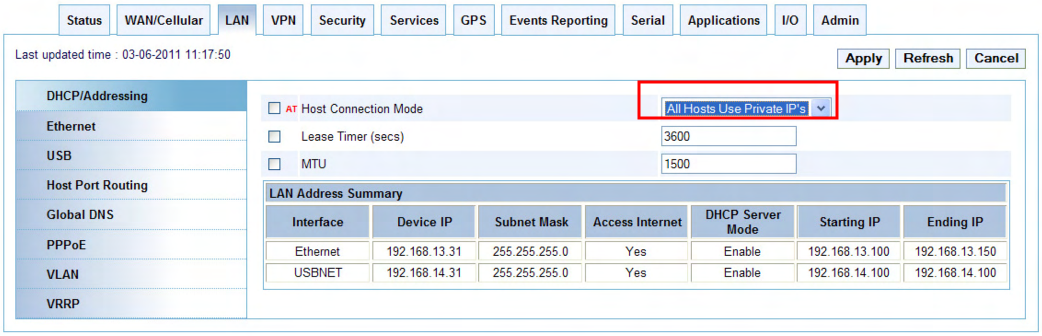
Tip: *When using Public mode, Sierra Wireless recommends connecting the device directly to the computer or other end device. Using a hub or switch may prevent the AirLink device from updating the IP address of the end device when an IP address is received from the cellular network.*

In ACEmanager, the Host Public mode and DHCP settings are part of the LAN tab**.** Subtabs of the LAN tab address the configuration of each interface or network type.

DHCP/Addressing

This section is mostly a status display of the configurations with a few options which are global to all the interface types. Interfaces which are enabled in the current configuration will be displayed with their configured settings.

Note: If the device has not been reset since configuration changes were made the current configuration in use may be different.



Last updated time : 03-06-2011 11:17:50

□ AT Host Connection Mode	All Hosts Use Private IP's
□ Lease Timer (secs)	3600
□ MTU	1500

LAN Address Summary

Interface	Device IP	Subnet Mask	Access Internet	DHCP Server Mode	Starting IP	Ending IP
Ethernet	192.168.13.31	255.255.255.0	Yes	Enable	192.168.13.100	192.168.13.150
USBNET	192.168.14.31	255.255.255.0	Yes	Enable	192.168.14.100	192.168.14.100

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

Command	Description
Host Connection Mode	Sets the Host Interface that uses the Public IP address granted 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 *Note: The connected computer receives the DHCP address from ALEOS and, it also has the default router set up to device IP.*
Lease Timer (secs)	Configurable DHCP lease time.
MTU	Sets the maximum transmission unit size.
LAN Address Summary	Displays the interfaces which have been enabled. By default, only the Ethernet and USB/net Interfaces are enabled.
Interface	The physical interface port or VLAN ID.
Device IP	The IP address of the AirLink device for the specified interface port.. By default, this is set to 192.168.13.31 for Ethernet and 192.168.14.31 for USB/net.

Command	Description
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.
Access Internet	Appears if the interface is configured to allow connected host(s) access to the Internet.
DHCP Server Mode	Indicates if the interface will have a DHCP server enabled to provide dynamically allocated IP addresses provided to connected hosts.
Starting IP	Ethernet DHCP pool starting IP address.
Ending IP	The ending IP for the interface. If the starting and ending IP are the same, there is a single address in the pool and only one host will receive an IP address from the DHCP serverfor that interface. Some interfaces, such as USB, can only have a single host connection. For others, statically assigned IP addresses in the same subnet but outside of the DHCP pool will still be able to connect and use the device in the same way as a DHCP connected host.

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. This DHCP host provides 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, e.g., 10.1.2.0.

2. When using a specific interface, the AirLink device acts as a DHCP server unless disabled. When the Host Connection Mode is Ethernet Uses Public IP, and 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 value is already a 1, it assigns 10.1.2.2 as the router address.

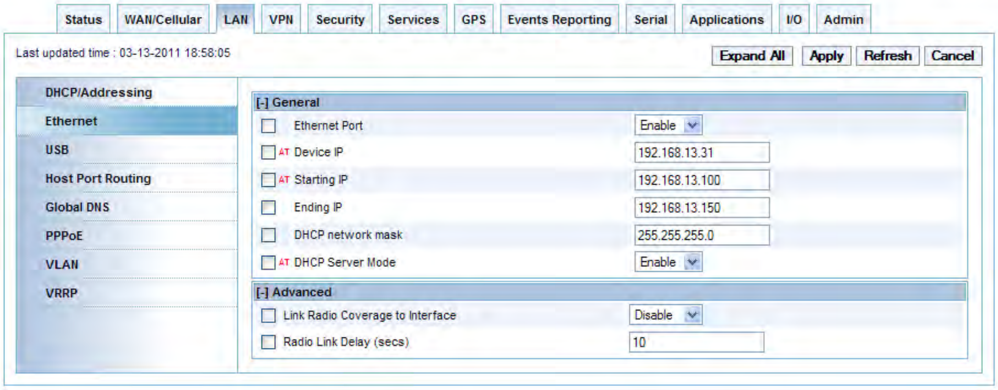
Note: The primary gateway to the cellular network, for any connected device, is enabled by default.

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, the DHCP server needs to be disabled. A tunnel is set up connecting a device (such as your computer or a router) with the AirLink device. The device will then use the MAC address of the AirLink device to send all outgoing packets.*

Ethernet

The AirLink device is equipped with an Ethernet port which can be enabled or disabled as needed. When the Ethernet port is disabled, no host can use the device on the Ethernet port with either a DHCP address or a statically assigned address. No ARP queries will receive a response on the Ethernet port.



Last updated time : 03-13-2011 18:58:05

[-] General

□ Ethernet Port: Enable
□ AT Device IP: 192.168.13.31
□ AT Starting IP: 192.168.13.100
□ Ending IP: 192.168.13.150
□ DHCP network mask: 255.255.255.0
□ AT DHCP Server Mode: Enable

[-] Advanced

□ Link Radio Coverage to Interface: Disable
□ Radio Link Delay (secs): 10

Figure 5-2: ACEmanager: LAN - Ethernet

Command	Description
General	
Ethernet Port	Enabled or disabled.
Device IP	The Ethernet IP address of the AirLink device. By default this is set to 192.168.13.31.
Starting IP	Ethernet DHCP pool starting IP address. *Note: If only one computer or device is 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 pool.
DHCP network mask	The Netmask given to any Ethernet DHCP client.
DHCP 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. Static IP hosts need to be within the same subnet as defined by the device IP and DHCP network mask.
Advanced	
Link Radio coverage to Interface	This disables the specified port when there is no cellular coverage. Options: • Disable • Ethernet • USB Default: Disable
Radio Link Delay (secs)	The delay in seconds before the selected interface goes down when there is no cellular coverage.

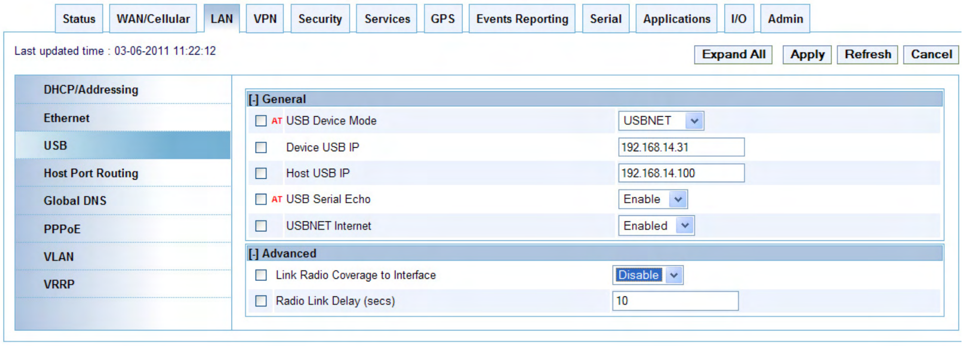
USB

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, or be disabled to prevent access by USB. 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.



Last updated time : 03-06-2011 11:22:12

[-] General

□	AT USB Device Mode	USBNET
□	Device USB IP	192.168.14.31
□	Host USB IP	192.168.14.100
□	AT USB Serial Echo	Enable
□	USBNET Internet	Enabled

[-] Advanced

□	Link Radio Coverage to Interface	Disable
□	Radio Link Delay (secs)	10

Figure 5-3: ACEmanager: LAN - USB

Note: There are USB/net and USB/serial drivers available for Windows XP and Windows 7 32-bit with a separate pair of drivers for Windows 7 64-bit. USB/serial works with Linx CDC-ACM drivers.

Note: A reboot is required to activate the USB mode change.

Command	Description
General	
USB Device Mode	*USBDEVICE=n 1 - USBNET 0 - USB Serial 2 - Disabled 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.
Host USB IP	The IP for the computer or device connected to the USB port.

Command	Description
USB Serial Echo	Toggle AT command echo mode when the USB is configured for virtual serial. 0 = OFF; 1 = ON
USBNET Internet	Enabled (default) or Disabled.
Advanced	
Link Radio Coverage to Interface	This disables the specified port when there is no cellular coverage. Options: • Disable • Ethernet • USB Default: Disable
Radio Link Delay (secs)	The delay in seconds before the selected interface goes down when there is no cellular coverage.

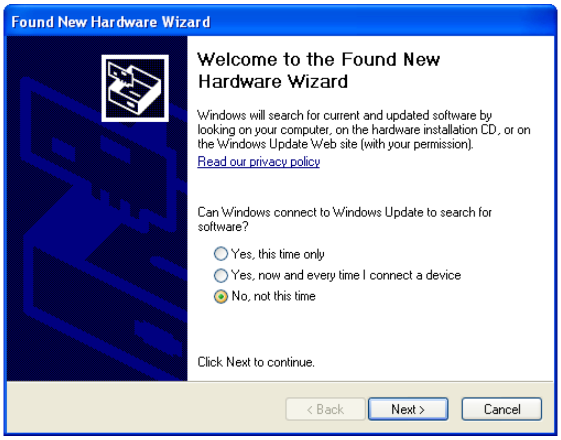
Installing the USB Drivers for Windows

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 will detect a new device and prompt you to install the driver.

Note: The directions in this section are for Windows XP. To install the drivers under Windows 7, you will need to start the driver installation from the Windows Device Manager.

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.



Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

Can Windows connect to Windows Update to search for software?

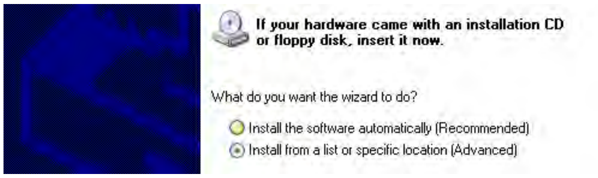
○ Yes, this time only
○ Yes, now and every time I connect a device
● No, not this time

Click Next to continue.

Figure 5-4: 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.



If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

○ Install the software automatically (Recommended)

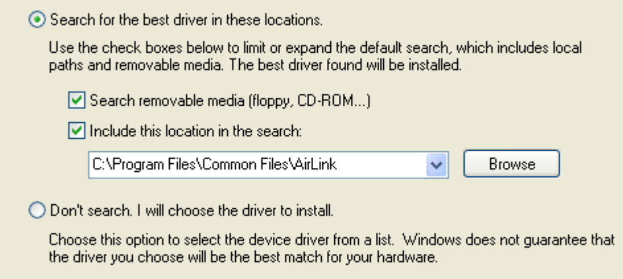
● Install from a list or specific location (Advanced)

Figure 5-5: 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.



● Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

☑ Search removable media (floppy, CD-ROM...)

☑ Include this location in the search:

C:\Program Files\Common Files\AirLink

○ Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

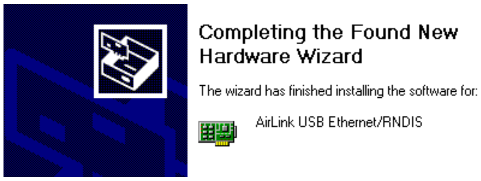
Figure 5-6: Hardware Wizard: Install location

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.

AirLink USB Ethernet/RNDIS

Figure 5-7: Hardware Wizard: Installing

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



Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

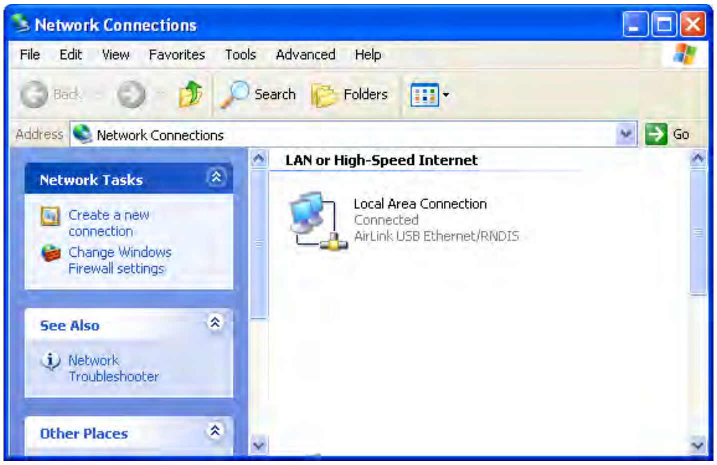
AirLink USB Ethernet/RNDIS

Figure 5-8: 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.*



Local Area Connection
Connected
AirLink USB Ethernet/RNDIS

Figure 5-9: Network Connections

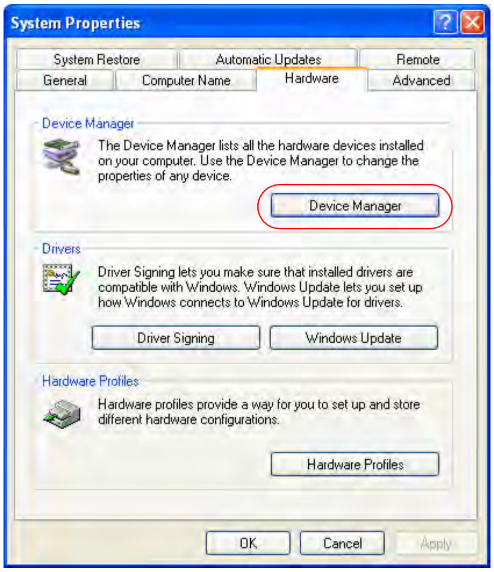
Note: By default, your Host IP for USB/net is 192.168.14.100.

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.



The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.

Hardware profiles provide a way for you to set up and store different hardware configurations.

Figure 5-10: 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.

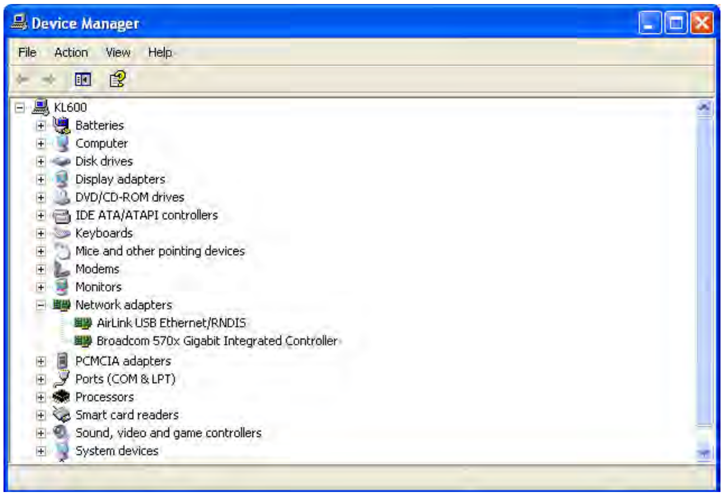


Figure 5-11: Device Manager - Ethernet

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

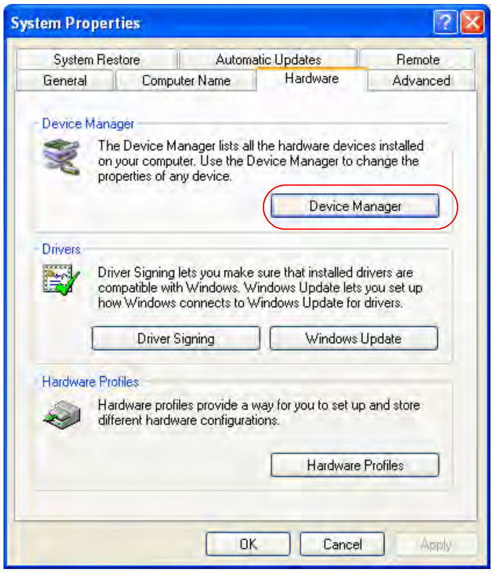
Virtual Serial

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.



The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.

Hardware profiles provide a way for you to set up and store different hardware configurations.

Figure 5-12: 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.*

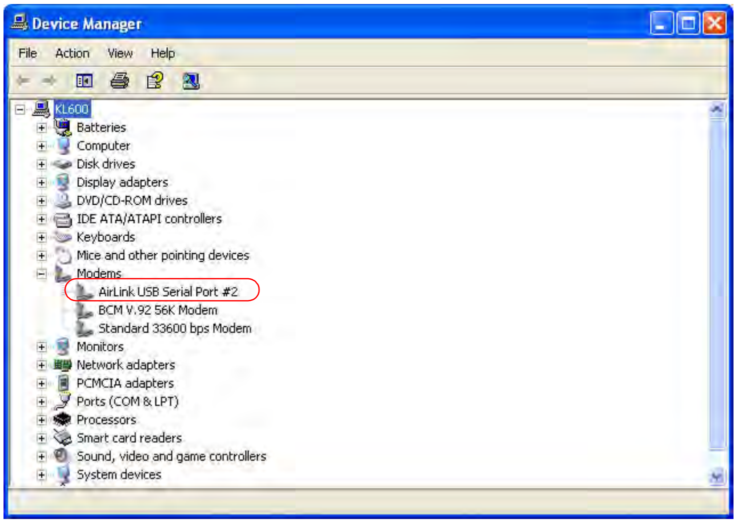


Figure 5-13: Device Manager - Serial

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.

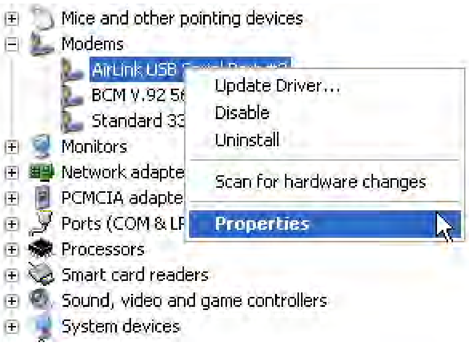
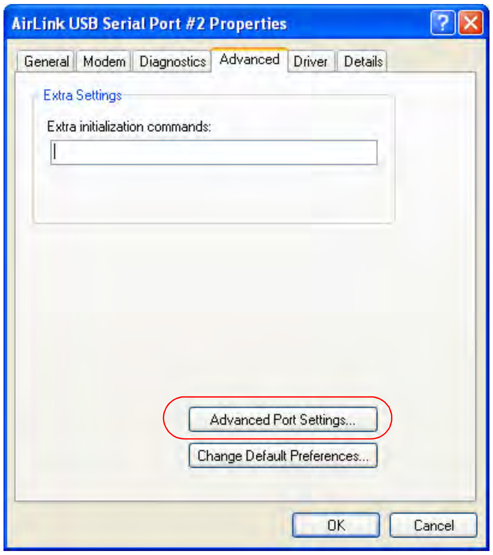


Figure 5-14: Device Manager: Driver menu

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



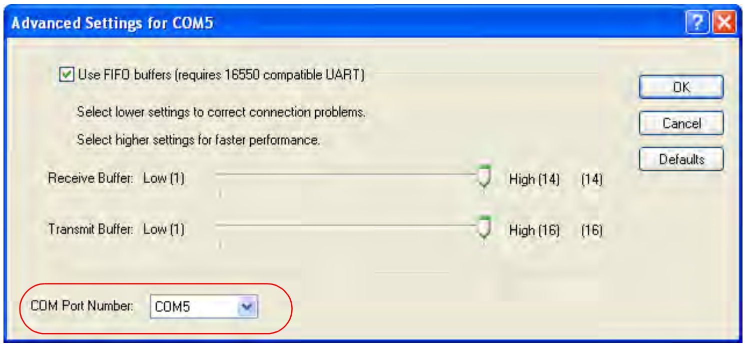
AirLink USB Serial Port #2 Properties

Extra Settings

Extra initialization commands:

Figure 5-15: 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.



Advanced Settings for COM5

☑ Use FIFO buffers (requires 16550 compatible UART)

Select lower settings to correct connection problems.

Select higher settings for faster performance.

Receive Buffer: Low (1) High (14) (14)

Transmit Buffer: Low (1) High (16) (16)

COM Port Number: COM5

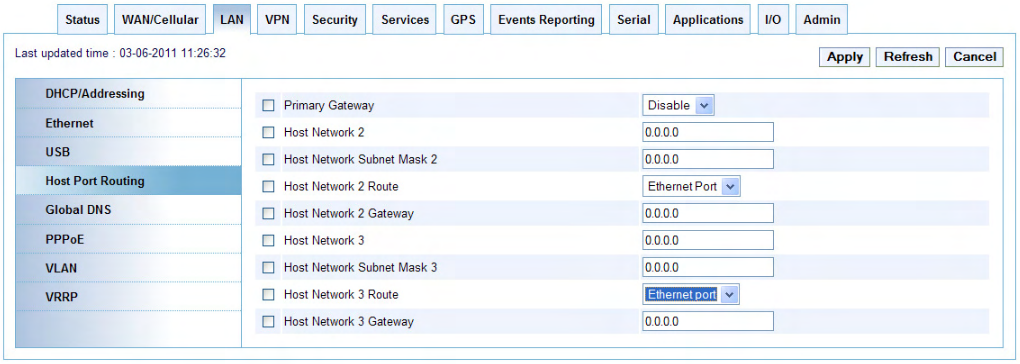
Figure 5-16: Advanced Settings

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.

Host Port Routing

The “Host Network” is the equivalent of the IP route command.



Last updated time : 03-06-2011 11:26:32

□ Primary Gateway	Disable
□ Host Network 2	0.0.0.0
□ Host Network Subnet Mask 2	0.0.0.0
□ Host Network 2 Route	Ethernet Port
□ Host Network 2 Gateway	0.0.0.0
□ Host Network 3	0.0.0.0
□ Host Network Subnet Mask 3	0.0.0.0
□ Host Network 3 Route	Ethernet port
□ Host Network 3 Gateway	0.0.0.0

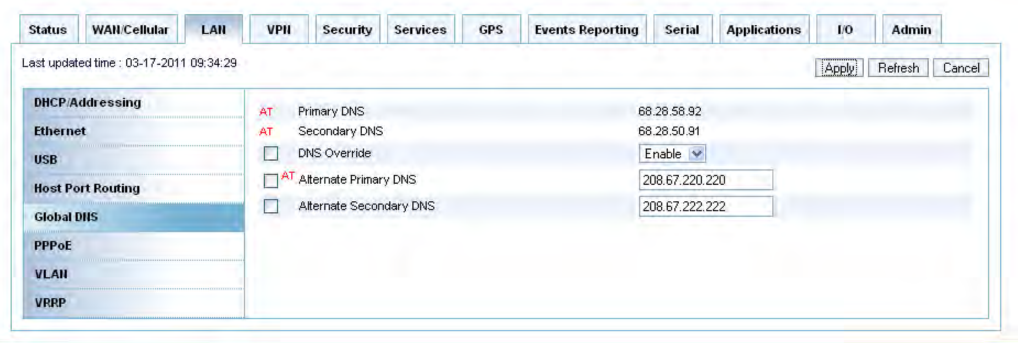
Figure 5-17: ACEmanager: LAN - Host Port Routing

Command	Description
Primary Gateway	When enabled, 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 interface connected to Ethernet. 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.

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.



Last updated time : 03-17-2011 09:34:29

AT	Primary DNS	68.28.58.92
AT	Secondary DNS	68.28.50.91
□	DNS Override	Enable
□ AT	Alternate Primary DNS	208.67.220.220
□	Alternate Secondary DNS	208.67.222.222

Figure 5-18: ACEmanager: LAN - Global DNS

Command	Description
Primary DNS	Primary carrier DNS IP Address. This and the secondary DNS are generally granted by the cellular network along with the Network IP.
Secondary DNS	Secondary carrier DNS IP Address.
DNS Override	Overrides the carrier DNS addresses with user configured ones. Some carriers will ignore the use of Alternate DNS servers and route all DNS requests to their own servers. Options: Disable or Enable. Default: Disable.
Alternate Primary DNS	Configurable DNS server to use instead of the cellular network granted one.
Alternate Secondary DNS	Configurable DNS server to use instead of the cellular network granted one.

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 (e.g., your AirLink device and your computer or router).

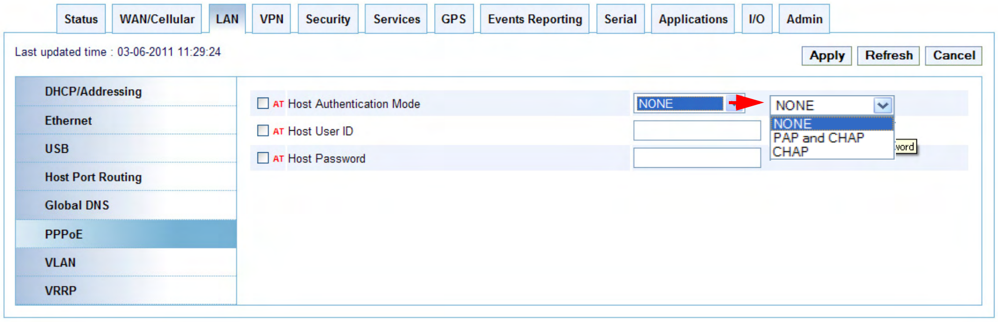
Application examples for PPPoE with your AirLink device:

- 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.



Last updated time : 03-06-2011 11:29:24

□ AT Host Authentication Mode NONE

NONE
NONE
PAP and CHAP
CHAP

□ AT Host User ID

□ AT Host Password

Figure 5-19: ACEmanager: LAN - 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. • NONE (Default) • PAP and CHAP • CHAP
Host User ID	Host User ID for PAP or CHAP. • user id (up to 64 bytes)
Host Password	Host Password for PAP or CHAP.

Configure the AirLink Device to Support PPPoE

Note: You must disable the DHCP server for PPPoE to work.

- From the groups on the left, select *PPPoE* under LAN.
- Change Host Authentication 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.*

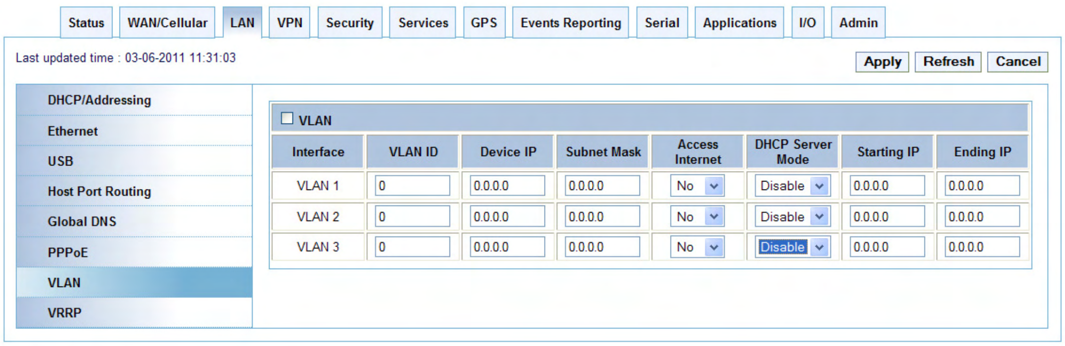
Optional: Configure *Device Name

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.

VLAN



Last updated time : 03-06-2011 11:31:03

□ VLAN

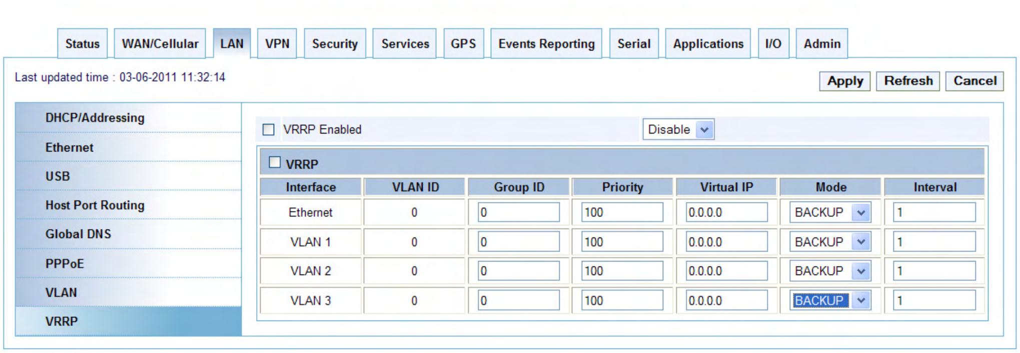
Interface	VLAN ID	Device IP	Subnet Mask	Access Internet	DHCP Server Mode	Starting IP	Ending IP
VLAN 1	0	0.0.0.0	0.0.0.0	No	Disable	0.0.0.0	0.0.0.0
VLAN 2	0	0.0.0.0	0.0.0.0	No	Disable	0.0.0.0	0.0.0.0
VLAN 3	0	0.0.0.0	0.0.0.0	No	Disable	0.0.0.0	0.0.0.0

Figure 5-20: ACEmanager: LAN - VLAN

Command	Description
Interface	Displays three VLAN IDs.
VLAN ID	Displays the VLAN ID.
Device IP	The IP address of the AirLink device for that VLAN interface.
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.
Access Internet	Choose access to the internet. Scroll down options: “Yes” or “No.”
DHCP Server Mode	Options are Enable and Disable. Default: Disable.
Starting IP	VLAN interface DHCP pool starting IP address.
Ending IP	The ending IP for the VLAN interface.

VRRP

VRRP (Virtual Router Redundancy Protocol) allows multiple routers to act as the default gateway router for a subnet, thereby reducing the possibility of a single point of failure.



Last updated time : 03-06-2011 11:32:14

☐ VRRP Enabled Disable

☐ VRRP

Interface	VLAN ID	Group ID	Priority	Virtual IP	Mode	Interval
Ethernet	0	0	100	0.0.0.0	BACKUP	1
VLAN 1	0	0	100	0.0.0.0	BACKUP	1
VLAN 2	0	0	100	0.0.0.0	BACKUP	1
VLAN 3	0	0	100	0.0.0.0	BACKUP	1

Figure 5-21: ACEmanager: LAN - VRRP

Command	Description
Interface	Displays Ethernet and three VLAN IDs.
VLAN ID	Displays the VLAN ID.
Group ID	Enter the VRRP Group ID. VRRP routers in the master and slave have the same Group ID.
Priority	VRRP decides whether the device is the master or slave. A greater value of priority indicates that the device is the master.
Virtual IP	If a device is configured with VRRP, the host connected to the device will display the Virtual ID. Virtual IP becomes the VRRP router’s Device IP.
Mode	Indicates whether the device is MASTER or BACKUP. The Priority number determines the master or backup status. Default: BACKUP.
Interval	VRRP advertised interval. Default: 1 second.

6: VPN Configuration

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) device, 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 four types of VPN: IPsec, GRE, SSL, and L2TP+IPsec. The AirLink device can support up to five VPN tunnels 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.

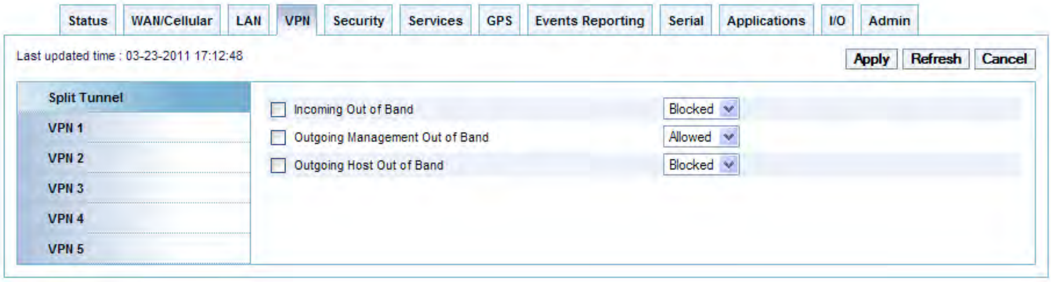
IPsec is a common network layer security control and is used to create a virtual private network (VPN).

The advantages of using the IPsec 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.

Split Tunnel

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



Last updated time : 03-23-2011 17:12:48

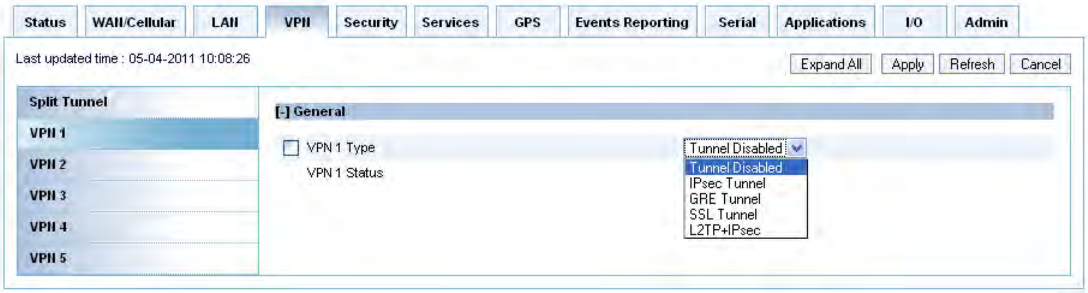
□ Incoming Out of Band	Blocked
□ Outgoing Management Out of Band	Allowed
□ Outgoing Host Out of Band	Blocked

Figure 6-1: ACEmanager: VPN - Split Tunnel

Field	Description
Incoming Out of Band	Allows all incoming out of band or out of tunnel traffic. Options: Blocked or Enabled. Default: Blocked.
Outgoing Management Out of Band	Outgoing ALEOS out of band can be blocked or allowed. Default: Allowed.
Outgoing Host Out of Band	Outgoing Host out of band can be blocked or allowed. Default: Blocked.

VPN 1

The VPN 1 tunnel can be configured as IPsec, GRE, SSL, or L2TP+IPsec. Enabling any of these tunnels will expose other options for configuring the tunnel.



Last updated time : 05-04-2011 10:08:26

□ VPN 1 Type: Tunnel Disabled

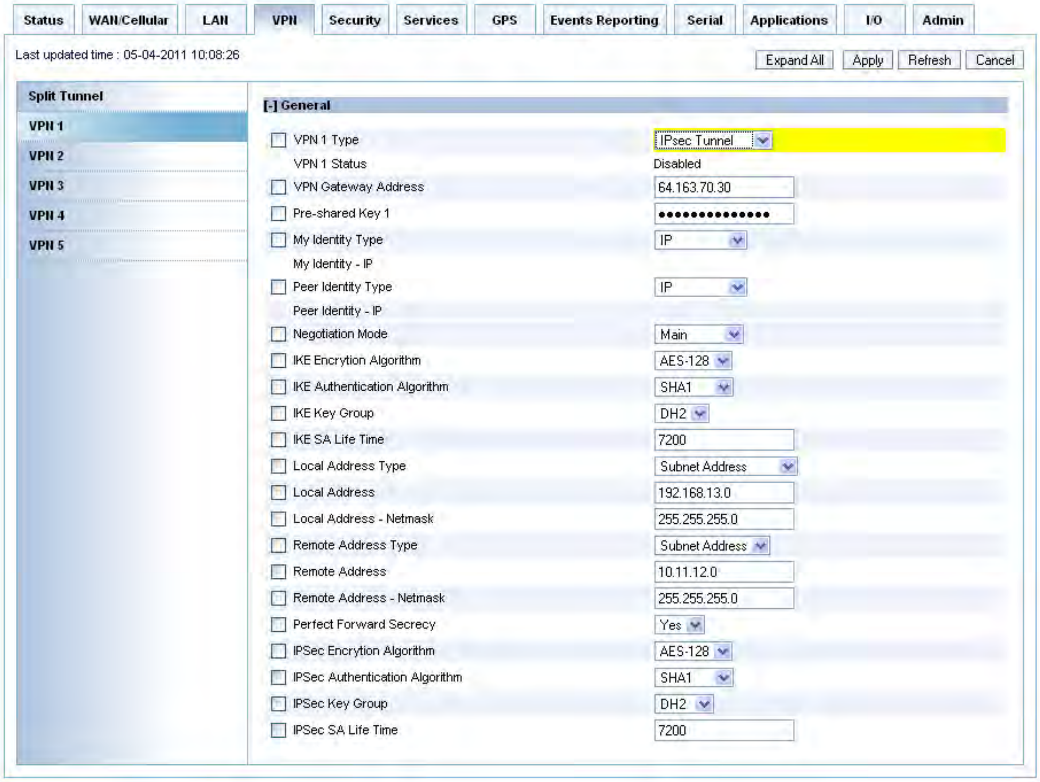
VPN 1 Status

Figure 6-2: ACEmanager: VPN - VPN 1

IPsec

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.

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.



Last updated time : 05-04-2011 10:08:26

[-] General

□ VPN 1 Type	IPsec Tunnel
VPN 1 Status	Disabled
□ VPN Gateway Address	64.163.70.30
□ Pre-shared Key 1	••••••••••••••
□ My Identity Type	IP
My Identity - IP	
□ Peer Identity Type	IP
Peer Identity - IP	
□ Negotiation Mode	Main
□ IKE Encryption Algorithm	AES-128
□ IKE Authentication Algorithm	SHA1
□ IKE Key Group	DH2
□ IKE SA Life Time	7200
□ Local Address Type	Subnet Address
□ Local Address	192.168.13.0
□ Local Address - Netmask	255.255.255.0
□ Remote Address Type	Subnet Address
□ Remote Address	10.11.12.0
□ Remote Address - Netmask	255.255.255.0
□ Perfect Forward Secrecy	Yes
□ IPSec Encryption Algorithm	AES-128
□ IPSec Authentication Algorithm	SHA1
□ IPSec Key Group	DH2
□ IPSec SA Life Time	7200

Figure 6-3: ACEmanager: VPN 1 - VPN - IPsec Tunnel

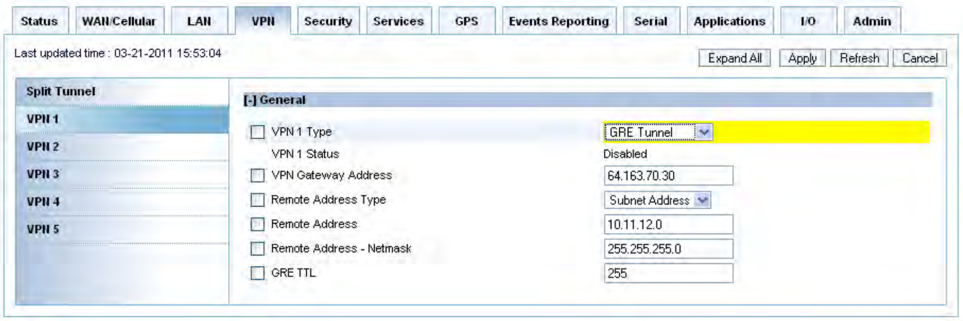
Field	Description
VPN # Type	Use this field to enable or disable the VPN # tunnel. If custom settings are used, they will be saved and the tunnel can be disabled and re-enabled without needing to reenter any of the settings. For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink Device VPN and the enterprise VPN server. Options: • Tunnel Disabled • IPsec Tunnel • GRE Tunnel • SSL Tunnel • L2TP+IPsec Default: Tunnel Disabled.
VPN # Status	Indicates the current status of the VPN # connection. Use this when troubleshooting a VPN # connection. Options: Disabled, Not Connected, or Connected.
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.
Pre shared Key 1	Pre-shared Key (PSK) used to initiate the VPN tunnel.

Field	Description
My Identity Type	Options: - IP (default) - The My Identity - IP field displays with the WAN IP address assigned by the carrier - FQDN - The My Identity - FQDN field displays. Enter a fully qualified domain name (FQDN) e. g., modemname.domainname.com - User FQDN - The My Identity - FQDN field displays. Enter a User FQDN whose values should include a username (E.g., user@domain.com).
My Identity - FQDN or **My Identity - IP**	My Identity - FQDN displays only when User FQDN or FQDN is selected from the My Identity Type drop-down menu. Enter an FQDN or User FDQN. My Identity - IP displays only when IP is selected from the My Identity Type drop-down menu. The WAN IP address assigned by the carrier displays.
Peer Identity Type	Required in some configurations to identify the client or peer side of a VPN connection. Options: - IP (default) - The Peer Identity - IP field displays with the IP address of a VPN server set up by Sierra Wireless for your testing purposes - FQDN - The Peer Identity - FQDN field displays. Enter an FQDN (E. g., modemname.domainname.com) - User FQDN - The Peer Identity - FQDN field displays. Enter a User FQDN whose values should include a username (E.g., user@domain.com).
Peer Identity - IP or **Peer Identity - FQDN**	Peer Identity - FQDN displays only when User FQDN or FQDN is selected from the Peer Identity Type drop-down menu. Enter the Peer FQDN or Peer User FQDN. Peer Identity - IP displays only when IP is selected from the Peer Identity Type drop-down menu. The VPN Gateway IP Address displays.
Negotiation Mode	Enable this configuration to operate the onboard VPN under Aggressive mode. Aggressive mode offers increased performance at the expense of security. Options: Main Mode or Aggressive Mode. Default: Main Mode.
IKE Encryption Algorithm	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 both 128-bit and 256-bit encryption. Options: DES, Blowfish, 3DES, Cast 128, AES-128, and AES-256. Default: AES-128.
IKE Authentication Algorithm	MD5 is an algorithm that produces a 128-bit digest for authentication. SHA1 is a more secure algorithm that produces a 160-bit digest. Options: MD5, SHA1, and SHA256. Default: SHA1.
IKE Key Group	Options: DH1, DH2, or DH5. Default: DH2
IKE SA Life Time	Determines how long the VPN tunnel is active in seconds. Options: 180 to 86400. Default: 7200.
Local Address Type	The network information of the device. Options: Use the Host Subnet, Single Address, and Subnet Address. Default: Subnet Address.
Local Address	Device subnet address.
Local Address - Netmask	Device subnet mask information. 24-bit netmask. Default: 255.255.255.0
Remote Address Type	The network information of the IPsec server behind the IPsec gateway. Options: Subnet Address and Single Address. Default: Subnet Address.
Remote Address	The IP address of the device behind the gateway.

Field	Description
Remote Address - Netmask	Remote subnet mask information. 24-bit netmask. Default: 255.255.255.0
Perfect Forward Secrecy	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. Options: Yes or No.
IPsec Encryption Algorithm	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 both 128-bit and 256-bit encryption. Options: None, DES, 3DES, AES-128, Blowfish, Cast 128, and AES-256. Default: AES-128.
IPsec Authentication Algorithm	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. Options: None, MD5, SHA1, and SHA 256. Default: SHA1.
IPsec Key Group	Determines how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during 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). Options: DH1, DH2, or DH5.
IPsec SA Life Time	Determines how long the VPN tunnel is active in seconds. Options: 180 to 86400. Default: 7200.

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 feature you can reconfigure IP architectures without worrying about connectivity. GRE creates a point-to-point link between routers on an IP network.



Last updated time : 03-21-2011 15:53:04

□ VPN 1 Type	GRE Tunnel
VPN 1 Status	Disabled
□ VPN Gateway Address	64.163.70.30
□ Remote Address Type	Subnet Address
□ Remote Address	10.11.12.0
□ Remote Address - Netmask	255.255.255.0
□ GRE TTL	255

Figure 6-4: ACEmanager: VPN - VPN1- GRE Tunnel

Please refer to the IPsec table for parameter descriptions.

Field	Description
VPN # Type	Options: Tunnel Disabled or GRE Tunnel. Enabling the GRE Tunnel will expose other options for configuring the tunnel.
VPN # Status	Indicates the status of the GRE tunnel on the device. Options: Disabled, Connected or Not Connected.
VPN Gateway Address	The IP address of the device that this client connects to. This IP address must be open to connections from the device.
Remote Address Type	The network information of the GRE server behind the GRE gateway.
Remote Address	The IP address of the device behind the gateway.
Remote Address - Netmask	The subnet network mask of the device behind the GRE gateway. *Note: Never use a 16-bit subnet mask: GRE tunnel establishment will fail.*
GRE TTL	GRE time to live (TTL) value is the upper bound on the time that a GRE packet can exist in a network. In practice, the TTL field is reduced by one on every router hop. This number is in router hops and not in seconds.

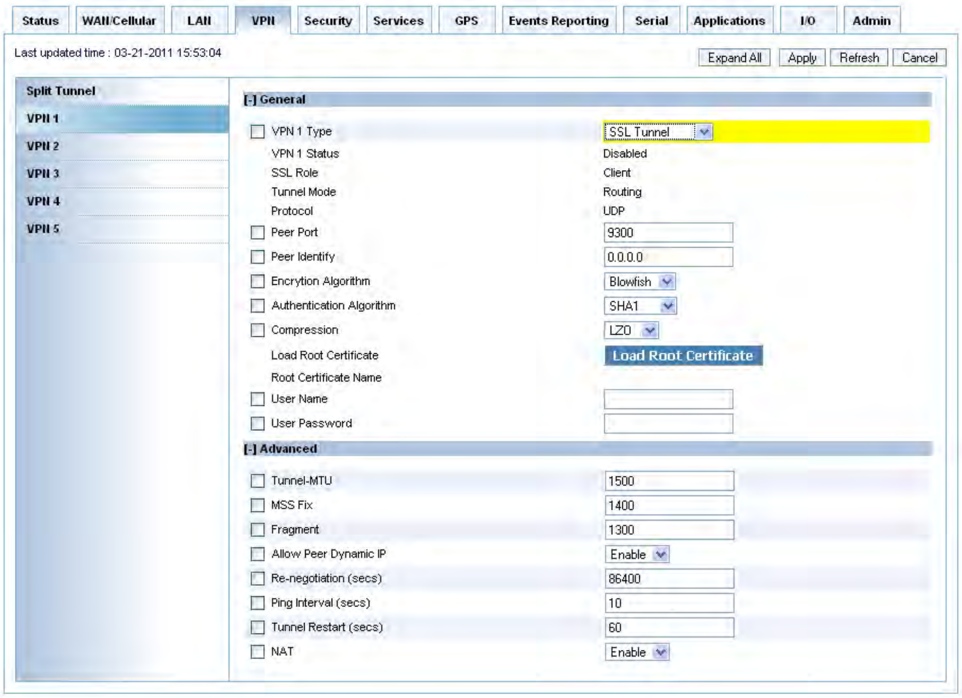
SSL Tunnel

The SSL tunnel allows the device and the server to communicate across a network securely. SSL provides endpoint authentication and secure communications over the Internet.

If the SSL tunnel is selected, the user can opt to secure remote communications via SSL.

The AirLink device client will authenticate the server using a PKI certificate. The server will authenticate the client via username and password. The Root CA certificate for the server certificate must be loaded on the device.

Note: SSL tunnel is based on the OpenVPN open source package. AirLink devices are SSL clients and will only talk to an SSL server (also based on the OpenVPN package).



Last updated time : 03-21-2011 15:53:04

[-] General

□ VPN 1 Type	SSL Tunnel
VPN 1 Status	Disabled
SSL Role	Client
Tunnel Mode	Routing
Protocol	UDP
□ Peer Port	9300
□ Peer Identify	0.0.0.0
□ Encrytion Algorithm	Blowfish
□ Authentication Algorithm	SHA1
□ Compression	LZO
Load Root Certificate	Load Root Certificate
Root Certificate Name	
□ User Name	
□ User Password	

[-] Advanced

□ Tunnel-MTU	1500
□ MSS Fix	1400
□ Fragment	1300
□ Allow Peer Dynamic IP	Enable
□ Re-negotiation (secs)	86400
□ Ping Interval (secs)	10
□ Tunnel Restart (secs)	60
□ NAT	Enable

Figure 6-5: ACEmanager: VPN - VPN1- SSL Tunnel

Field	Description
VPN 1 Type	Options: Tunnel Disabled or SSL Tunnel. Enabling the SSL Tunnel will expose other options for configuring the tunnel.
VPN 1 Status	Indicates the status of the SSL tunnel on the device. Options: Disabled, Connected or Not Connected.
SSL Role	The AirLink device can only be an SSL client. Default: Client.
Tunnel Mode	The Tunnel Mode is set to “Routing”.

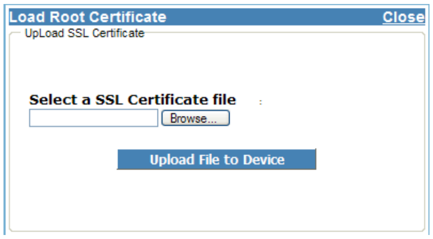
Field	Description
Protocol	Displays the protocol used for configuration. Only supports UDP.
Peer Port	The Peer Port is the UPD port on the peer device.
Peer Identity	Enter the IP address or Fully Qualified Domain Name (FQDN) of the peer device.
Encryption Algorithm	Options: DES, Blowfish, DES, Cast128, AES-128, and AES-256
Authentication Algorithm	Options: MD5, SHA-1, and SHA-256.
Compression	Options: LZ0 or NONE.
Load Root Certificate	Load Root Certificate loads the server root CA certificate. When the button is selected, a window will pop-up and enable the user to browse and select the file containing the root CA certificate.
Root Certificate Name	The Root Certificate Name will display here.
User Name	The user name required for client authentication.
User Password	The user password required for client authentication.
Tunnel-MTU	Default: 1500 bytes.
MSS Fix	Default: 1400 bytes.
Fragment	Default: 1300 bytes.
Allow Peer Dynamic IP	Options: Enable or Disable.
Re-negotiation (seconds)	Default: 24 hours.
Ping Interval (seconds)	This is the keep-alive sent by the client. Default: 0 seconds.
Tunnel Restart (seconds)	Enter the time for a tunnel restart (unit in seconds).
NAT	Options: Enable or Disable. Note that this is a Carrier NAT, not a local NAT.

Load Root Certificate

Once an user accepts the default certificate, the SSL connection can be completed.

To load a root certificate,

1. Click on Load Root Certificate.
2. A dialog-box displays. Select a SSL Certificate File.



3. Click on Upload File to Device.

L2TP+IPsec

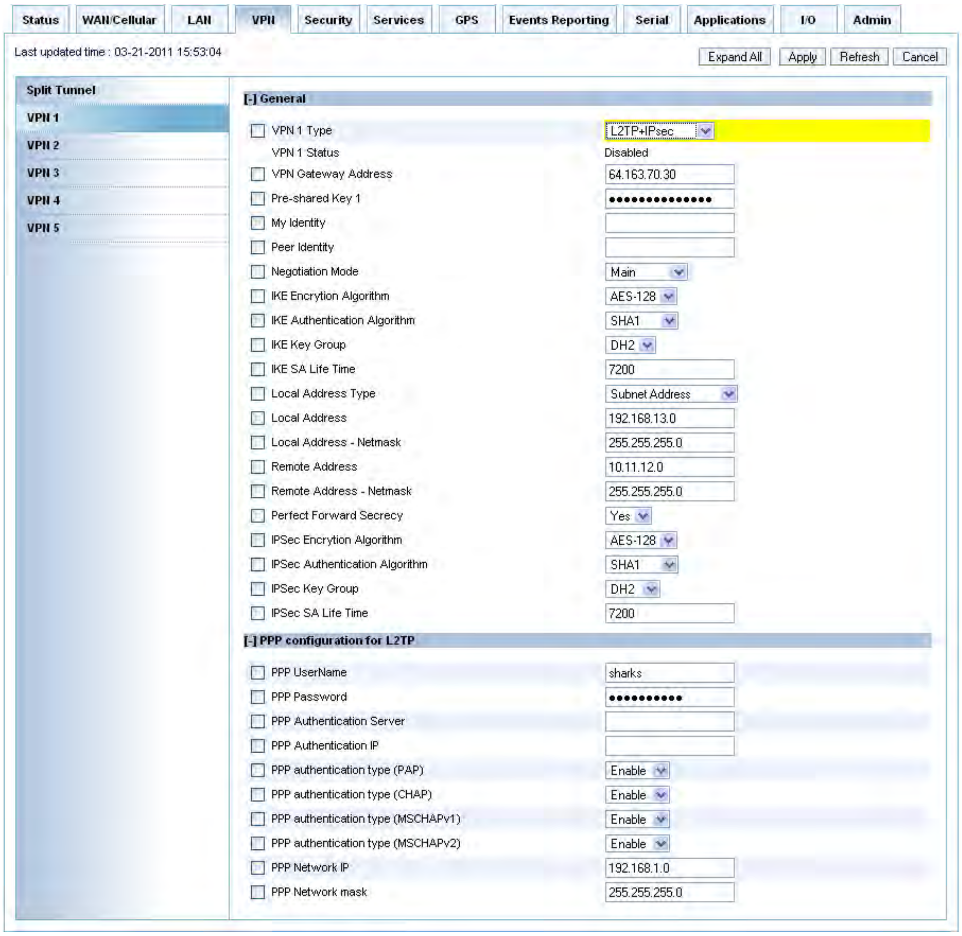
Layer 2 Tunneling Protocol (L2TP) is an standard protocol for encapsulating PPP data packets and passing them transparently across an IP network. Typically, L2TP is used as a tunneling protocol to support VPNs. It does not provide security (encryption or confidentiality) by itself, but relies on an encryption protocol that it passes within the tunnel for security.

L2TP is a point-to-point connection tunnel establishment. L2TP by default uses UDP port 1701.

PPP sessions within the L2TP tunnel supports the following authentication using username and password:

- PAP
- CHAP
- MSCHAPv1
- MSCHAPv2

The authentication method used in the connection is selected through negotiation between the PPP endpoints. The PPP configuration is only available on VPN tunnel.



Last updated time : 03-21-2011 15:53:04

[-] General

□ VPN 1 Type	L2TP+IPsec
VPN 1 Status	Disabled
□ VPN Gateway Address	64.163.70.30
□ Pre-shared Key 1	••••••••••••••
□ My Identity	
□ Peer Identity	
□ Negotiation Mode	Main
□ IKE Encryption Algorithm	AES-128
□ IKE Authentication Algorithm	SHA1
□ IKE Key Group	DH2
□ IKE SA Life Time	7200
□ Local Address Type	Subnet Address
□ Local Address	192.168.13.0
□ Local Address - Netmask	255.255.255.0
□ Remote Address	10.11.12.0
□ Remote Address - Netmask	255.255.255.0
□ Perfect Forward Secrecy	Yes
□ IPSec Encryption Algorithm	AES-128
□ IPSec Authentication Algorithm	SHA1
□ IPSec Key Group	DH2
□ IPSec SA Life Time	7200

[-] PPP configuration for L2TP

□ PPP UserName	sharks
□ PPP Password	••••••••••
□ PPP Authentication Server	
□ PPP Authentication IP	
□ PPP authentication type (PAP)	Enable
□ PPP authentication type (CHAP)	Enable
□ PPP authentication type (MSCHAPv1)	Enable
□ PPP authentication type (MSCHAPv2)	Enable
□ PPP Network IP	192.168.1.0
□ PPP Network mask	255.255.255.0

Figure 6-6: ACEmanager: VPN - VPN1- L2TP+IPsec

To configure each LTTP tunnel:

1. Configure PPP instance
2. Configure L2TP

- Local Address Type field changes to single address.
- Local Address will be carrier given address of the device (with a 24 Bit Netmask).
- Remote Address will be VPN gateway address with 24-bit Netmask.

3. Configure IPsec route
4. Configure static route - PPP Network IP and PPP Network Mask

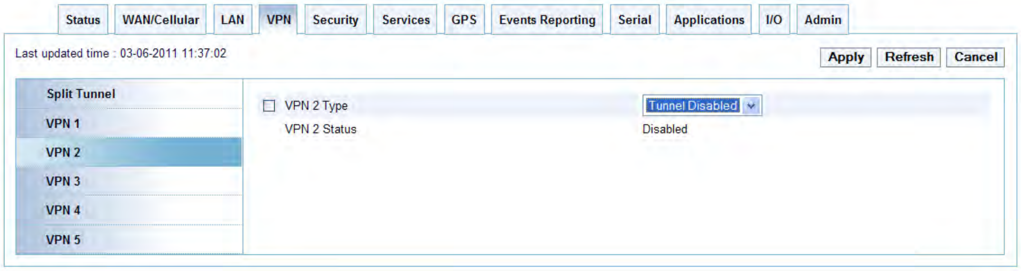
Field	Description
General	
VPN # Type	Use this field to enable or disable the VPN # tunnel. If custom settings are used, they will be saved and the tunnel can be disabled and re-enabled without needing to reenter any of the settings. For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink Device VPN and the enterprise VPN server. Options: • Tunnel Disabled • IPsec Tunnel • GRE Tunnel • SSL Tunnel • L2TP+IPsec Default: Tunnel Disabled.
VPN # Status	Indicates the current status of the VPN # connection. Use this when troubleshooting a VPN # connection. Options: Disabled, Not Connected, or Connected.
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.
Pre shared Key 1	Pre-shared Key (PSK) used to initiate the VPN tunnel.
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. Default: The VPN server IP address.
Negotiation Mode	Enable this configuration to operate the onboard VPN under Aggressive mode. Aggressive mode offers increased performance at the expense of security. Options: Main Mode or Aggressive Mode. Default: Main Mode.
IKE Encryption Algorithm	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 both 128-bit and 256-bit encryption. Options: DES, Blowfish, 3DES, Cast 128, AES-128, and AES-256. Default: AES-128.
IKE Authentication Algorithm	MD5 is an algorithm that produces a 128-bit digest for authentication. SHA1 is a more secure algorithm that produces a 160-bit digest. Options: MD5, SHA1, and SHA256. Default: SHA1.
IKE Key Group	Options: DH1, DH2, or DH5. Default: DH2
IKE SA Life Time	Determines how long the VPN tunnel is active in seconds. Options: 180 to 86400. Default: 7200.
Local Address Type	The network information of the device. Options: Use the Host Subnet, Single Address, and Subnet Address. Default: Subnet Address.
Local Address	Device subnet address.
Local Address - Netmask	Device subnet mask information. 24-bit netmask. Default: 255.255.255.0

Field	Description
Remote Address	The IP address of the device behind the gateway.
Remote Address - Netmask	Remote subnet mask information. 24-bit netmask. Default: 255.255.255.0
Perfect Forward Secrecy	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. Options: Yes or No.
IPsec Encryption Algorithm	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 both 128-bit and 256-bit encryption. Options: None, DES, 3DES, AES-128, Blowfish, Cast 128, and AES-256. Default: AES-128.
IPsec Authentication Algorithm	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. Options: None, MD5, SHA1, and SHA 256. Default: SHA1.
IPsec Key Group	Determines how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during 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). Options: DH1, DH2, or DH5.
IPsec SA Life Time	Determines how long the VPN tunnel is active in seconds. Options: 180 to 86400. Default: 7200.
PPP configuration for L2TP	
PPP User Name	Enter a PPP User Name. This user name needs to be entered as per the configuration on the router.
PPP Password	Enter a PPP Password
PPP Authentication Server	By default no PPP Authentication server is used.
PPP Authentication IP	If you are using an authentication server, enter your PPP authentication IP.
PPP authentication type (PAP)	*Note: PPP authentication parameters are independently configurable authentication methods. All PPP authentication type fields are enabled by default.* If you enable PAP, configure the following: • PAP Username • PAP Password • PAP Server (optional, if not set, the server uses the above password) • PAP IP Address (optional, if not set, any local IP address is acceptable)
PPP authentication type (chap)	If you enable CHAP, MSCHAPv1, or MSCHAPv2, then the following parameters can be configured: • PAP Username • PAP Password • PAP Server (optional, if not set, the server uses the above password) • PAP IP Address (optional, if not set, any local IP address is acceptable)
PPP authentication type (MSCHAPv1)	
PPP authentication type (MSCHAPv2)	

Field	Description
PPP Network IP	IPsec server network behind the IPsec concentrator. The network connected to the remote end of the PPP connection.
PPP network Mask	The network mask of the remote PPP network.

VPN 2 to VPN 5

The VPN 2 through VPN 5 sections only allow configuration of the IPsec and GRE tunnels on the device. Figure 6-3 shows the screen display for the VPN 2 submenu; screen data fields for the VPN 3, 4, and 5 submenus are identical.



Last updated time : 03-06-2011 11:37:02

□ VPN 2 Type: Tunnel Disabled

VPN 2 Status: Disabled

Figure 6-7: ACEmanager: VPN - VPN 2

There are three options in the scroll down menu: Tunnel Disabled, IPsec Tunnel, and GRE Tunnel. Enabling the IPsec or GRE Tunnel will expose other options for configuring that tunnel. The options shown in Figures 6-3 and 6-4 for VPN 1 are the same for VPNs 2 through 5.

7: Security Configuration

The Security tab that displays in ACEmanager is applicable to Sierra Wireless AirLink GX400 devices.

The security tab covers firewall-type functions. These functions include how data is routed or restricted from one side of the device to the other, i.e., 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.

The DMZ is used to direct unsolicited inbound traffic to a specific LAN connected host, such as a computer running a web server or other internal application. The DMZ with public mode is particularly useful for certain services like VPN, NetMeeting, and streaming video that may not work well with a NAT router.

Options for DMZ are Automatic, Manual, and Disable.

Automatic uses the first connected host. If more than one host is available (multiple Ethernet on a switch connected to the device and/or Ethernet with USB/net) and you want to specify the host to use as the DMZ, select Manual and enter the IP address of the desired host.

Note: Port Forwarding and DMZ require Private Mode.

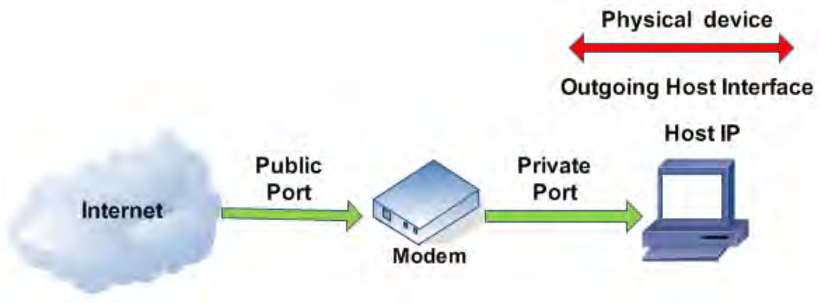
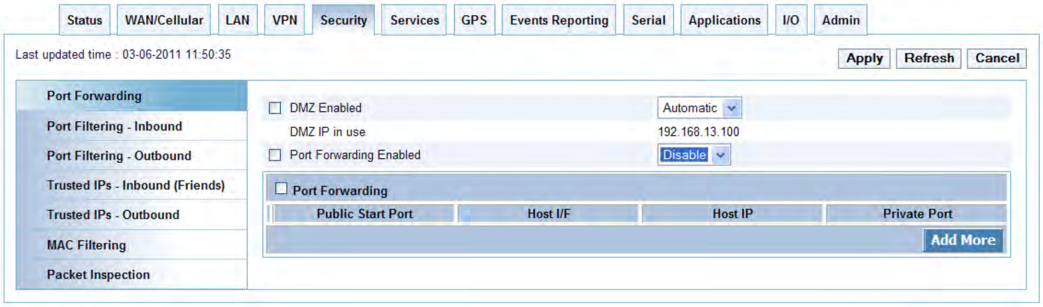


Figure 7-1: Port Forwarding



Last updated time : 03-06-2011 11:50:35

☐ DMZ Enabled	Automatic
DMZ IP in use	192.168.13.100
☐ Port Forwarding Enabled	Disable

☐ Port Forwarding

Public Start Port	Host I/F	Host IP	Private Port

Figure 7-2: ACEmanager: Security - Port Forwarding

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

Field	Description
DMZ Enabled	The AirLink device allows a single client to connect to the Internet through a demilitarized zone (DMZ). Options are Automatic, Manual, and Disable. Default: Automatic. • Automatic - enables the first connected host or the Public Mode interface as the DMZ. • Manual - inserts a specific IP address in the DMZ IP field • Disable - no connected host receives unsolicited traffic from the cellular network or Internet.
DMZ IP	This field only displays if Manual is selected for the DMZ Enabled field; this field does not display if the DMZ is disabled. This is the IP address of the private mode host that should be used as the DMZ.
DMZ IP in use	IP address of the host to which inbound unsolicited packets will be sent. When the device passes the Network IP to the configured public host, the DMZ IP in Use displays the public IP.
Port Forwarding Enabled	Enables port forwarding rules. Options are Enable and Disable. Default: Disable.
Port Forwarding	
Public Start Port	A single port on the public network (cellular network accessible).
Host I/F	The protocol to be used with the forwarded port: TCP or UDP. Only connections of that type on that port will be forwarded.
Host IP	IP address of a device connected to the Host I/F interface.
Private Port	The single port on the device at the Host IP.

The following is an example of configuring a port forward rule for a 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. Select Ethernet as the Host I/F.
5. Enter 192.168.13.100 as the Host IP.
6. 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.

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.

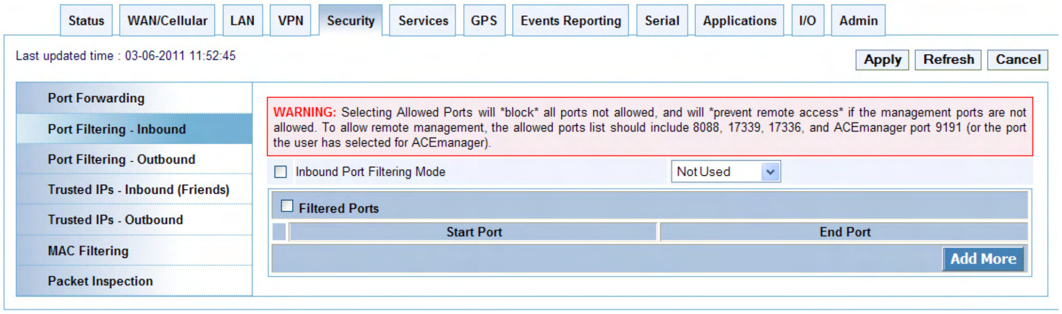
Port Filtering - Inbound

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.



Last updated time : 03-06-2011 11:52:45

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).

☐ Inbound Port Filtering Mode: Not Used

☐ Filtered Ports

	Start Port	End Port

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

Field	Description
Inbound Port Filtering Mode	Options: • Not Used • Blocked Ports - ports though which traffic is blocked. Listed below. • Allowed Ports - ports through which traffic is allowed. Listed below. Default: Not Used
Filtered Ports	
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).*

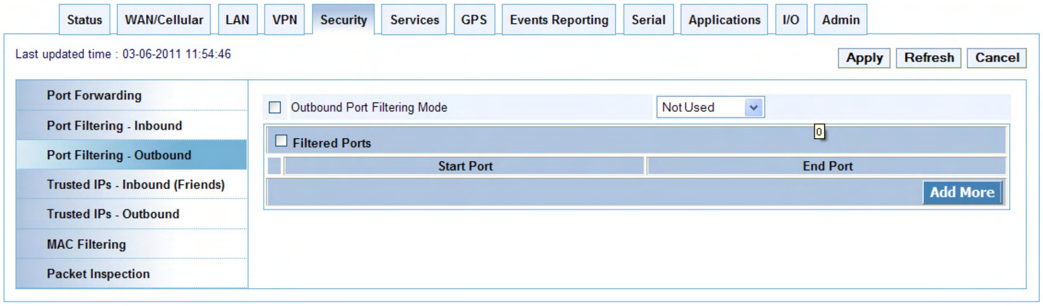
Port Filtering - Outbound

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.



Last updated time : 03-06-2011 11:54:46

□ Outbound Port Filtering Mode: Not Used

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

Field	Description
Outbound Port Filtering Mode	Allowed and blocked ports through which traffic is either allowed or blocked (respectively) are listed. Default: Not Used. *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.

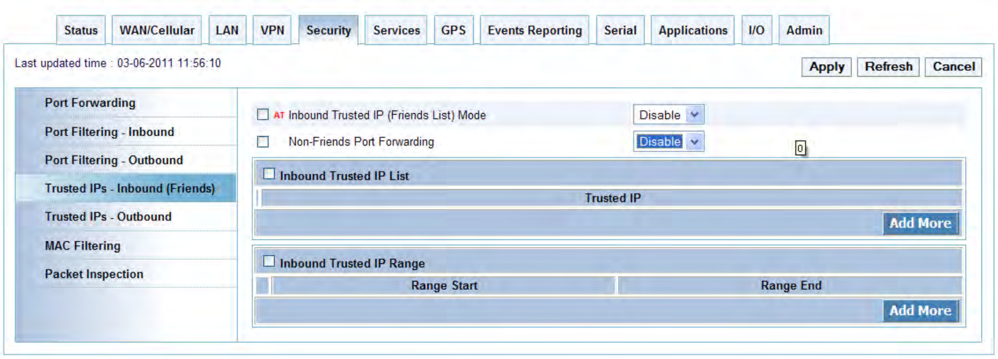
Trusted IPs - Inbound (Friends)

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.



Last updated time : 03-06-2011 11:56:10

☐ AT Inbound Trusted IP (Friends List) Mode — Disable

☐ Non-Friends Port Forwarding — Disable

0

☐ Inbound Trusted IP List

Trusted IP

☐ Inbound Trusted IP Range

Range Start | Range End

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

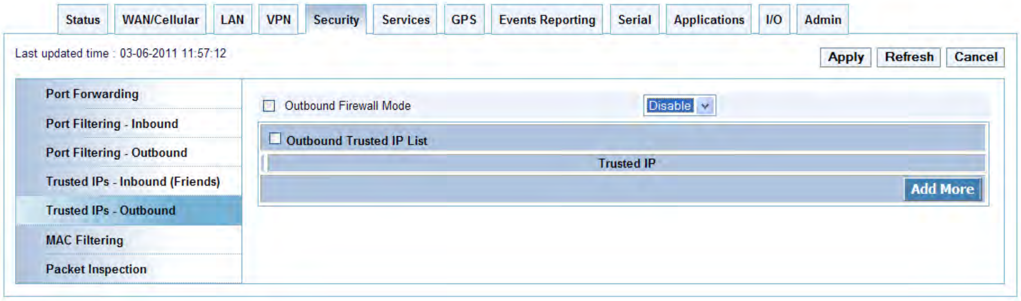
Field	Description
Inbound Trusted IP (Friend's List) Mode	Disables or Enables port forwarding rules. Options are Disable or Enable. Default: Disable.
Non-Friends Port Forwarding	Non-Friends port forwarding is like an allow rule for any of the forwarded ports. If it is enabled, the port forwarding rules apply to all incoming packets. If it is disabled, only Friends List IPs get through. Options are Disable or Enable. Default: Disable.
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 - Outbound

Trusted IPs-Outbound restricts LAN access to the external network (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.



Last updated time : 03-06-2011 11:57:12

☐ Outbound Firewall Mode Disable

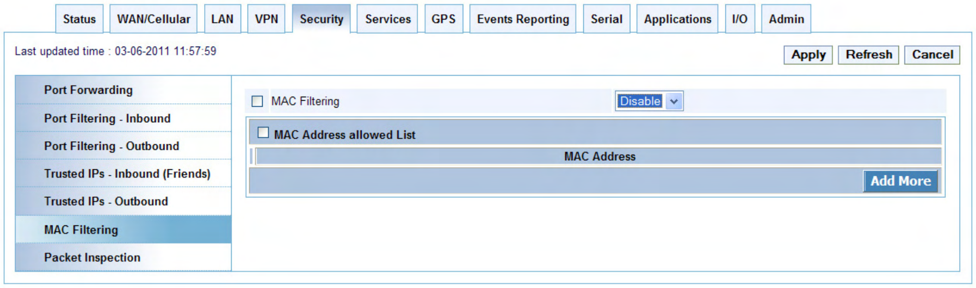
☐ Outbound Trusted IP List

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

Field	Description
Outbound Firewall Mode	Disables or Enables port forwarding rules. Options are Disable or Enable. Default: Disable.
Outbound Trusted IP List	Each entry can be configured to allow a single IP address (e.g., 64.100.100.2) or the IP addresses from a complete subnet (e.g., 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 block or allow a connection from a computer or other device by blocking or allowing the MAC address of its network interface adapter.



Last updated time : 03-06-2011 11:57:59

□ MAC Filtering: Disable

□ MAC Address allowed List

MAC Address

Figure 7-7: ACEmanager: Security - MAC Filtering

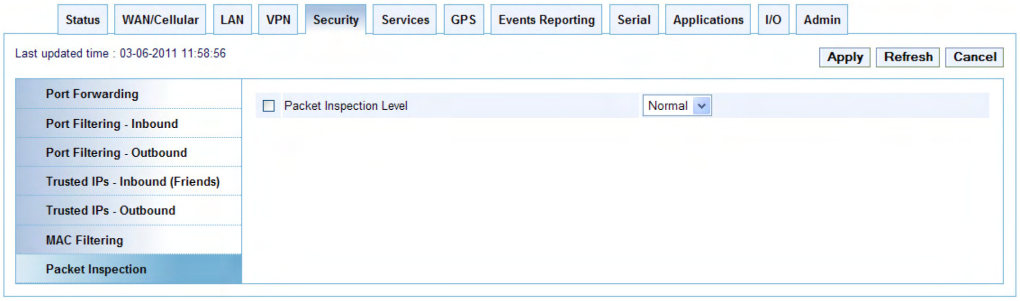
Field	Description
MAC Filtering	Enable or disable MAC Filtering. Default: Disable.
MAC Address allowed List	Allows or blocks the MAC Addresses listed. Add MAC addresses by clicking on the *Add More* button.
MAC Address	This is the MAC Address of the interface adapter on a computer or other device. **Tip:** *You can use the Status > LAN table to obtain the MAN addresses of connected hosts.*

Packet Inspection

The Packet Inspection group supports two modes of security: Normal (default)and High Security. A Stateful Packet Inspection (SPI) firewall is a firewall that tracks the states of network connections and makes decisions on packet forwarding based on the states defined in the accept or reject policy rules.

Use of an SPI firewall allows for additional device security by implementing default packet state filtering policies.

Such a firewall will typically pass all outgoing packets through but will only allow incoming packets if they are part of an “Established” connection, ensuring security. Stateful firewalls are able to track the state of flows in connectionless protocols (UDP) and connection oriented protocols (TCP).



Last updated time : 03-06-2011 11:58:56

□ Packet Inspection Level Normal

Figure 7-8: ACEmanager: Security - MAC Filtering

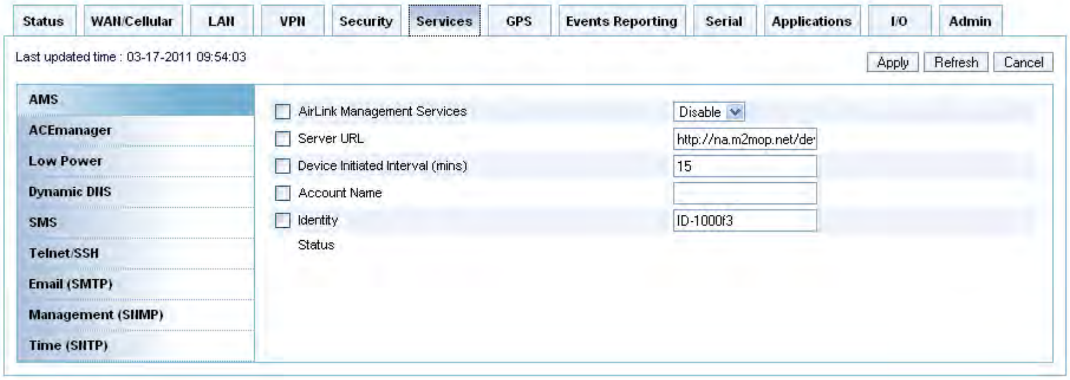
Field	Description
Packet Inspection Level	Enable or disable MAC Filtering. Default: Normal.

8: Services Configuration

The Services tab that displays in ACEmanager is applicable to the Sierra Wireless AirLink GX400.

The sections of the Services tab allow the configuration of external services that extend the functionality of the AirLink device.

AMS (AirLink Management Services)



Last updated time : 03-17-2011 09:54:03

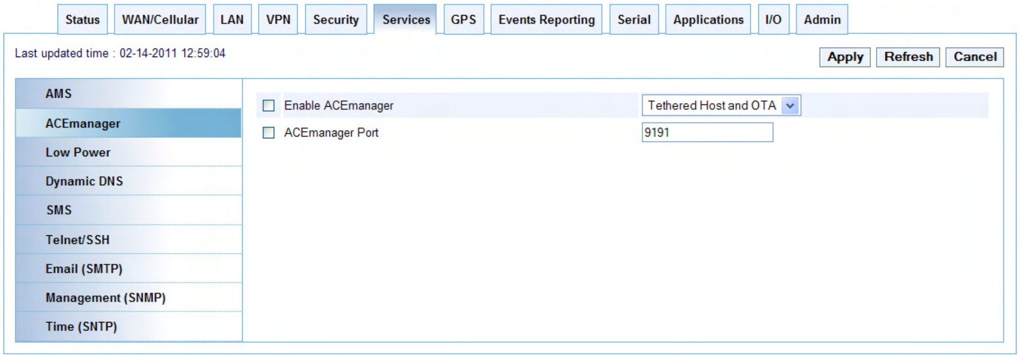
□ AirLink Management Services	Disable
□ Server URL	http://na.m2mop.net/de
□ Device Initiated Interval (mins)	15
□ Account Name	
□ Identity	ID-1000f3
Status	

Figure 8-1: ACEmanager: Services - AMS

Field	Description
AirLink Management Services	Disables or enables AMS management via the AMS Device Initiated feature.
Server URL	The AMS server URL address. By default, this is http://na.m2mop.net/device/msci

Field	Description
Device Initiated Interval (mins)	This field determines how often the AirLink device checks for software updates and settings changes from AMS. AMS can also query the AirLink device at a regular interval if settings allow. Refer to AirLink Management Services documentation for more information. Default: 15 minutes.
Account Name	Displays your account name.
Identity	Displays the identity number.
Status	Displays the status of the AMS connection.

ACEmanager



Last updated time : 02-14-2011 12:59:04

□ Enable ACEmanager: Tethered Host and OTA

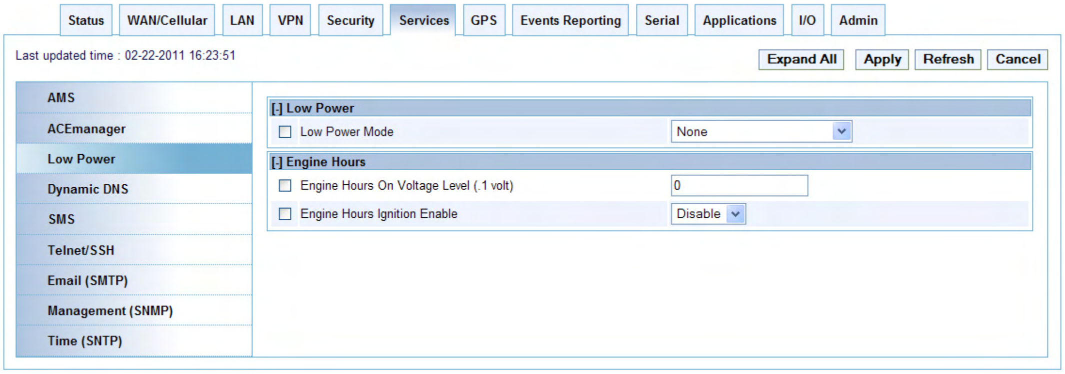
□ ACEmanager Port: 9191

Figure 8-2: ACEmanager: Services - ACEmanager

Field	Description
Enable ACEmanager	Configures the availability for connections to ACEmanager: Tethered Host (Ethernet, USB/net, or DUN), OTA (remote connections), and WiFi. Default: Tethered Host and OTA
ACEmanager Port	Identifies the port set for ACEmanager (9191 in Figure 8-2 example). Reboot the device if you change the port settings.

Low Power

The AirLink device switches into Low Power mode when configured events occur. Low Power mode is a standby mode in which the device uses minimal power while being ready to activate quickly.



Last updated time : 02-22-2011 16:23:51

[-] Low Power

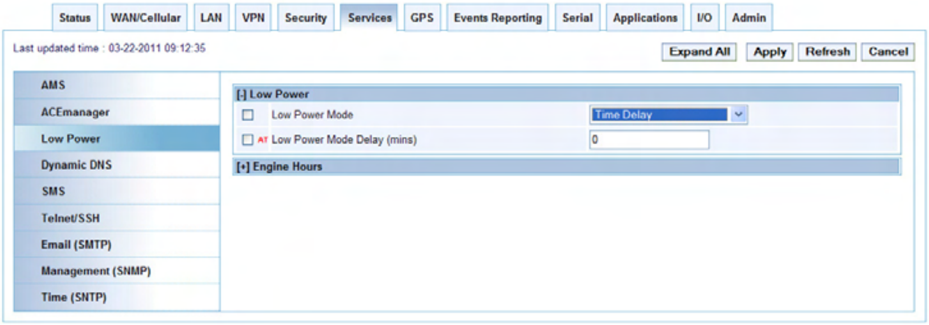
□ Low Power Mode: None

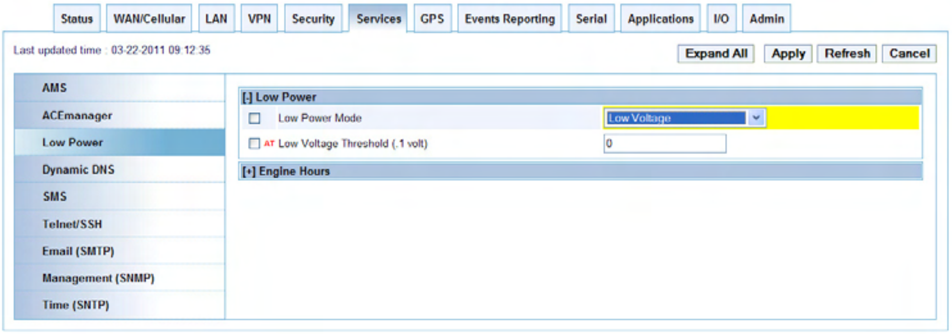
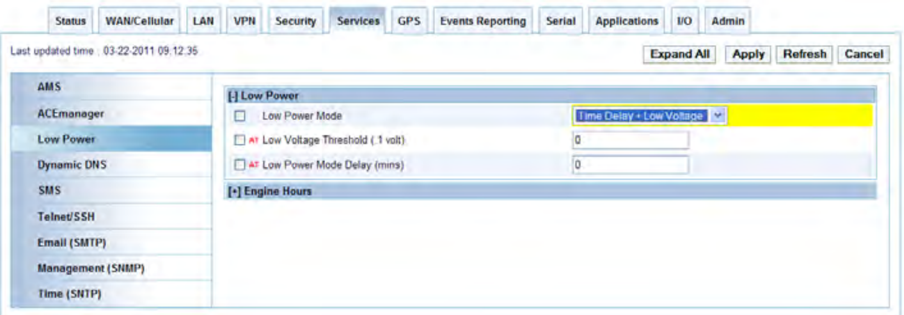
[-] Engine Hours

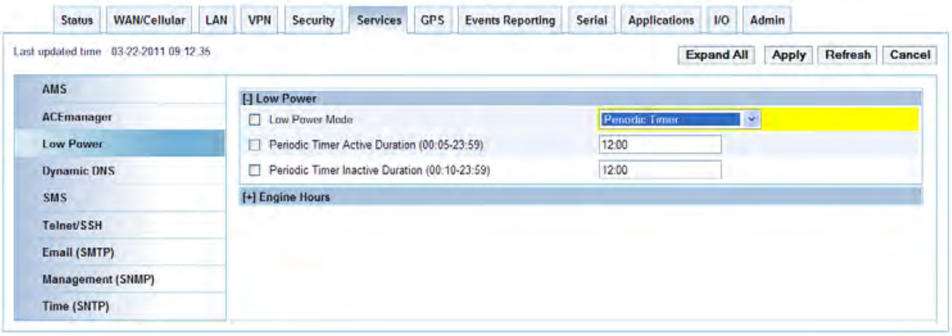
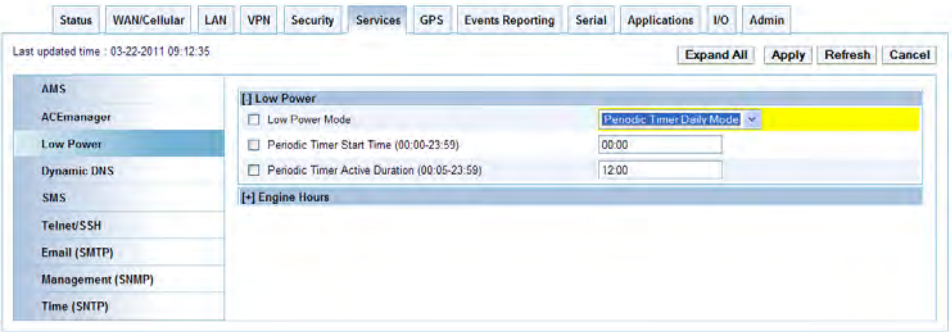
□ Engine Hours On Voltage Level (.1 volt): 0

□ Engine Hours Ignition Enable: Disable

Figure 8-3: ACEmanager: Services - Low Power

Field	Description
Low Power	
Low Power Mode	Allows you to set one of the following low power mode parameters: • None • Time Delay • Low Voltage • Time Delay + Low voltage • Periodic Timer • Periodic Timer Daily Mode Default: None.
Time Delay	Time delay in minutes (max 255). 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.  Last updated time : 03-22-2011 09:12:35 [-] Low Power □ Low Power Mode: Time Delay □ AT Low Power Mode Delay (mins): 0 [+] Engine Hours Low Power Mode Delay (Minutes): The number of minutes after one of the Low Power events happens until the AirLink device enters the low power mode.

Field	Description
Low Voltage	If you select Low Voltage, you need to set the Low Voltage Threshold. Low Voltage Threshold: Set the voltage level at which the device goes into low power mode (threshold in tenths of volts). Example: VLTG=130 would place the device in a low power standby state if the voltage goes below 13.0V.  Status WAN/Cellular LAN VPN Security Services GPS Events Reporting Serial Applications I/O Admin Expand All Apply Refresh Cancel AMS ACEmanager Low Power Dynamic DNS SMS Telnet/SSH Email (SMTP) Management (SNMP) Time (SNTP) [-] Low Power [+] Engine Hours AT Last updated time : 03-22-2011 09:12:35 □ Low Power Mode: Low Voltage □ AT Low Voltage Threshold (.1 volt): 0
Time Delay + Low Voltage	If you select this option, the device will delay going into Low Power mode caused by a low voltage drop (below threshold) or ignition off.  Status WAN/Cellular LAN VPN Security Services GPS Events Reporting Serial Applications I/O Admin Expand All Apply Refresh Cancel AMS ACEmanager Low Power Dynamic DNS SMS Telnet/SSH Email (SMTP) Management (SNMP) Time (SNTP) [-] Low Power [+] Engine Hours AT Last updated time : 03-22-2011 09:12:35 □ Low Power Mode: Time Delay + Low Voltage □ AT Low Voltage Threshold (.1 volt): 0 □ AT Low Power Mode Delay (mins): 0 • Low Voltage Threshold: Set the voltage level at which the device goes into low power mode (threshold in tenths of volts). Example: VLTG=130 would place the device in a low power standby state if the voltage goes below 13.0V. • Low Power Mode Delay (Minutes): The number of minutes after one of the Low Power events happens until the AirLink device enters the Low Power mode. *Note: There is always a minimum of 1 minute between the power down event and actual shutdown (to give the AirLink device time to prepare); entering zero, for Low Power Mode Delay, will not power down the device immediately.*

Field	Description
Periodic Timer	If you select the Periodic Timer, two fields display: • Periodic Timer Active Duration - Enter the time for how long the device needs to be in Active mode • Period Timer Inactive Duration - Enter the time for how long the device should be inactive after the Active mode expires. The Low Power mode process will repeat in a cyclical way (active and inactive).  Status WAN/Cellular LAN VPN Security Services GPS Events Reporting Serial Applications I/O Admin Expand All Apply Refresh Cancel AMS ACEmanager Low Power Dynamic DNS SMS Telnet/SSH Email (SMTP) Management (SNMP) Time (SNTP) Last updated time : 03-22-2011 09:12:36 [-] Low Power □ Low Power Mode: Periodic Timer □ Periodic Timer Active Duration (00:05-23:59): 12:00 □ Periodic Timer Inactive Duration (00:10-23:59): 12:00 [+] Engine Hours
Periodic Timer Daily Mode	This mode allows you to specify when the device should be active and when it should be in Low Power mode on a daily basis. If you select the Periodic Timer Daily Mode, two fields display: • Periodic Timer Start Time (00:00-23:59 UTC) - Enter the time to start the AirLink device in the Active mode. • Period Timer Active Duration (00:00-23:59 UTC) - Enter the time for how long the device should be active. The device will become active at the start time (UTC) and stay active for the active duration.  Status WAN/Cellular LAN VPN Security Services GPS Events Reporting Serial Applications I/O Admin Expand All Apply Refresh Cancel AMS ACEmanager Low Power Dynamic DNS SMS Telnet/SSH Email (SMTP) Management (SNMP) Time (SNTP) Last updated time : 03-22-2011 09:12:35 [-] Low Power □ Low Power Mode: Periodic Timer Daily Mode □ Periodic Timer Start Time (00:00-23:59): 00:00 □ Periodic Timer Active Duration (00:05-23:59): 12:00 [+] Engine Hours
Engine Hours	
Engine Hours On Voltage Level (.1 Volt)	This command sets the voltage above the level at which the engine should be considered "ON". To enter a voltage of 13.0 volts, enter 130.
Engine Hours Ignition Enable	Engine Hours are counted when the ignition sense is high.

Configuring Engine Hours

ALEOS can keep track of how long the engine has been on (Engine Hours) which is determined by either Ignition Sense or the Power In voltage. There two configuration fields to govern how Engine Hours is determined.

- **Engine On Voltage Level (.1 Volt)** - Use the Power In voltage to monitor engine usage. Set the voltage to higher than the maximum “at rest” voltage of your battery to track how long the engine has been on.
- **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 when the engine is running. Thus, a value of 130 (13.0 Volts) will correctly identify when the engine is on.

Dynamic DNS

Dynamic DNS allows an AirLink device WAN IP address to be published to a proprietary Sierra Wireless dynamic DNS service called IP Manager, or to an alternate third party service provider.

If you have one Sierra Wireless AirLink device, or a fleet of devices, it can be difficult to keep track of the current IP addresses, especially if the addresses are not 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:

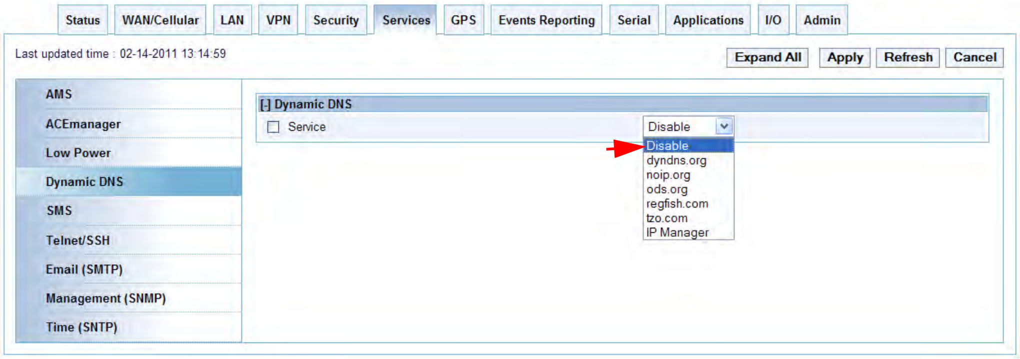
- Requesting a location update from a delivery truck
- Contacting a surveillance camera to download logs or survey a specific area
- An oil derek that needs to be triggered to begin pumping
- Sending text to be displayed by a road sign
- Updating the songs to be played on a juke box
- Updating advertisements 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, for data only being sent out, or for 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 will not 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 (which can cost a premium as opposed to. dynamic accounts), Sierra Wireless AirLink Solutions developed IP Manager. IP Manager works 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.



Last updated time : 02-14-2011 13:14:59

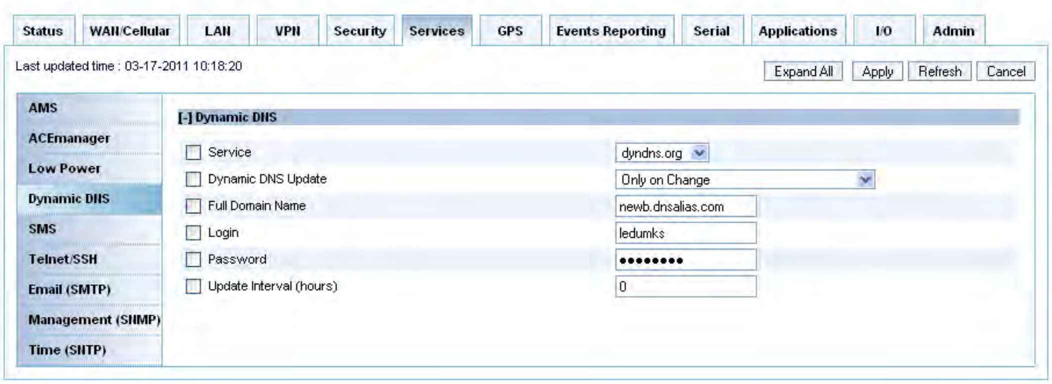
[-] Dynamic DNS

□ Service Disable

Figure 8-4: ACEmanager: Services - Dynamic DNS Service

Field	Description
Service	Allows you to select a Dynamic DNS service provider. Options are: • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager Default: Disable.

Third Party Services



Last updated time : 03-17-2011 10:18:20

[-] Dynamic DNS

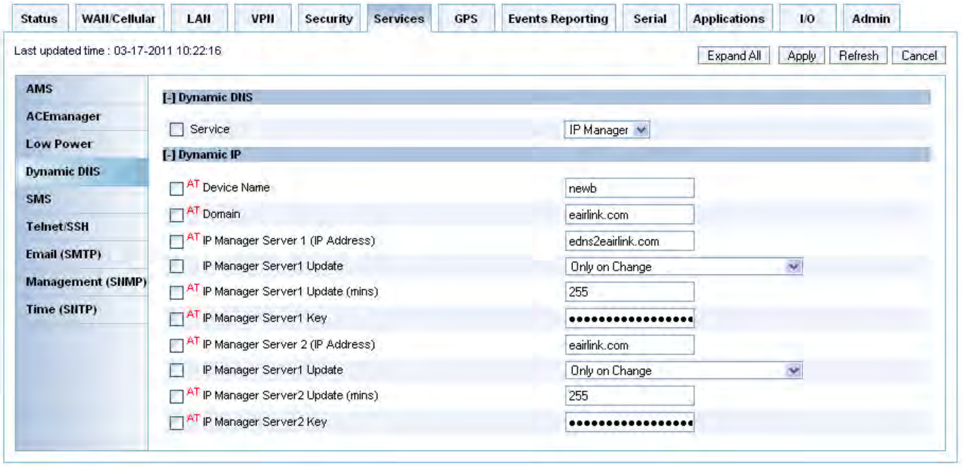
□ Service	dyndns.org
□ Dynamic DNS Update	Only on Change
□ Full Domain Name	newb.dnsalias.com
□ Login	ledumks
□ Password	••••••••
□ Update Interval (hours)	0

Figure 8-5: ACEmanager: Services - Dynamic DNS 3rd Party Services

Figure 8-5 is a sample third party service information screen. The third party service selected from the Service drop down menu in this example is “dyndns.org.” These same fields will be displayed for all Service selections other than IP Manager and disabled.

Field	Description
Service	Allows you to select a Dynamic DNS service provider. Options are: • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager Default: Disable.
Dynamic DNS Update	Options are: • Only on Change • Periodically Update (Not Recommended)
Full Domain Name	The name of a specific AirLink gateway or device.
Login	Provides the user’s service login name.
Password	Provides the user’s password in encrypted format.
Update Interval (hours)	Indicates the time (in hours) between checks for service updates from the selected third party service when periodic is selected.

IP Manager



Last updated time : 03-17-2011 10:22:16

[-] Dynamic DNS

□ Service	IP Manager

[-] Dynamic IP

□ AT Device Name	newb
□ AT Domain	eairlink.com
□ AT IP Manager Server 1 (IP Address)	edns2eairlink.com
□ IP Manager Server1 Update	Only on Change
□ AT IP Manager Server1 Update (mins)	255
□ AT IP Manager Server1 Key	●●●●●●●●●●●●●●●●●
□ AT IP Manager Server 2 (IP Address)	eairlink.com
□ IP Manager Server1 Update	Only on Change
□ AT IP Manager Server2 Update (mins)	255
□ AT IP Manager Server2 Key	●●●●●●●●●●●●●●●●●

Figure 8-6: ACEmanager: Services - Dynamic DNS IP Manager

Figure 8-6 shows the Dynamic IP fields that appear after selecting IP Manager as your Dynamic DNS Service.

Field	**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 Server 1 (IP Address) and **IP Manager Server 2 (IP Address)**	The IP address or domain name of the dynamic DNS server which is running IP Manager.
IP Manager Server 1 Update and **IP Manager Server 2 Update**	Options: • Only on Change • Periodic.
IP Manager Server1 Update (mins) and **IP Manager Server2 Update (mins)**	How often, in minutes, you want the address sent to the IP Manager.
IP Manager Server 1 Key and **IP Manager Server 2 Key**	User defined password key used instead of the 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 an IP change notification to the IP Manager. The IP Manager acknowledges the change and updates 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.

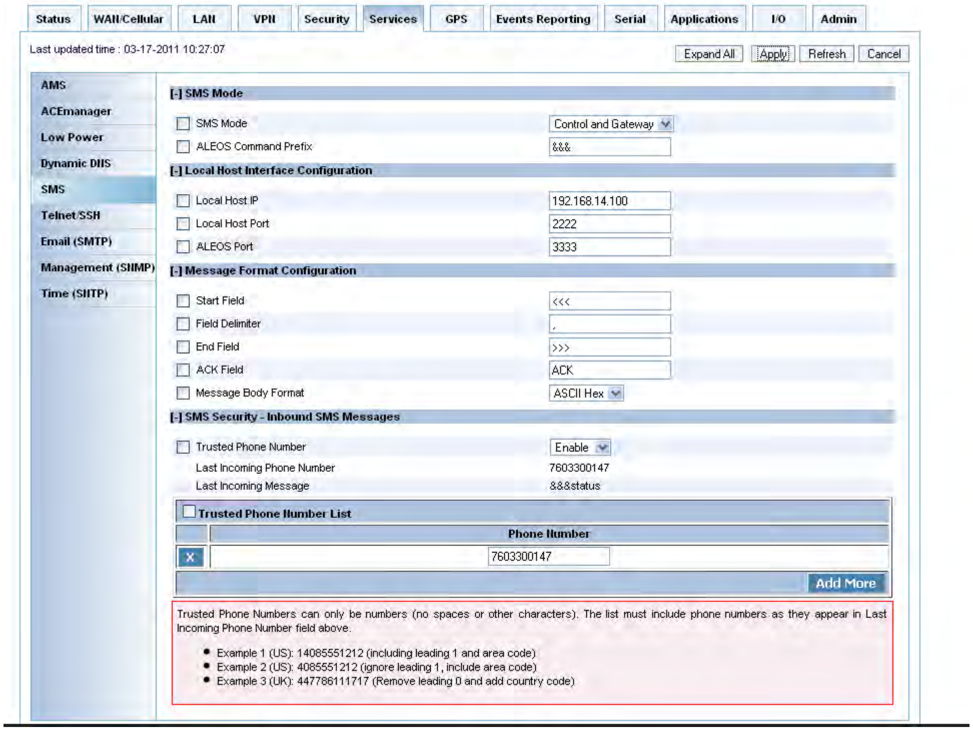
Note: The fully qualified domain name of your AirLink device will be a subdomain of the domain used by the IP Manager server.

SMS

ALEOS has the ability to:

- Receive commands via SMS message
- Act as an SMS gateway for a host connected to a local interface.

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.*



Last updated time : 03-17-2011 10:27:07

[-] SMS Mode

□ SMS Mode	Control and Gateway
□ ALEOS Command Prefix	&&&

[-] Local Host Interface Configuration

□ Local Host IP	192.168.14.100
□ Local Host Port	2222
□ ALEOS Port	3333

[-] Message Format Configuration

□ Start Field	<<<
□ Field Delimiter	,
□ End Field	>>>
□ ACK Field	ACK
□ Message Body Format	ASCII Hex

[-] SMS Security - Inbound SMS Messages

□ Trusted Phone Number	Enable
Last Incoming Phone Number	7603300147
Last Incoming Message	&&&status

□ Trusted Phone Number List

	Phone Number
X	7603300147

Trusted Phone Numbers can only be numbers (no spaces or other characters). The list must include phone numbers as they appear in Last Incoming Phone Number field above.

- Example 1 (US): 14085551212 (including leading 1 and area code)
- Example 2 (US): 4085551212 (ignore leading 1, include area code)
- Example 3 (UK): 447786111717 (Remove leading 0 and add country code)

Figure 8-7: ACEmanager: Services - SMS sample screen

The Services > SMS page displays four categories of features:

- SMS Mode
- Local Host Interface Configuration
- Message Format configuration
- SMS Security - Inbound SMS Messages.

Four SMS message modes can be selected in the SMS Mode category:

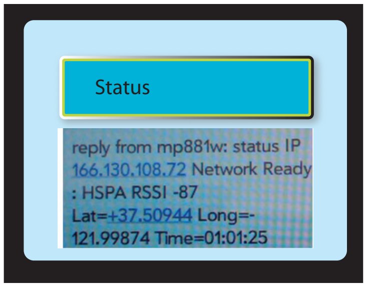
- Not Enabled (default)
- Control Only
- Gateway Only
- Control and Gateway

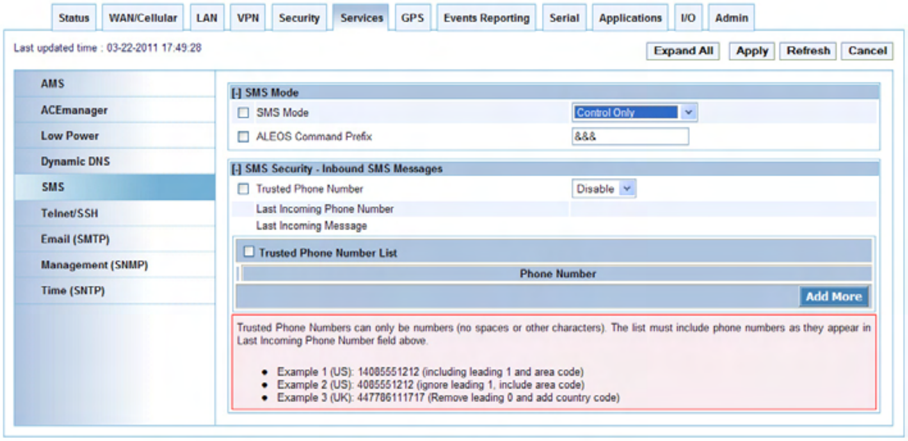
Control Only

The ALEOS SMS Mode Control Only feature allows some remote management of the AirLink device with SMS messaging. SMS allows users to:

- Retrieve current device status
- Reset the AirLink device
- Control the relay I/O.

When an SMS command is received, the AirLink device performs the action requested and sends a response back to that same phone number from which it received the SMS.

SMS Command	Device Action	SMS Response
Note: All responses start with "reply from [modem name]:"		
status	**None**	status IP [Network IP] [Network Status]: [technology type] RSS signalled Lat = [Latitude] Long = [Longitude] Time = [hh:mm:ss]  reply from mp881w: status IP 166.130.108.72 Network Ready : HSPA RSSI -87 Lat=+37.50944 Long=-121.99874 Time=01:01:25
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 y can be 0 or 1 (Off or Drive active low)



Last updated time : 03-22-2011 17:49:28

[-] SMS Mode

□ SMS Mode	Control Only
□ ALEOS Command Prefix	&&&

[-] SMS Security - Inbound SMS Messages

□ Trusted Phone Number	Disable
Last Incoming Phone Number	
Last Incoming Message	

□ Trusted Phone Number List

Phone Number

Trusted Phone Numbers can only be numbers (no spaces or other characters). The list must include phone numbers as they appear in Last Incoming Phone Number field above.

- Example 1 (US): 14085551212 (including leading 1 and area code)
- Example 2 (US): 4085551212 (ignore leading 1, include area code)
- Example 3 (UK): 447786111717 (Remove leading 0 and add country code)

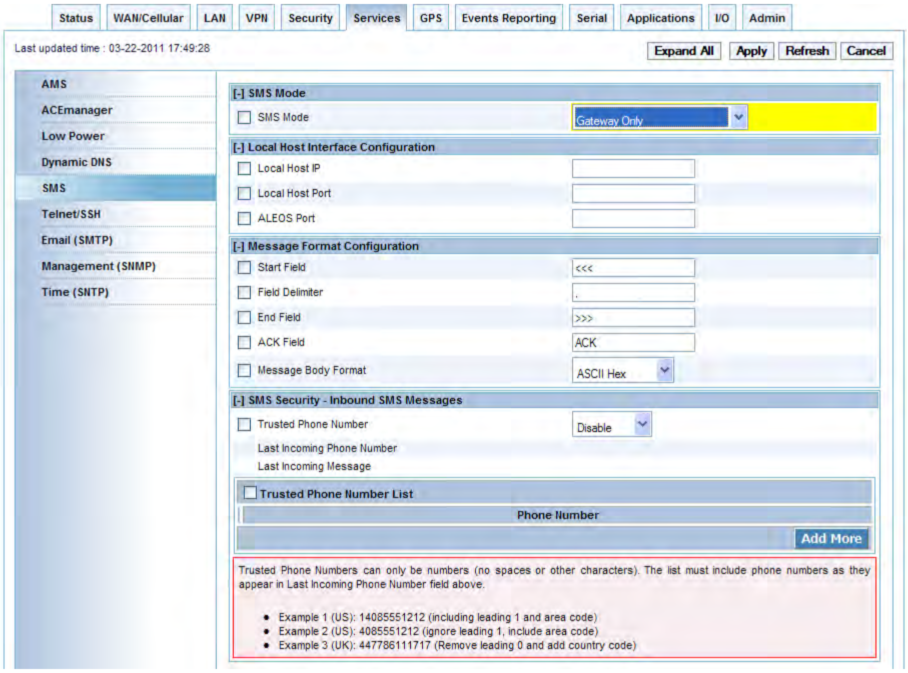
Figure 8-8: ACEmanager: Services - SMS - Control Only

Field	Description
ALEOS Command Prefix	The ALEOS Command Prefix is a configurable string of characters that can be configured if you choose Control Only or Control and Gateway mode. Any SMS command sent to the device needs to be prepended by the prefix. For example, “&&&Status” sent to device will receive the status command response. *Note: ALEOS Command Prefix can be blank in Control Only mode.*
Trusted Phone Number	Allows you to Enable or Disable a trusted phone number.
Last Incoming Phone Number	The last inbound phone number is displayed here. This will only be erased with a reset to defaults.
Last Incoming Message	The last incoming message is the last inbound SMS from the phone number.This will only be erased with a reset to defaults.
Trusted Phone Number List	Trusted phone numbers are listed here.

Gateway Only

The SMS gateway feature allows a locally connected host to use SMS for over the air transmission. SMS messages received by the device (inbound) will be sent on to the configured host. Messages sent by the host to a configured port on the device will be sent out as an SMS by the device (outbound).

Essentially, the device will forward SMS messages between the cellular radio and the connected host.



Last updated time : 03-22-2011 17:49:28

[-] SMS Mode

☐ SMS Mode: Gateway Only

[-] Local Host Interface Configuration

☐ Local Host IP

☐ Local Host Port

☐ ALEOS Port

[-] Message Format Configuration

☐ Start Field: <<<

☐ Field Delimiter: ,

☐ End Field: >>>

☐ ACK Field: ACK

☐ Message Body Format: ASCII Hex

[-] SMS Security - Inbound SMS Messages

☐ Trusted Phone Number: Disable

Last Incoming Phone Number

Last Incoming Message

☐ Trusted Phone Number List

Phone Number

Trusted Phone Numbers can only be numbers (no spaces or other characters). The list must include phone numbers as they appear in Last Incoming Phone Number field above.

- Example 1 (US): 14085551212 (including leading 1 and area code)
- Example 2 (US): 4085551212 (ignore leading 1, include area code)
- Example 3 (UK): 447786111717 (Remove leading 0 and add country code)

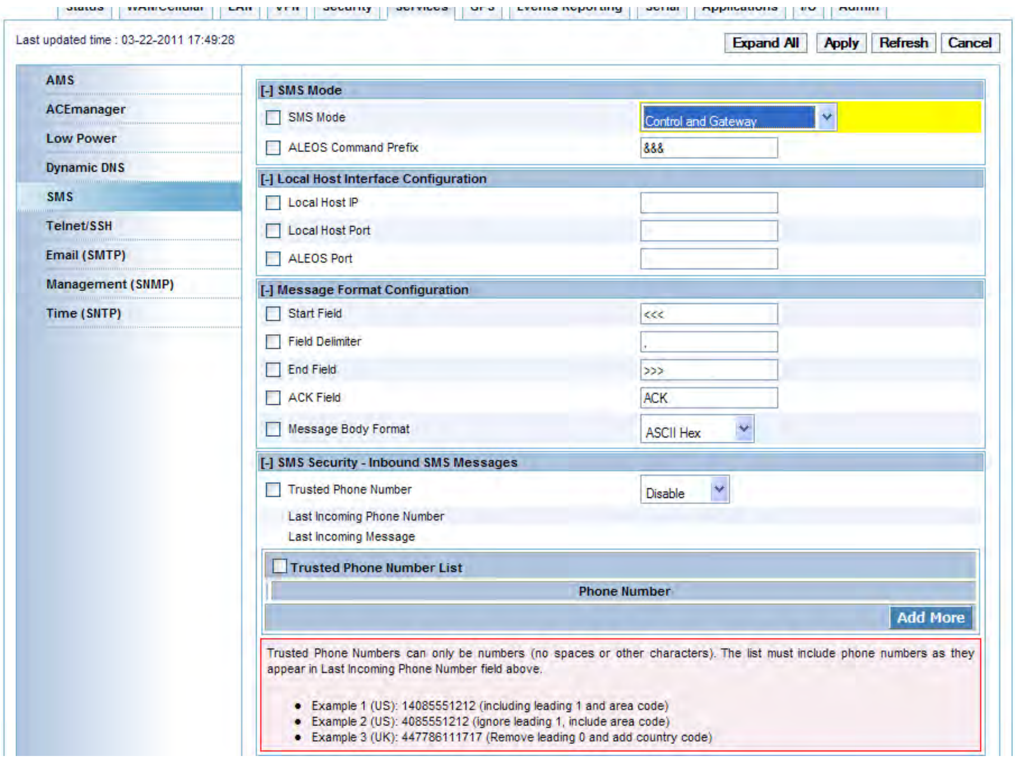
Figure 8-9: ACEmanager: Services - SMS - Gateway Only

See the table that follows figure 8-10 for descriptions of the fields that display when the SMS Mode “Gateway Only” is selected.

Control and Gateway

This SMS Mode allows both Control and Gateway messages.

- Control Messages: These are mobile terminated messages intended to configure ALEOS or to obtain ALEOS status.
- Gateway Messages: These messages may be mobile terminated or mobile originated and ALEOS acts as a gateway. In either case, the actual message origin or destination is the device connected to a local port, and ALEOS relays the message contents through the radio SMS interface.



Last updated time : 03-22-2011 17:49:28

[-] SMS Mode

□ SMS Mode	Control and Gateway
□ ALEOS Command Prefix	&&&

[-] Local Host Interface Configuration

□ Local Host IP	
□ Local Host Port	
□ ALEOS Port	

[-] Message Format Configuration

□ Start Field	<<<
□ Field Delimiter	,
□ End Field	>>>
□ ACK Field	ACK
□ Message Body Format	ASCII Hex

[-] SMS Security - Inbound SMS Messages

□ Trusted Phone Number	Disable
Last Incoming Phone Number	
Last Incoming Message	

□ Trusted Phone Number List

Phone Number

Trusted Phone Numbers can only be numbers (no spaces or other characters). The list must include phone numbers as they appear in Last Incoming Phone Number field above.

- Example 1 (US): 14085551212 (including leading 1 and area code)
- Example 2 (US): 4085551212 (ignore leading 1, include area code)
- Example 3 (UK): 447786111717 (Remove leading 0 and add country code)

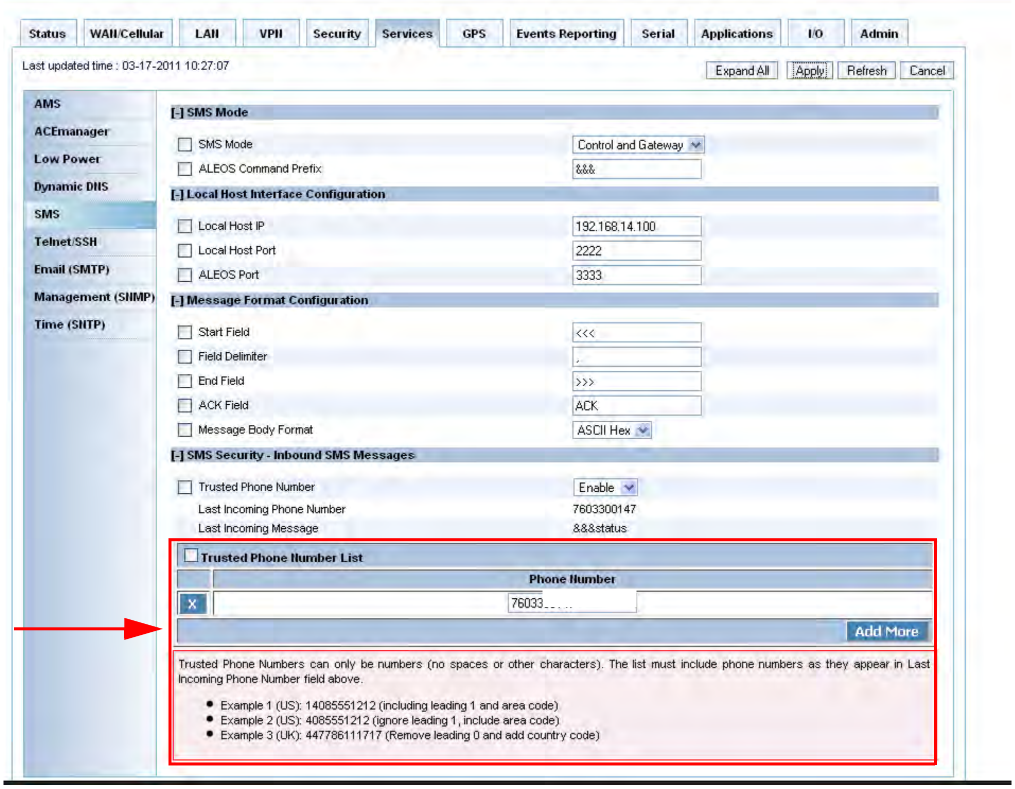
Figure 8-10: ACEmanager: Services - SMS - Control and Gateway

The following table provides descriptions of the fields that display when the SMS Modes “Gateway Only” or “Control and Gateway” are selected.

Field	Description
SMS Mode	There are four SMS message modes that the user can select in the SMS Mode section. The options are: • Not Enabled (Default) • Control Only • Gateway Only • Control and Gateway
ALEOS Command Prefix	The ALEOS Command Prefix is a configurable string of characters that shows up if you chose Control Only mode or Control and Gateway mode. This field does not display if Gateway Only mode is selected. Any SMS command sent to the device needs to be prepended by the prefix. For example, “&&&Status” sent to device will receive the status command response. *Note: ALEOS Command Prefix can be blank in Control Only mode.*
Local Host IP	IP address of the attached local host.
Local Host Port	The UDP port the host is listening to.
ALEOS Port	The UDP port on which the AirLink device is listening.
Start Field	Start the SMS message with a delimiter. The packet sent to the host will have a start and an end delimiter which enclose the message.
Field Delimiter	What you want as your SMS message field delimiter. The packet sent to the host will have a start and an end delimiter which enclose the message.
End Field	End the SMS message with a delimiter. The packet sent to the host will have a start and an end delimiter which enclose the message.
ACK Field	ALEOS will provide an ACK for message acknowledgement on every SMS message when it is passed to the radio. If ALEOS does not send an ACK, wait for 30 seconds and retry. Default: ACK.
Message Body Format	The only SMS body format available is the ASCII Hex. The other types of SMS body formats are set SMS protocols. Default: ASCII Hex
Trusted Phone Number	Options: Enable or Disable.
Last Incoming Phone Number	The last inbound phone number is displayed here. This will only be erased with a reset to defaults.
Last Incoming Message	The last incoming message is the last inbound SMS from the phone number.This will only be erased with a reset to defaults.
Trusted Phone Number List	Trusted phone numbers are listed here.

SMS Security- Inbound SMS Messages

When Trusted Phone Number security is enabled, incoming messages coming from the phone numbers in the Trusted Phone Number list, are the only ones for which commands will be performed (relay, response etc) or gateway messages forwarded. Incoming messages from all other phone numbers will be ignored.



Last updated time : 03-17-2011 10:27:07

[-] SMS Mode

□ SMS Mode: Control and Gateway

□ ALEOS Command Prefix: &&&

[-] Local Host Interface Configuration

□ Local Host IP: 192.168.14.100

□ Local Host Port: 2222

□ ALEOS Port: 3333

[-] Message Format Configuration

□ Start Field: <<<

□ Field Delimiter: ,

□ End Field: >>>

□ ACK Field: ACK

□ Message Body Format: ASCII Hex

[-] SMS Security - Inbound SMS Messages

□ Trusted Phone Number: Enable

Last Incoming Phone Number: 7603300147

Last Incoming Message: &&&status

□ Trusted Phone Number List

	Phone Number
X	76033[redacted]

Trusted Phone Numbers can only be numbers (no spaces or other characters). The list must include phone numbers as they appear in Last Incoming Phone Number field above.

- Example 1 (US): 14085551212 (including leading 1 and area code)
- Example 2 (US): 4085551212 (ignore leading 1, include area code)
- Example 3 (UK): 447786111717 (Remove leading 0 and add country code)

Figure 8-11: ACEmanager: Services - SMS

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. If Trusted Phone Number is enabled, no will be performed on the message.
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 the Trusted Phone Number.

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

Note: Phone Numbers (both trusted and not trusted) will be displayed in the Last Incoming Phone number field.

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.

With Trusted Phone Number enabled, only those SMS messages from Trusted Phone Numbers will receive responses to commands or messages acted on, as applicable.

SMSM2M

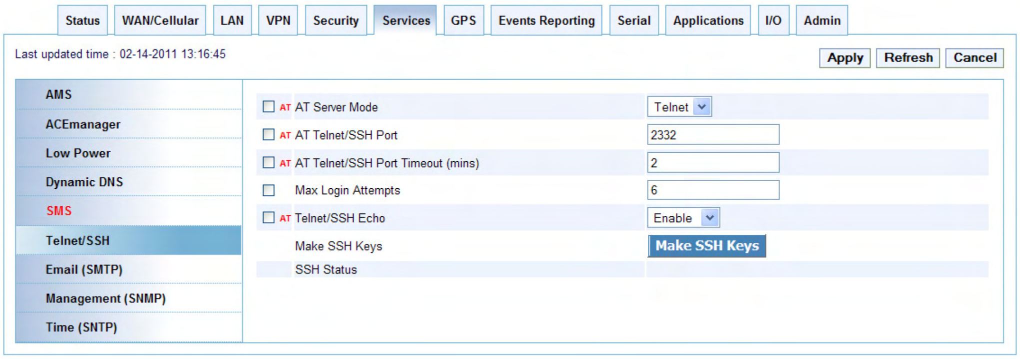
SMS messages can be sent from the serial command interface. Enter AT*SMSM2M=”[phone] [message]”. The phone number needs to be in the same format as numbers entered in the Trusted Phone Number List. The message needs to be 140 characters or less. To send several messages back to back, you need to wait for the OK before sending the next.

Telnet/SSH

Use the Telnet or SSH protocol to connect to any AirLink device and send AT commands.

A secure mechanism to connect remote clients is a requirement for many users. In ACEmanager now, Secure Shell (SSH) is supported 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.



Last updated time : 02-14-2011 13:16:45

□ AT AT Server Mode	Telnet
□ AT AT Telnet/SSH Port	2332
□ AT AT Telnet/SSH Port Timeout (mins)	2
□ Max Login Attempts	6
□ AT Telnet/SSH Echo	Enable
Make SSH Keys	Make SSH Keys
SSH Status	

Figure 8-12: ACEmanager: Services - Telnet

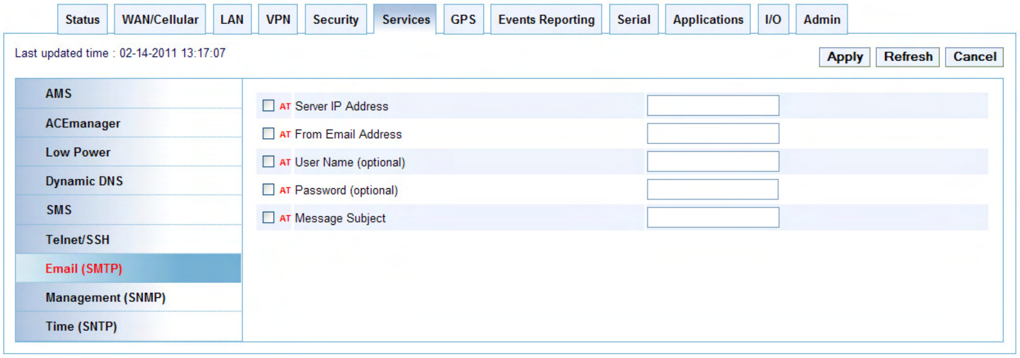
Field	Description
AT Server mode	Select either Telnet or SSH mode. Default: Telnet.
AT Telnet/SSH Port	Sets or queries the port used for the AT Telnet/SSH server. Default: 2332. **Tip:** *Many networks have the ports below 1024 blocked. It is recommended to use a higher numbered port.* After configuring SSH, apply and reset your device.
AT Telnet/SSH Port Timeout (mins)	Telnet/SSH port inactivity time out. Default: 2 (minutes).
Max Login Attempts	Sets the maximum number of login attempts. Default: 6.
Telnet/SSH Echo	Enable or disable the toggle AT command echo mode.
Make SSH Keys	Creates keys for SSH session applications.
SSH Status	Provides the status of the SSH session.

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 settings for a relay server for the device to use.

Note: The SMTP function will only work with a mail server that will allow relay email from the ALEOS device’s Net IP.



Last updated time : 02-14-2011 13:17:07

□ AT Server IP Address
□ AT From Email Address
□ AT User Name (optional)
□ AT Password (optional)
□ AT Message Subject

Figure 8-13: ACEmanager: Services - Email (SMTP)

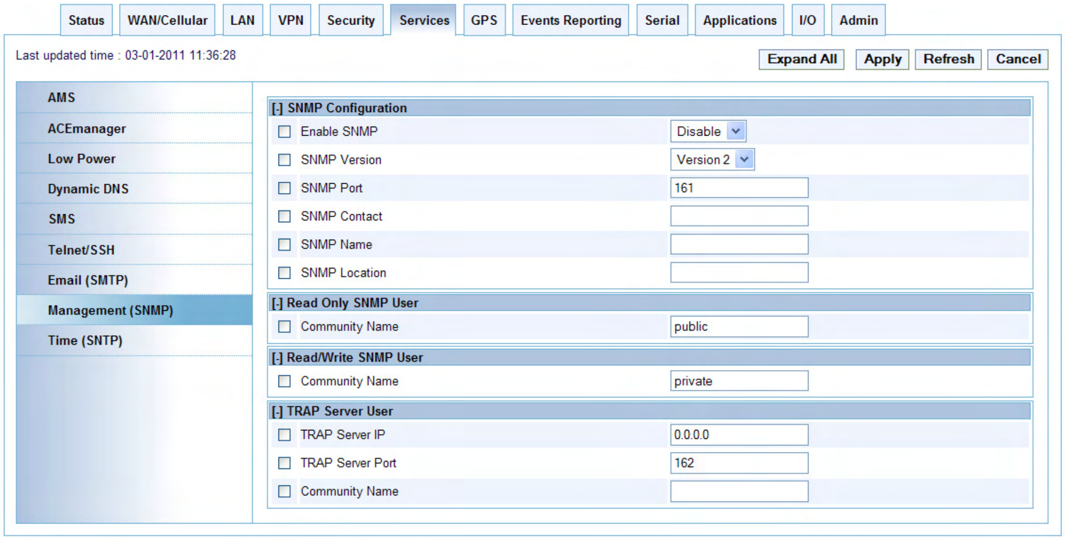
Field	Description
Server IP Address	Specify the IP address or Fully Qualified Domain Name (FQDN) of the SMTP server to use. • d.d.d.d = IP Address • name = domain name (maximum: 40 characters).
From Email Address	Sets the email address from which the SMTP message is being sent. • email = email address (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: The email server used for the relay may require a user name or password.*
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 the 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 device, 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 device, 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 device can be configured as an SNMP agent and supports SNMPv2c and SNMPv3.



Last updated time : 03-01-2011 11:36:28

[-] SNMP Configuration

□ Enable SNMP	Disable
□ SNMP Version	Version 2
□ SNMP Port	161
□ SNMP Contact	
□ SNMP Name	
□ SNMP Location	

[-] Read Only SNMP User

□ Community Name	public

[-] Read/Write SNMP User

□ Community Name	private

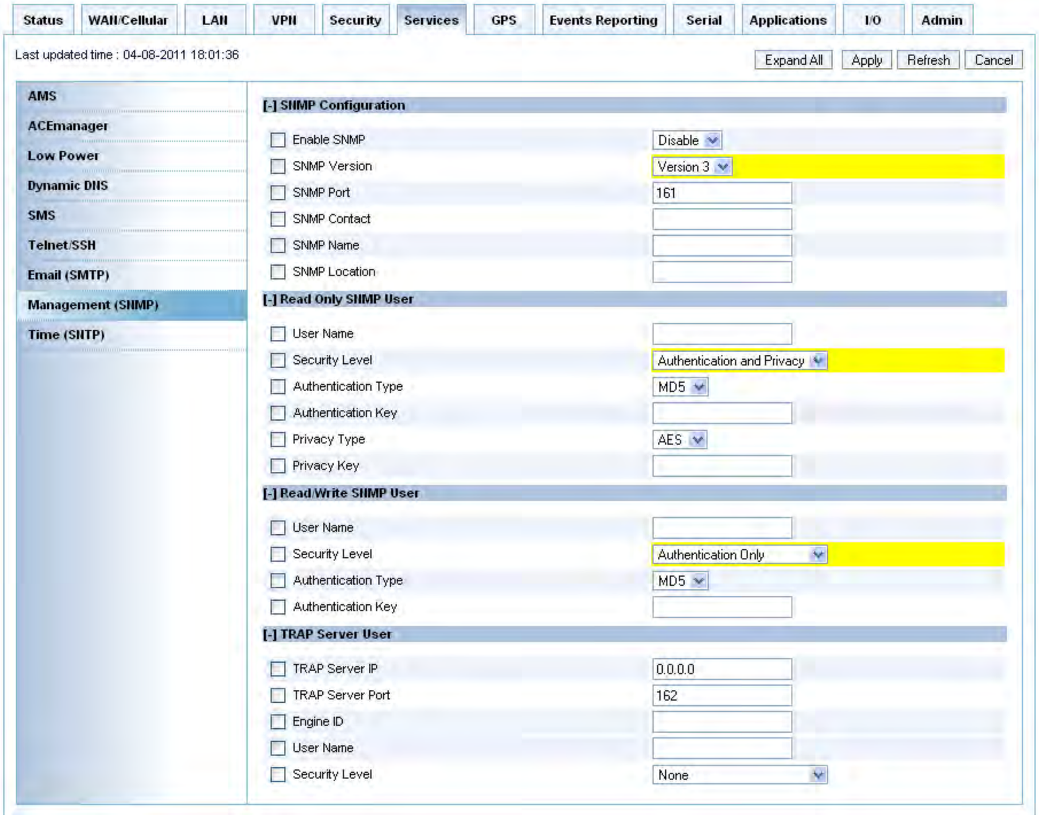
[-] TRAP Server User

□ TRAP Server IP	0.0.0.0
□ TRAP Server Port	162
□ Community Name	

Figure 8-14: ACEmanager: Services- Management (SNMPv2c)

Field	Description
SNMP Configuration **Enable SNMP**	Allows you to setup your SNMP configuration. Default: Disable.
SNMP Version	Allows you to select either SNMP protocol Version 2 or Version 3 communications. Default: Version 2.
SNMP Port	This controls which port the SNMP Agent listens on: • SNMP is disabled • 65535.

Field	Description
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
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.
Read Only SNMP User Community Name	Allows all SNMP users to view but not change the network configuration. Default: public.
Read/Write SNMP User Community Name	Identifies which SNMP user can change the network configuration. Default: private.
TRAP Server User **TRAP Server IP**	Identifies the IP address of the Trap Server.
TRAP Server Port	Identifies the specific port the Trap Server is on.
Community Name	Identifies the Community Name of the Trap Server.



Last updated time : 04-08-2011 18:01:36

[-] SNMP Configuration

□ Enable SNMP	Disable
□ SNMP Version	Version 3
□ SNMP Port	161
□ SNMP Contact	
□ SNMP Name	
□ SNMP Location	

[-] Read Only SNMP User

□ User Name	
□ Security Level	Authentication and Privacy
□ Authentication Type	MD5
□ Authentication Key	
□ Privacy Type	AES
□ Privacy Key	

[-] Read/Write SNMP User

□ User Name	
□ Security Level	Authentication Only
□ Authentication Type	MD5
□ Authentication Key	

[-] TRAP Server User

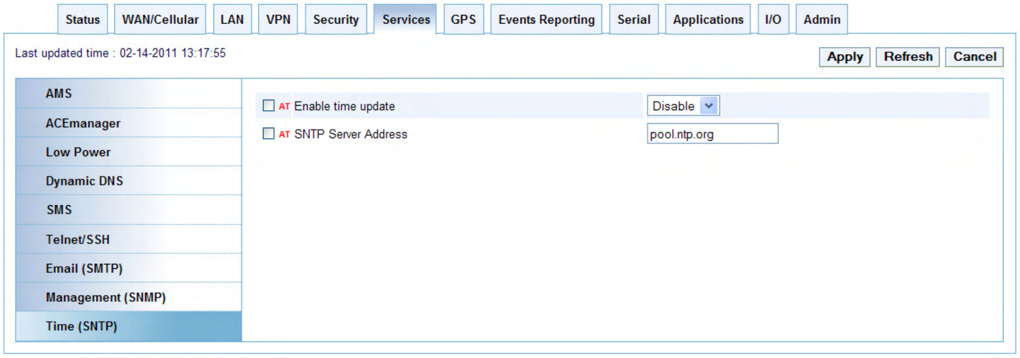
□ TRAP Server IP	0.0.0.0
□ TRAP Server Port	162
□ Engine ID	
□ User Name	
□ Security Level	None

Figure 8-15: ACEmanager: Services- Management (SNMPv3)

Field	Description
SNMP Configuration **Enable SNMP**	Allows you to setup your SNMP configuration. Default: Disable.
SNMP Version	Allows you to select either SNMP protocol Version 2 or Version 3 communications. Default: Version 3.
SNMP Port	This controls which port the SNMP Agent listens on: • SNMP is disabled • 65535.
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
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.
Read Only SNMP User **User Name**	Allows all SNMP users to view but not change the network configuration.
Security Level	Security types available: Authentication and Privacy, Authentication Only, and None.
Authentication Type	Authentication types available: MD5 or SHA1.
Authentication Key	This key authenticates SNMP requests for SNMPv3.
Privacy Type	Privacy types available: AES 128, DES, and None.
Privacy Key	This key ensures the confidentiality of SNMP messages via encryption.
Read/Write SNMP User **User Name**	Identifies which SNMP user can change the network configuration.
Security Level	Security types available: Authentication and Privacy, Authentication Only, and None.
Authentication Type	Authentication types available: MD5 or SHA1.
Authentication Key	This key authenticates SNMP requests for SNMPv3.
TRAP Server User **TRAP Server IP**	Identifies the IP address of the Trap Server.
TRAP Server Port	Identifies the specific port the Trap Server is on.
Engine ID	Identifies the SNMPv3 agent in the device. Entered by the system administrator.
User Name	Identifies the User Name of the Trap Server.
Security Level	Security types available: Authentication and Privacy, Authentication Only, and None.

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. Normally your device will synchronize with the cellular network or GPS.



Last updated time : 02-14-2011 13:17:55

□ AT Enable time update: Disable

□ AT SNTP Server Address: pool.ntp.org

Figure 8-16: ACEmanager: Services - Time (SNTP)

Field	Description
Enable time update	Enables daily SNTP update of the system time. Default: Disable.
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

9: GPS Configuration

The GPS tab that displays in ACEmanager is applicable across the Sierra Wireless AirLink GX400.

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 AirLink devices include:

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

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, the AirLink device uses the UDP (User Datagram Protocol) to communicate with the host server.

In RAP-based AVL, each device sends its command status and responses to the Host server and the Host sends commands to one or more 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 include:

- Air-Trak
- TrackStar
- CompassCom
- Zoll Data
- HTE
- Spillman

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.

An example of a tracking application using NMEA is 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.

An example of a tracking application using TAIP is 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.*

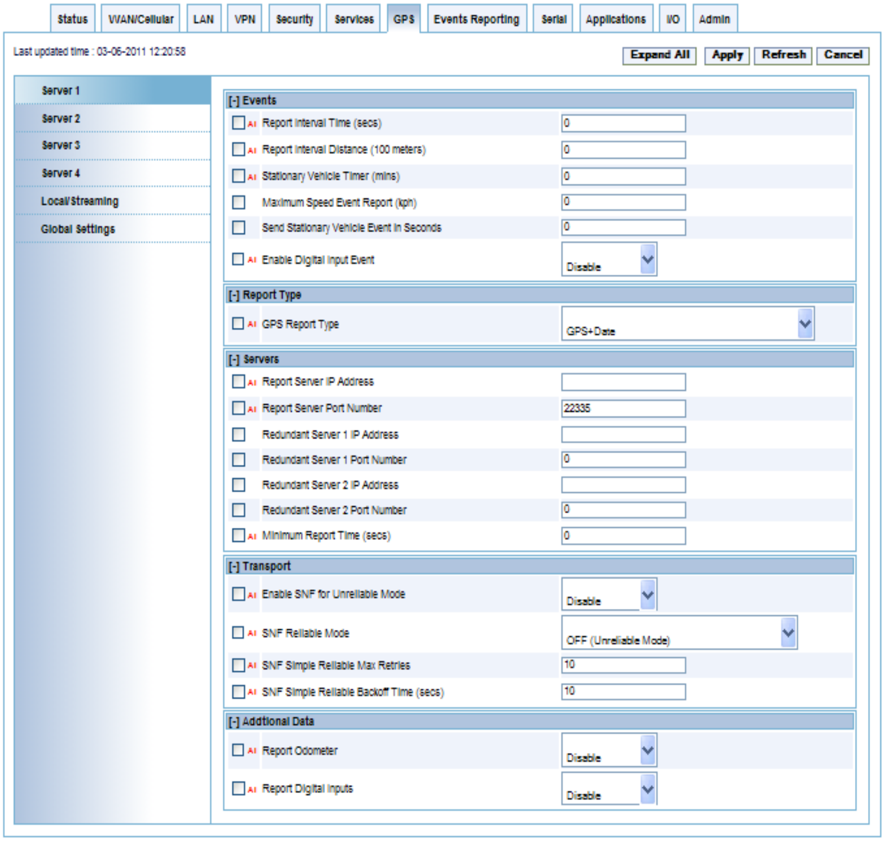
Before Configuring GPS

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?
- **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

GPS data configured for your AirLink device is sent to Server 1.



Last updated time : 03-06-2011 12:20:58

[-] Events	
□ AI Report Interval Time (secs)	0
□ AI Report Interval Distance (100 meters)	0
□ AI Stationary Vehicle Timer (mins)	0
□ Maximum Speed Event Report (kph)	0
□ Send Stationary Vehicle Event In Seconds	0
□ AI Enable Digital Input Event	Disable
[-] Report Type	
□ AI GPS Report Type	GPS+Date
[-] Servers	
□ AI Report Server IP Address	
□ AI Report Server Port Number	22335
□ Redundant Server 1 IP Address	
□ Redundant Server 1 Port Number	0
□ Redundant Server 2 IP Address	
□ Redundant Server 2 Port Number	0
□ AI Minimum Report Time (secs)	0
[-] Transport	
□ AI Enable SNF for Unreliable Mode	Disable
□ AI SNF Reliable Mode	OFF (Unreliable Mode)
□ AI SNF Simple Reliable Max Retries	10
□ AI SNF Simple Reliable Backoff Time (secs)	10
[-] Addtional Data	
□ AI Report Odometer	Disable
□ AI Report Digital Inputs	Disable

Figure 9-1: ACEmanager: GPS Server 1

Table 9-1: GPS: Server 1

Field	Description
Events	
Report Interval Time (secs)	GPS Report Time Interval. See also *PPMINTIME, *PPTSV, +CTA. n=seconds (1 - 65535) *Note: Your cellular carrier may impose a minimum transmit time.*
Report Interval Distance (100 meters)	GPS Report Distance Interval in 100 meter units (kilometers). 1 mile is approximately 1.61 kilometers. • n=0: Disabled • n=1-65535

Table 9-1: GPS: Server 1

Field	Description
Stationary Vehicle Timer (mins)	Timer for Stationary Vehicles. Time interval in minutes that the AirLink 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.*
Maximum Speed Event Report (kph)	Specifies the speed which will trigger Maximum Speed Event Report in kilometers per hour.
Send Stationary Vehicle Event in Seconds	Specifies the time (in seconds) in which a Stationary Vehicle Event should be sent.
Enable Digital Input Event	Allows you to enable or disable digital input events. • Disable • Enable Default: Disable
Report Type	
GPS Report Type	Sets the type of GPS Report: • GPS Data • GPS+Date • GPS+Date+RF • GPS+Date+RF+EIO • NMEA GGA+VTG • NMEA GGA+VTG+RMC • TAIP data • Compact TAIP data • TAIP LN report • TAIP TM report Default: GPS+Date

Table 9-1: GPS: Server 1

Field	Description
Servers	
Report Server IP Address	IP address or FQDN (fully qualified domain name) where GPS reports are sent (ATS Server IP). Also see *PPPORT. • d.d.d.d=IP address Example: AT*PPIP=192.100.100.100
Report Server Port Number	Port where GPS reports are sent. • n=1-65535 Default: 22335
Redundant Server 1 IP Address	IP address or FQDN of redundant Server 1.
Redundant Server 1 Port Number	Port number of redundant Server 1.
Redundant Server 2 IP Address	IP address or FQDN of redundant Server 2.
Redundant Server 2 Port Number	Port number of redundant Server 2.
Minimum Report Time (secs)	Specifies the minimum time (in seconds) between partial packets being sent.
Transport	
Enable SNF for Unreliable Mode	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. Options: • Disable • Enable Default: Disable
SNF Reliable Mode	Store and Forward Reliability: GPS reports will be retransmitted if not acknowledged by the server. Options: • OFF (Unreliable Mode) • Reliable Mode • Simple Reliable Mode • UDP Sequence Mode • TCP Listen Mode • TCP Default: OFF (Unreliable Mode)
SNF Simple Reliable Max Retries	Maximum number of retries when in Simple Reliable Mode. • n=0: Disabled • n=1-255 retries
SNF Simple Reliable Backoff Time (secs)	Backoff time (in seconds) when in Simple Reliable Mode.

Table 9-1: GPS: Server 1

Field	Description
Additional Data	
Report Odometer	Enables odometer reporting. Options: • Disable • Enable Default: Disable
Report Digital Inputs	Enables input reporting. Options: • Disable • Enable Default: Disable

Redundant Server

When a redundant server is enabled, each time a message is sent out to the main server 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.

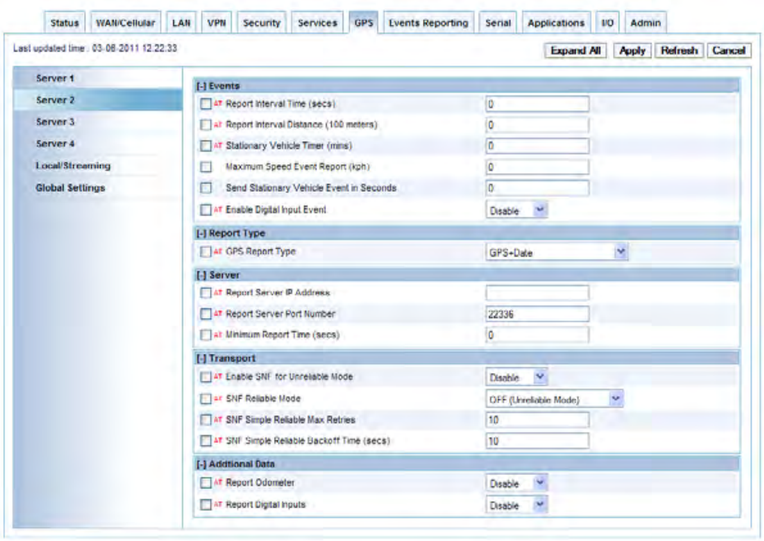
The redundant servers can be running the same or different application than the primary server. The messages to the redundant server are independent of the primary server settings or state.

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.

Server 2 to Server 4

GPS data can be sent to multiple servers. The GPS configuration screens for Server 2, Server 3, and Server 4 are identical to the configuration screen for Server 1 **except** for the elimination of the four redundant server fields in the Servers submenu section.



Last updated time : 03-08-2011 12:22:33

[-] Events

□ AT Report Interval Time (secs)	0
□ AT Report Interval Distance (100 meters)	0
□ AT Stationary Vehicle Timer (mins)	0
□ Maximum Speed Event Report (kph)	0
□ Send Stationary Vehicle Event in Seconds	0
□ AT Enable Digital Input Event	Disable

[-] Report Type

□ AT GPS Report Type	GPS+Date

[-] Server

□ AT Report Server IP Address	
□ AT Report Server Port Number	22336
□ AT Minimum Report Time (secs)	0

[-] Transport

□ AT Enable SNF for Unreliable Mode	Disable
□ AT SNF Reliable Mode	OFF (Unreliable Mode)
□ AT SNF Simple Reliable Max Retries	10
□ AT SNF Simple Reliable Backoff Time (secs)	10

[-] Additional Data

□ AT Report Odometer	Disable
□ AT Report Digital Inputs	Disable

Figure 9-2: ACEmanager: GPS - Server 2

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 after 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”.

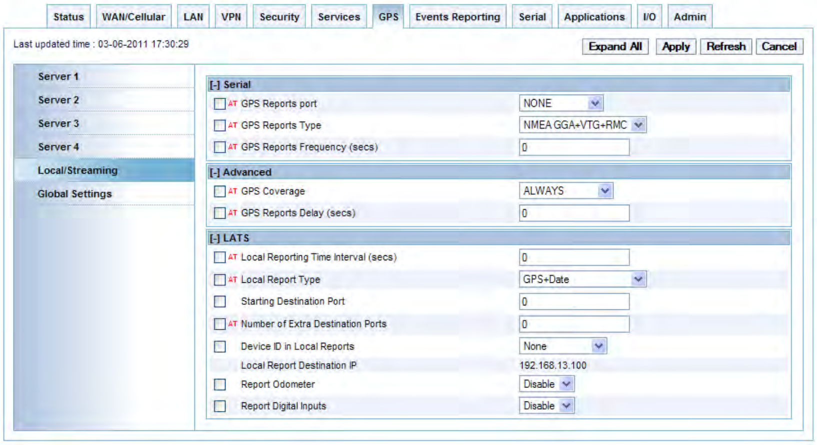
  On the other side, if the server receives an out of sequence packet, it will send a message to the device noting the missing sequence and the AirLink device will retransmit.
- **Simple Reliable Mode -** The AirLink device will ‘give up’ after a configured number, **PPMAXRETRIES*, of attempts and discard 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 0x30 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 -** The same as UDP Unreliable but using TCP instead of UDP.
- **TCP Listen Reliable -** TCP Listen Reliable is the same as UDP Sequence Reliable except the Reports Server must initiate the connection using TCP before the AirLink device will send reports. This allows servers to by-pass some firewalls.

Local/Streaming



Last updated time : 03-06-2011 17:30:29

[-] Serial

□ AT GPS Reports port	NONE
□ AT GPS Reports Type	NMEA GGA+VTG+RMC
□ AT GPS Reports Frequency (secs)	0

[-] Advanced

□ AT GPS Coverage	ALWAYS
□ AT GPS Reports Delay (secs)	0

[-] LATS

□ AT Local Reporting Time Interval (secs)	0
□ AT Local Report Type	GPS+Date
□ Starting Destination Port	0
□ AT Number of Extra Destination Ports	0
□ Device ID in Local Reports	None
Local Report Destination IP	192.168.13.100
□ Report Odometer	Disable
□ Report Digital Inputs	Disable

Figure 9-3: ACEmanager: GPS - Local/Streaming

Table 9-2: GPS: Local/Streaming

Field	Description
Serial	
GPS Reports port	Send GPS strings out serial or USB serial link. Options: • NONE • DB9 Serial • USB Serial • DB9 and USB Default: NONE
GPS Reports Type	GPS Report type to send via the serial link: • NMEA GGA+VTG+RMC • TAIP data • TAIP compact data • TAIP LN report • TAIP TM report Default: NMEA GGA+VTG+RMC
GPS Reports Frequency (secs)	Persistent GPS frequency (in seconds): • n= time interval between successive sets of GPS sentences Max Value: 65535 up to 18 hours

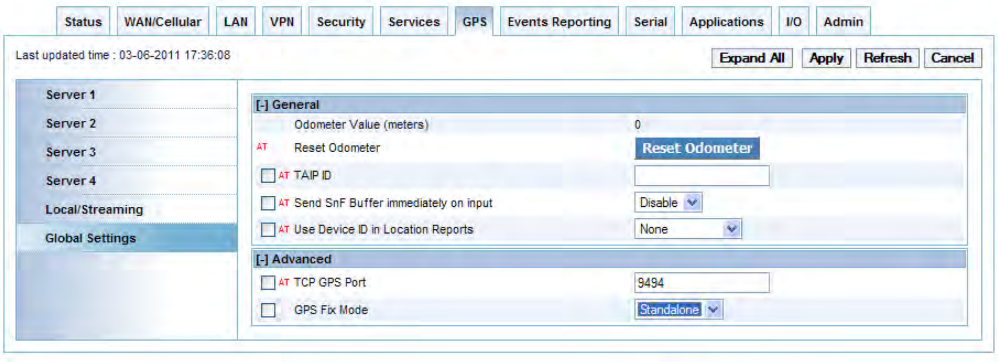
Table 9-2: GPS: Local/Streaming

Field	Description
Advanced	
GPS Coverage	Allows an AirLink device to be configured to send GPS sentences out of the serial port when the device loses cellular coverage. This feature is configured by 2 fields. This field controls the status of the sentences. Options: • ALWAYS • Out of Coverage Default: ALWAYS
GPS Report Delay (secs)	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 or USB/serial port.
LATS	
Local Reporting Time Interval (secs)	LATS (Local ATS) - Causes GPS reports to be sent out over the Ethernet link every *n* seconds when there is an Ethernet, USBnet, or PPPoE connection to the serial host or a connection to the Ethernet port is established. • Disable • 1-255 seconds
Local Report Type	Indicates the type of GPS report to send to the local server. Sets one of the following Local Report types: • GPS Data • GPS+Date • GPS+Date+RF • GPS+Date+RF+EIO • NMEA GGA+VTG • NMEA GGA+VTG+RMC • TAIP data • TAIP Compact data • TAIP LN report • TAIP TM report Default: GPS+Date
Starting Destination Port	Identifies the initial Destination Port to send the reort to via UDP.
Number of Extra Destination Ports	Indicates the number of additional destination ports that the report is to be sent to.
Device ID in Local Reports	Indicates the Device ID to use in Local Reports. Options: • None • Phone Number • ESN/IMEI Default: None
Local Report Destination IP	Indicates the address of the destination IP to use in Local Reports.

Table 9-2: GPS: Local/Streaming

Field	Description
Report Odometer	Enables odometer reporting. Options: • Disable • Enable Default: Disable
Report Digital Inputs	Enables input reporting. Options: • Disable • Enable Default: Disable

Global Settings



Last updated time : 03-06-2011 17:36:08

[-] General

	Odometer Value (meters)	0
AT	Reset Odometer	Reset Odometer
□ AT	TAIP ID	
□ AT	Send SnF Buffer immediately on input	Disable
□ AT	Use Device ID in Location Reports	None

[-] Advanced

□ AT	TCP GPS Port	9494
□	GPS Fix Mode	Standalone

Figure 9-4: ACEmanager: GPS - Global Settings

Table 9-3: GPS: Global Settings

Field	Description
General	
Odometer Value (meters)	The current odometer value (in meters) of the AirLink device. Maximum value is approximately 4.3 billion meters (2.5 million miles). 1 mile is approximately 1600 meters. • n= meters Default: 0
Reset Odometer	Press the Reset Odometer button to reset the current odometer reading.
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)

Table 9-3: GPS: Global Settings

Field	Description
Send SnF Buffer immediately on input	Flushes store and forward buffer when an input event (digital inputs, stationary events, and maximum speed events) occurs. • Disable • Enable Default: Disable
Use Device ID in Location Reports	Enable input reporting. • None • Phone Number • ESN/IMEI Default: None
Advanced	
TCP 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)
GPS Fix Mode	Specifies the GPS fix mode. • Standalone • MS Based

10: Events Reporting Configuration

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

Introduction

Events Reporting allows the users to generate reports or perform actions in response to the events that are configured in the ALEOS software.

An Event is a measurement of a physical property AND a state change or a threshold crossing. For example, radio module signal strength (RSSI) is a physical property. A threshold crossing could be set to -105 dBm. The user can configure an Event which consists of the RSSI with the -105 dBm threshold. There are many Events that can be configured; these are described in detail below.

An Action is an activity which can be performed, such as sending a report to a remote server, sending an SNMP trap, changing the value on a digital signal line, or turning off cellular communication with any devices connected to a host port. If a report is to be sent, the user has the option of including user selected data with that report.

Events and Actions work together. When an Event is triggered, this means that, for the physical property being measured, the state change has occurred, or the threshold crossing has occurred.   The Event will then effect the Action to occur. Following on to the previous example, if the user has configured an RSSI Event, then the user can have a report sent (example: SMS Message) once the threshold is crossed.   This relationship is shown conceptually in Figure 10-1.

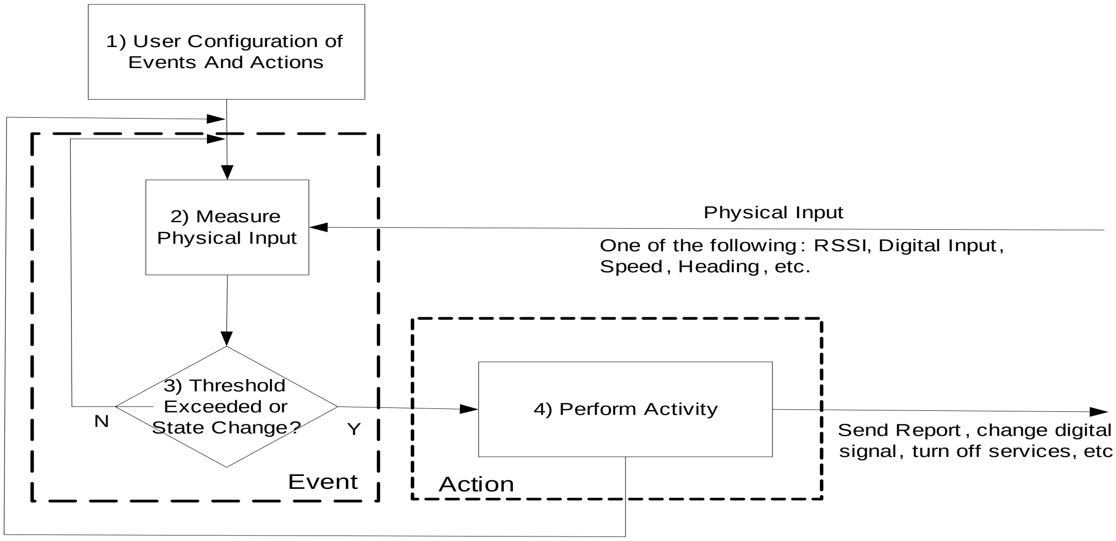

1) User Configuration of Events And Actions
2) Measure Physical Input
Physical Input
One of the following: RSSI, Digital Input, Speed, Heading, etc.
3) Threshold Exceeded or State Change?
N
Y
Event
4) Perform Activity
Send Report, change digital signal, turn off services, etc
Action

Figure 10-1: Events Reporting Concept

The procedure of how Events Reporting works is described below:

1. The user configures the events and actions.
2. After deployment, the device begins measuring a physical input.
3. The measurement is compared to the user configured threshold or state change. If no change, then another measurement is performed. If a state change (or threshold crossing) occurs, then the flow moves to step 4,
4. The Action associated with the Event. In step 4, a report may be generated, or some other activity is performed. Afterwards, the flow returns to step 1.

Additional Behavior and Features

Events/Actions are not one shot activities. After an Action is performed, the Event is still active and will trigger the next time the state change or threshold crossing occurs.

A single Event may activate one or more Actions. For example, if RSSI is below threshold, the user can turn off data services (Action 1) and send an SMS message (Action 2).

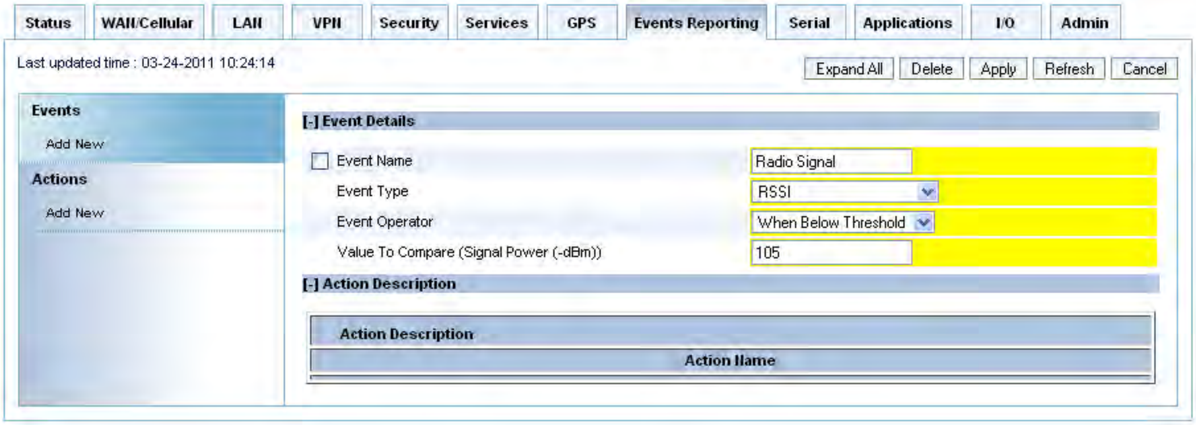
A single Action may be activated by one or more Events. For example, if user speed (in a vehicle) is above a threshold or if the vehicle heading changes, either Event can perform the same action.

Configuration Overview

To configure Events and Actions, the user must go through the following steps. These will be illustrated in the sections below.

1. Define an Event – Events can be configured using the ACEmanager User Interface. Select the Events Reporting Tab, and then select the *Add New* subtab to add an event (e.g., RSSI)>

Note in the Action Description frame that there are no actions listed.



Last updated time : 03-24-2011 10:24:14

[-] Event Details

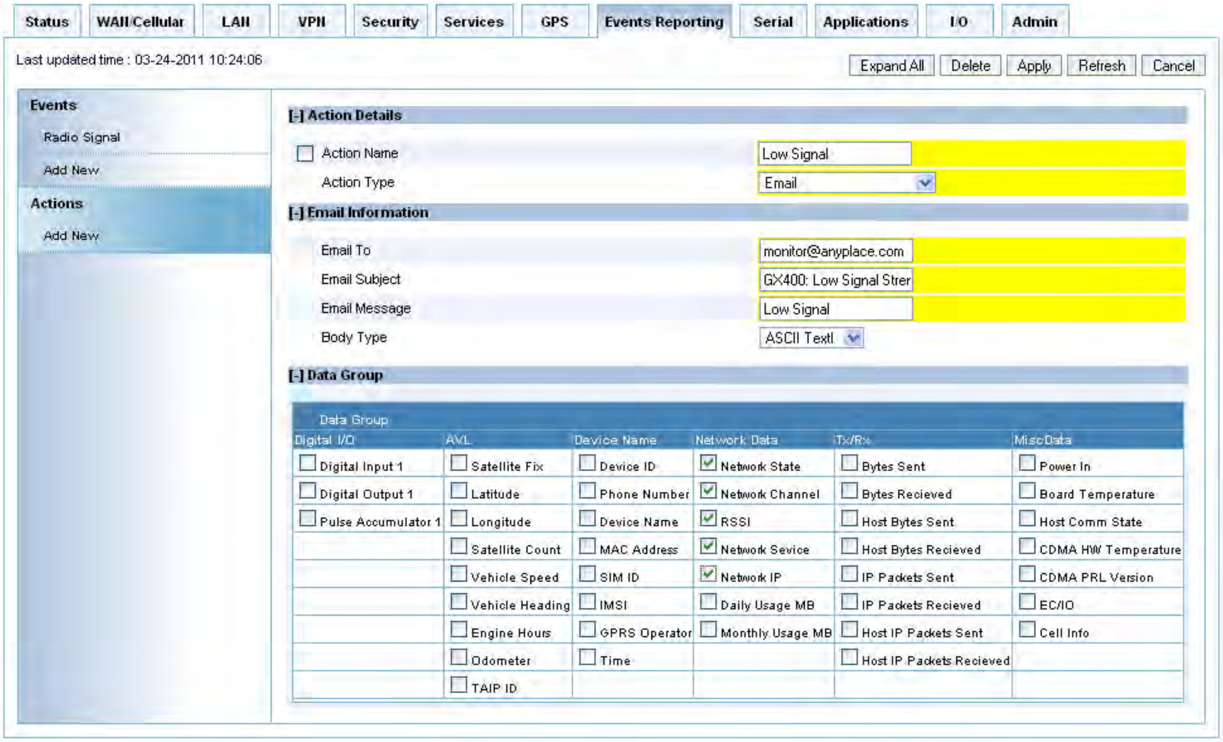
□ Event Name	Radio Signal
Event Type	RSSI
Event Operator	When Below Threshold
Value To Compare (Signal Power (-dBm))	105

[-] Action Description

Action Description
Action Name

Figure 10-2: ACEmanager: Events Reporting - Events - Add New

2. Define an Action – This is done on the Actions group.



Last updated time : 03-24-2011 10:24:06

[-] Action Details

□ Action Name	Low Signal
Action Type	Email

[-] Email Information

Email To	monitor@anyplace.com
Email Subject	GX400: Low Signal Strer
Email Message	Low Signal
Body Type	ASCII Textl

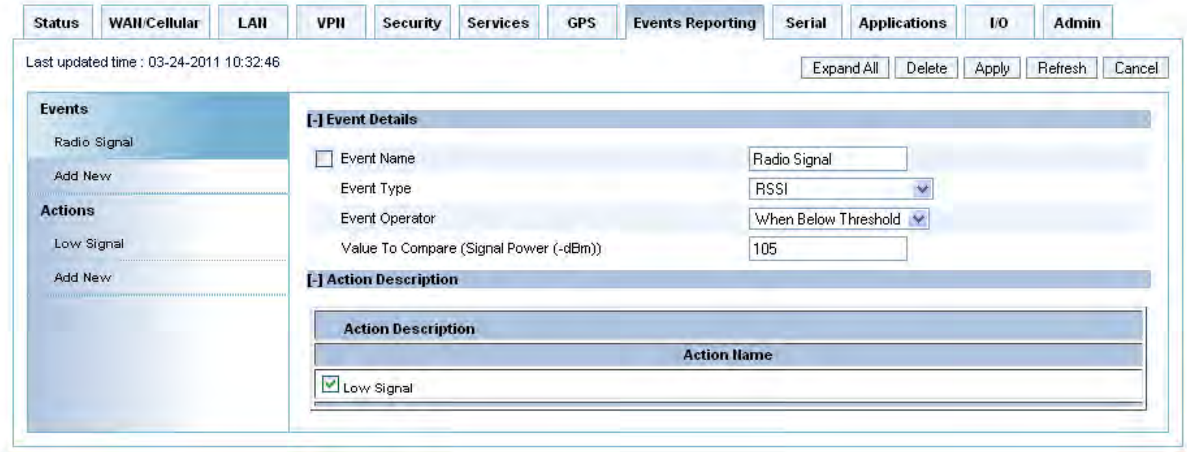
[-] Data Group

Data Group

Digital I/O	AVL	Device Name	Network Data	Tx/Rx	MiscData
□ Digital Input 1	□ Satellite Fix	□ Device ID	☑ Network State	□ Bytes Sent	□ Power In
□ Digital Output 1	□ Latitude	□ Phone Number	☑ Network Channel	□ Bytes Recieved	□ Board Temperature
□ Pulse Accumulator 1	□ Longitude	□ Device Name	☑ RSSI	□ Host Bytes Sent	□ Host Comm State
	□ Satellite Count	□ MAC Address	☑ Network Sevice	□ Host Bytes Recieved	□ CDMA HW Temperature
	□ Vehicle Speed	□ SIM ID	☑ Network IP	□ IP Packets Sent	□ CDMA PRL Version
	□ Vehicle Heading	□ IMSI	□ Daily Usage MB	□ IP Packets Recieved	□ EC/IO
	□ Engine Hours	□ GPRS Operator	□ Monthly Usage MB	□ Host IP Packets Sent	□ Cell Info
	□ Odometer	□ Time		□ Host IP Packets Recieved	
	□ TAIP ID				

Figure 10-3: ACEmanager: Events Reporting - Actions - Add New

3. Associate the Action with the Event – This is done by clicking on the Events group. On the Events page, note that the new Action (Low Signal) is displayed in the Action Description frame. Users can check the box to associate this action with the Cell Radio Sign Event.



Last updated time : 03-24-2011 10:32:46

[-] Event Details

□ Event Name	Radio Signal
Event Type	RSSI
Event Operator	When Below Threshold
Value To Compare (Signal Power (-dBm))	105

[-] Action Description

Action Description

Action Name
☑ Low Signal

Figure 10-4: ACEmanager: Events Reporting - Events - Cell Radio Sign

Table 10-1: Events Types

Event Name	Event Type	Threshold or State Change Options
Digital Inputs		
Digital Input	State Change	Switch Closed Switch Opened On Any Change
Pulse Accumulator	Threshold Crossing	
AVL		
GPS Fix	State Change	Fix Lost Fix Obtained Any Fix Change
Vehicle Speed	Threshold Crossing	Vehicle Speed (KM/h)
Heading Change	Threshold Crossing	Heading Change (degrees)
Engine Hours	Threshold Crossing	Engine Hours
Network		
RSSI	Threshold Crossing	Signal Power (-dBm)
Network State	State Change	When Device is Ready
Network Service	State Change	• Voice • Roaming • 2G • 3G • EVDO Rev A or HSPA • Any Service Change

Table 10-1: Events Types

Other Report Types		
Periodic Reports	Threshold Crossing (Time)	Period to compare (seconds)
Power In	Threshold Crossing	Power threshold (volts)
Board Temperature	Threshold Crossing	Degrees Celsius
CDMA Radio Module	Threshold Crossing	Degrees Celsius
Data Usage		
Daily Data Usage	Threshold Crossing	Percentage of daily threshold
Monthly Data Usage	Threshold Crossing	Percentage of monthly threshold

Action Description

Select a name for the action of your choice.

Action Type

Under the Events Reporting Action tab, there is an Action Type field which has different parameters listed in the scroll-down menu.

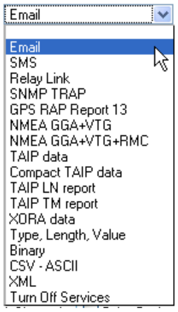
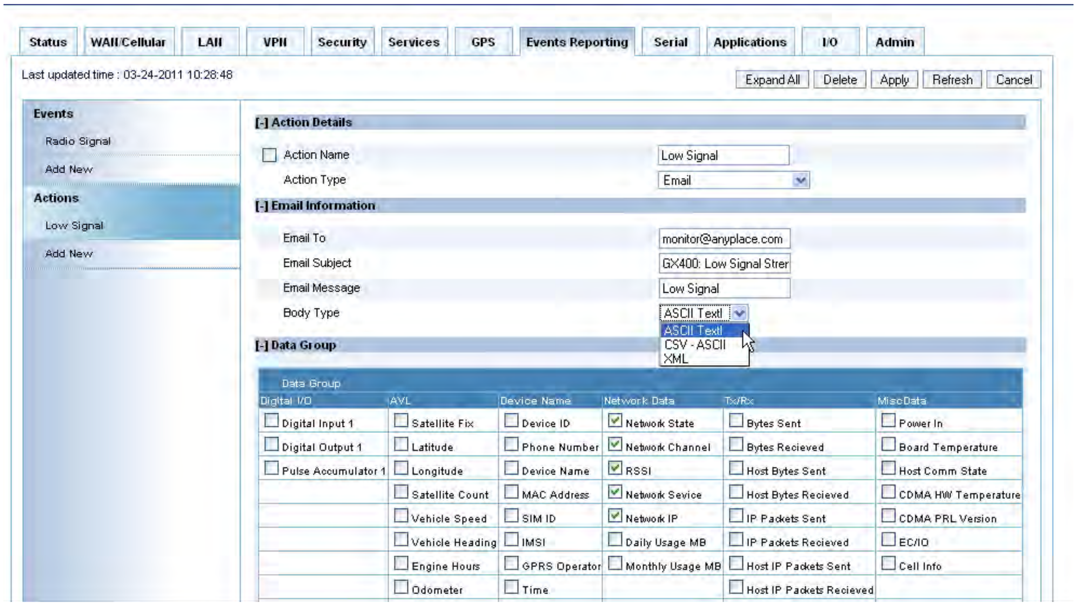


Figure 10-5: ACEmanager: Events Reporting - Action - Action Type scroll down

There are nine 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



Last updated time : 03-24-2011 10:28:48

[-] Action Details

□ Action Name	Low Signal
Action Type	Email

[-] Email Information

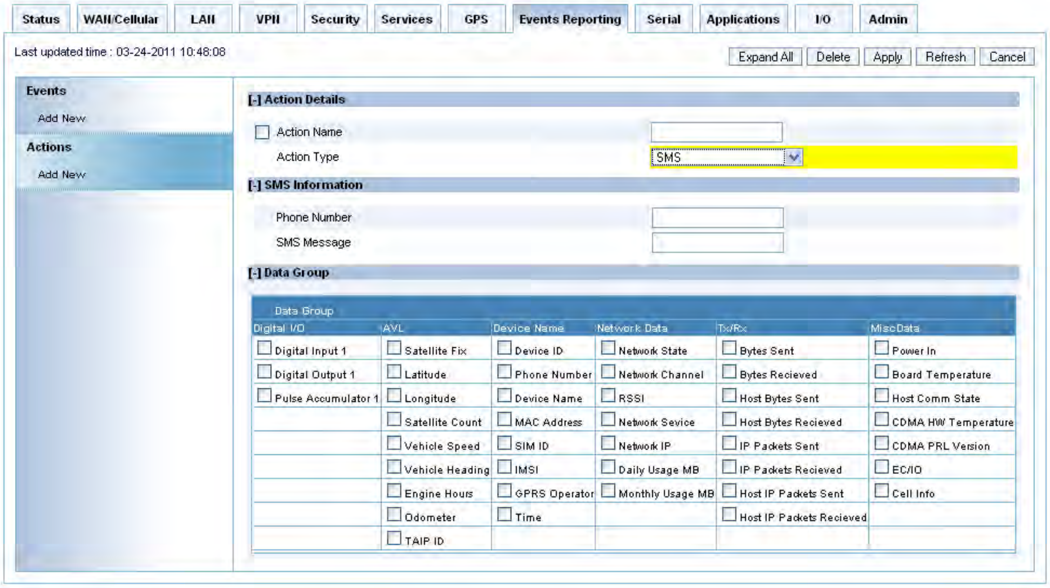
Email To	monitor@anyplace.com
Email Subject	GX400: Low Signal Strer
Email Message	Low Signal
Body Type	ASCII Text ASCII Text CSV - ASCII XML

[-] Data Group

Data Group

Digital I/O	AVL	Device Name	Network Data	Tx/Rx	MiscData
□ Digital Input 1	□ Satellite Fix	□ Device ID	☑ Network State	□ Bytes Sent	□ Power In
□ Digital Output 1	□ Latitude	□ Phone Number	☑ Network Channel	□ Bytes Recieved	□ Board Temperature
□ Pulse Accumulator 1	□ Longitude	□ Device Name	☑ RSSI	□ Host Bytes Sent	□ Host Comm State
	□ Satellite Count	□ MAC Address	☑ Network Sevice	□ Host Bytes Recieved	□ CDMA HW Temperature
	□ Vehicle Speed	□ SIM ID	☑ Network IP	□ IP Packets Sent	□ CDMA PRL Version
	□ Vehicle Heading	□ IMSI	□ Daily Usage MB	□ IP Packets Recieved	□ EC/IO
	□ Engine Hours	□ GPRS Operator	□ Monthly Usage MB	□ Host IP Packets Sent	□ Cell Info
	□ Odometer	□ Time		□ Host IP Packets Recieved	

Figure 10-6: ACEmanager: Events Reporting - Action Type - Email (similar fields for SMS)



Last updated time : 03-24-2011 10:48:08

[-] Action Details

□ Action Name	
Action Type	SMS

[-] SMS Information

Phone Number	
SMS Message	

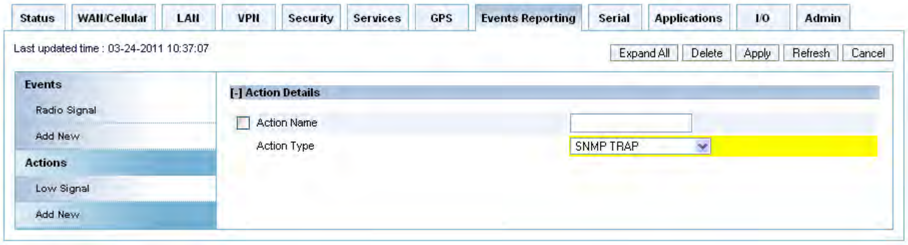
[-] Data Group

Data Group

Digital I/O	AVL	Device Name	Network Data	Tx/Rx	MiscData
□ Digital Input 1	□ Satellite Fix	□ Device ID	□ Network State	□ Bytes Sent	□ Power In
□ Digital Output 1	□ Latitude	□ Phone Number	□ Network Channel	□ Bytes Recieved	□ Board Temperature
□ Pulse Accumulator 1	□ Longitude	□ Device Name	□ RSSI	□ Host Bytes Sent	□ Host Comm State
	□ Satellite Count	□ MAC Address	□ Network Sevice	□ Host Bytes Recieved	□ CDMA HW Temperature
	□ Vehicle Speed	□ SIM ID	□ Network IP	□ IP Packets Sent	□ CDMA PRL Version
	□ Vehicle Heading	□ IMSI	□ Daily Usage MB	□ IP Packets Recieved	□ EC/IO
	□ Engine Hours	□ GPRS Operator	□ Monthly Usage MB	□ Host IP Packets Sent	□ Cell Info
	□ Odometer	□ Time		□ Host IP Packets Recieved	
	□ TAIP ID				

Figure 10-7: ACEmanager: Events Reporting - Action Type - SMS

- SNMP Trap notification
  - Destination IP is configured in the SNTP menu.



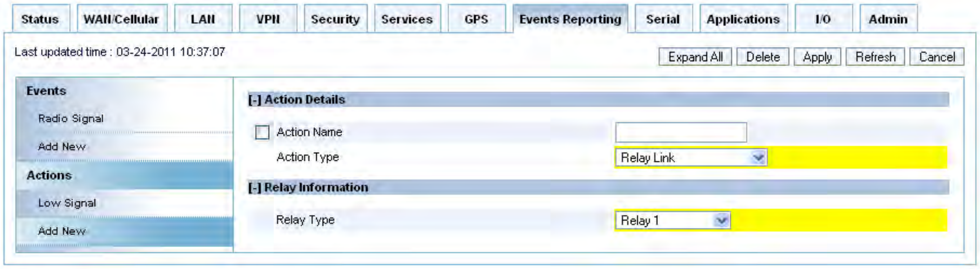
Last updated time : 03-24-2011 10:37:07

[-] Action Details

□ Action Name	
Action Type	SNMP TRAP

Figure 10-8: ACEmanager: Events Reporting - Action Type - SNMP TRAP

- Relay Link
  - Select the relay to link to, and Invert if necessary.



Last updated time : 03-24-2011 10:37:07

[-] Action Details

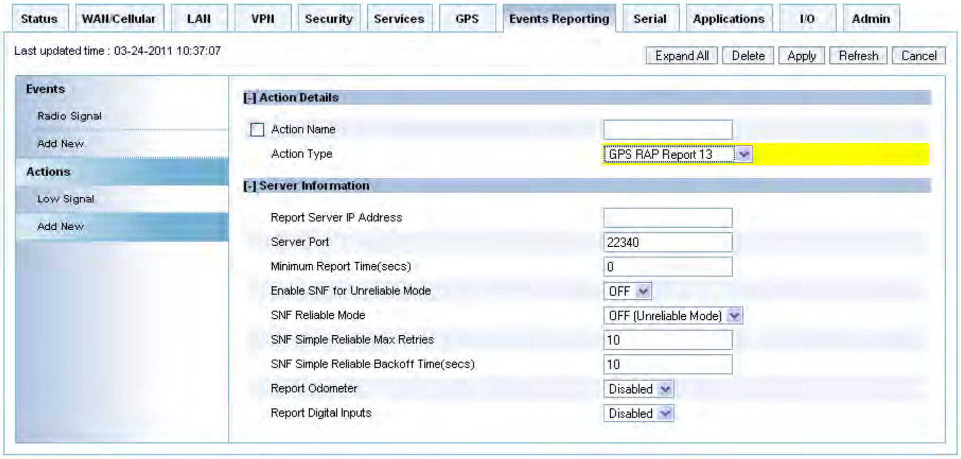
□ Action Name	
Action Type	Relay Link

[-] Relay Information

Relay Type	Relay 1

Figure 10-9: ACEmanager: Events Reporting - Action Type - Relay Link

- GPS RAP/Report 13 message
  - Destination report server and report type is configured in the AirLink Device Menu.



Last updated time : 03-24-2011 10:37:07

[-] Action Details

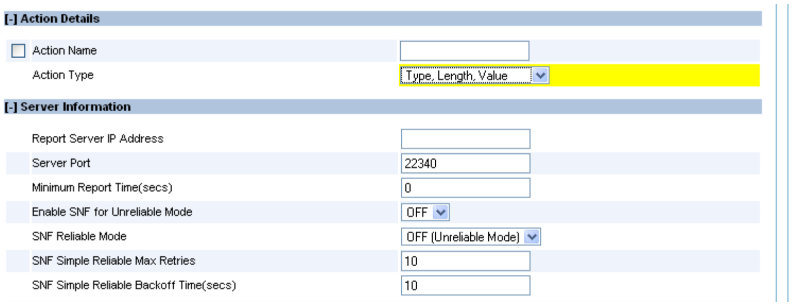
□ Action Name	
Action Type	GPS RAP Report 13

[-] Server Information

Report Server IP Address	
Server Port	22340
Minimum Report Time(secs)	0
Enable SNF for Unreliable Mode	OFF
SNF Reliable Mode	OFF (Unreliable Mode)
SNF Simple Reliable Max Retries	10
SNF Simple Reliable Backoff Time(secs)	10
Report Odometer	Disabled
Report Digital Inputs	Disabled

Figure 10-10: ACEmanager: Events Reporting - Action Type - GPS RAP Report 13

- Events Protocol message to a server
  - Destination report server is configured
  - Report format – TLV (Type, Length and Value), Binary, ASCII, XML. See Events Protocol (Appendix A) for details.



[-] Action Details

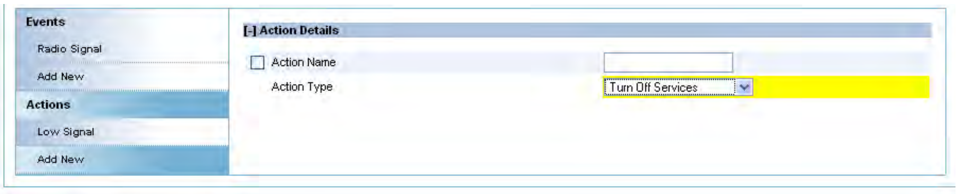
□ Action Name	
Action Type	Type, Length, Value

[-] Server Information

Report Server IP Address	
Server Port	22340
Minimum Report Time(secs)	0
Enable SNF for Unreliable Mode	OFF
SNF Reliable Mode	OFF (Unreliable Mode)
SNF Simple Reliable Max Retries	10
SNF Simple Reliable Backoff Time(secs)	10

Figure 10-11: ACEmanager: Events Reporting - Action Type - Type, Length, Value

- Turn-Off Services - This is also an option in the scroll-down list of the Action Type field.



[-] Action Details

□ Action Name	
Action Type	Turn Off Services

Figure 10-12: ACEmanager: Events - Actions - Action Type - Turn off Services

Email/SMS

- **To** - The email address where the report should be sent.
- **Subject** - The subject that should be displayed.
- **Message** - The message you want included with each report.
- **Body Type** - Select message in ASCI Text, SVS SCI and XML.

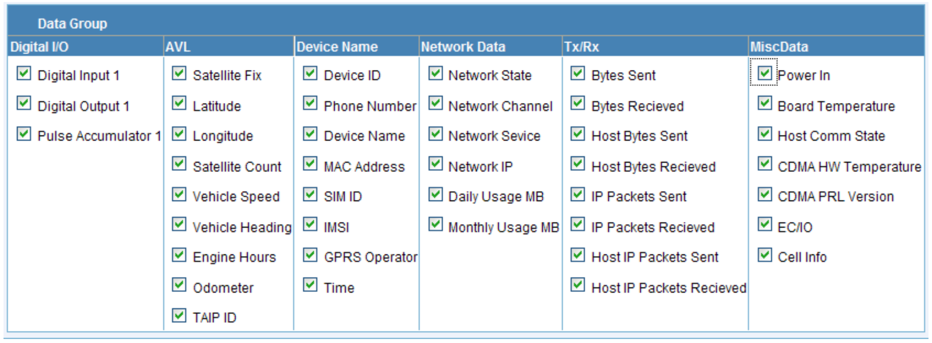
Note: You cannot send an Email with your AirLink device unless the Email server you have configured allows your AirLink device as a relay host. Talk to your network administrator to ensure you can send email through the email server using your AirLink device.

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.

Report Groups

You can select the data you want to be included in the report groups. The options are displayed. Check the box corresponding to the data displayed.

By default, all the boxes are checked.



Data Group

Digital I/O	AVL	Device Name	Network Data	Tx/Rx	MiscData
☑ Digital Input 1	☑ Satellite Fix	☑ Device ID	☑ Network State	☑ Bytes Sent	☑ Power In
☑ Digital Output 1	☑ Latitude	☑ Phone Number	☑ Network Channel	☑ Bytes Recieved	☑ Board Temperature
☑ Pulse Accumulator 1	☑ Longitude	☑ Device Name	☑ Network Sevice	☑ Host Bytes Sent	☑ Host Comm State
	☑ Satellite Count	☑ MAC Address	☑ Network IP	☑ Host Bytes Recieved	☑ CDMA HW Temperature
	☑ Vehicle Speed	☑ SIM ID	☑ Daily Usage MB	☑ IP Packets Sent	☑ CDMA PRL Version
	☑ Vehicle Heading	☑ IMSI	☑ Monthly Usage MB	☑ IP Packets Recieved	☑ EC/IO
	☑ Engine Hours	☑ GPRS Operator		☑ Host IP Packets Sent	☑ Cell Info
	☑ Odometer	☑ Time		☑ Host IP Packets Recieved	
	☑ TAIP ID				

Figure 10-13: ACEmanager: Events Reporting - Actions - Reports

The reports attributes are:

- AVL

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 AirLink Device.

- Digital I/O

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**- The status of the specific digital input.
- **Enable for Digital Output 1** The status of the specific relay output.
- **Enable for Pulse Accumulator 1**- The pulse count of the specific digital input.

- Network Data

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 the AirLink device is connected.
- **Enable for RSSI** - The network state for the AirLink device.
- **Enable for Network Service** - The network service for the AirLink device.
- **Enable for Network IP** - The IP address given by the cellular network.

- Tx/Rx

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

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.

- Misc Data

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 -** 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.

Note: For each group you can enable individual fields.

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

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.

Configure Events

To configure events,

1. Enter an Event Description. The event description will be displayed in the Events group in the left hand side panel.
2. Select any action and click on Add Action. Then select any Action Type and configure accordingly.
3. Click on Save and the action will be displayed in the Available Actions menu.

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.*

11: 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.

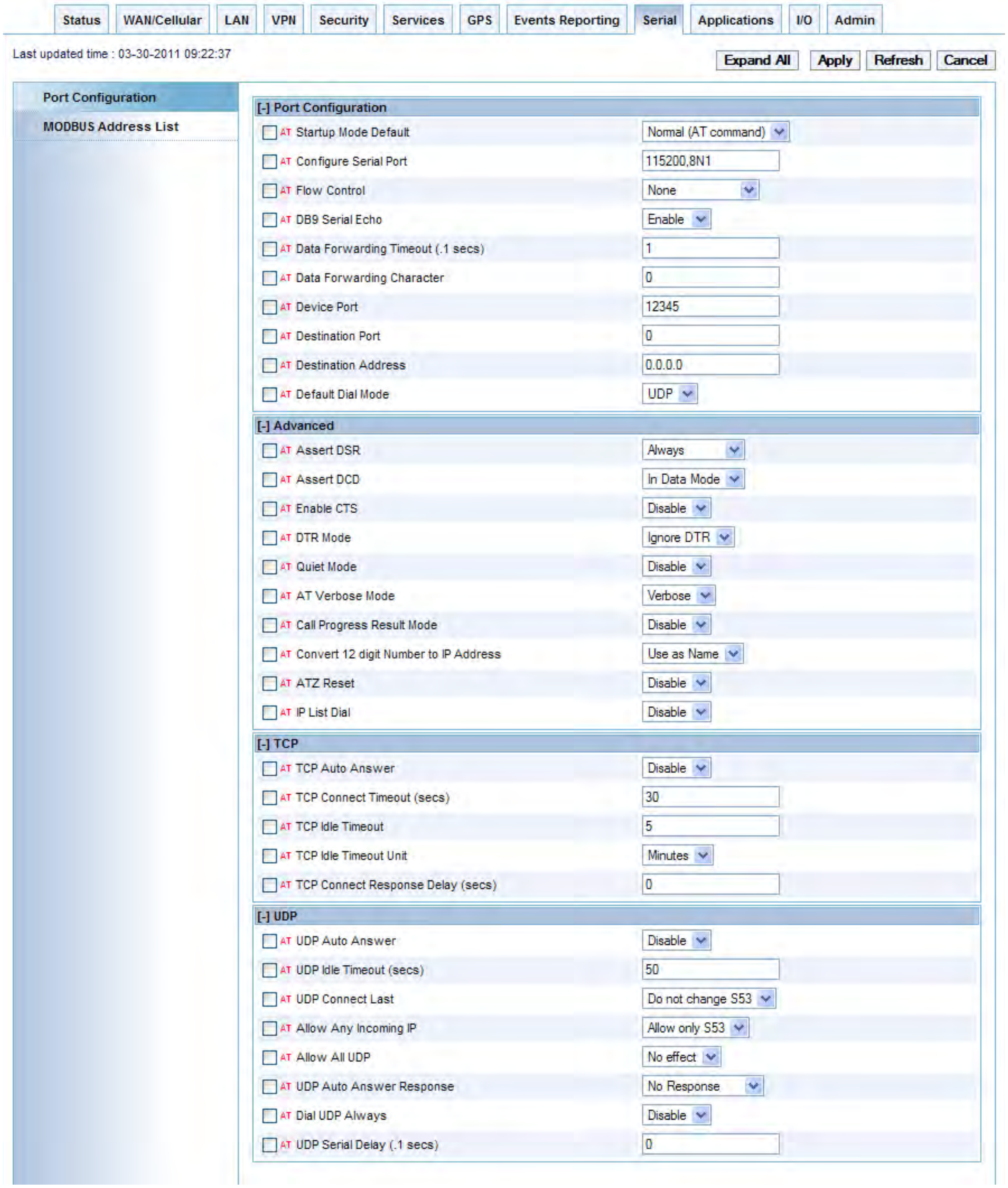
Port Configuration

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

Serial Port Configuration consists of four categories of configurable parameters:

- Port Configuration
- Advanced
- TCP
- UDP

These categories and their parameters are shown in Figure 11-1, and described in Table 11-1.



Last updated time : 03-30-2011 09:22:37

[-] Port Configuration	
□ AT Startup Mode Default	Normal (AT command)
□ AT Configure Serial Port	115200,8N1
□ AT Flow Control	None
□ AT DB9 Serial Echo	Enable
□ AT Data Forwarding Timeout (.1 secs)	1
□ AT Data Forwarding Character	0
□ AT Device Port	12345
□ AT Destination Port	0
□ AT Destination Address	0.0.0.0
□ AT Default Dial Mode	UDP
[-] Advanced	
□ AT Assert DSR	Always
□ AT Assert DCD	In Data Mode
□ AT Enable CTS	Disable
□ AT DTR Mode	Ignore DTR
□ AT Quiet Mode	Disable
□ AT AT Verbose Mode	Verbose
□ AT Call Progress Result Mode	Disable
□ AT Convert 12 digit Number to IP Address	Use as Name
□ AT ATZ Reset	Disable
□ AT IP List Dial	Disable
[-] TCP	
□ AT TCP Auto Answer	Disable
□ AT TCP Connect Timeout (secs)	30
□ AT TCP Idle Timeout	5
□ AT TCP Idle Timeout Unit	Minutes
□ AT TCP Connect Response Delay (secs)	0
[-] UDP	
□ AT UDP Auto Answer	Disable
□ AT UDP Idle Timeout (secs)	50
□ AT UDP Connect Last	Do not change S53
□ AT Allow Any Incoming IP	Allow only S53
□ AT Allow All UDP	No effect
□ AT UDP Auto Answer Response	No Response
□ AT Dial UDP Always	Disable
□ AT UDP Serial Delay (.1 secs)	0

Figure 11-1: ACEmanager: Serial - Port Configuration

Table 11-1: Serial Port Configuration

Field	Description
Port Configuration	
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 . • Normal (AT command) • UDP • TCP • Modbus ASCII • Modbus RTU (Binary) • BSAP • Variable Modbus Default: Normal
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. • None - No flow control is being used. • Hardware - RTS/CTS hardware flow control is being used. • Transparent SW - 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 @@. Default: None
DB9 Serial Echo	Toggle AT command echo mode. • Enable • Disable. With more than one connection type (serial, Telnet, and USB/Serial, the echo command is set differently on each interface. Default: Enable.
Data Forwarding Timeout (.1 secs)	Data forwarding idle time-out. If set to 0, a forwarding time-out of 10ms is used. Used in UDP or TCP PAD mode. Increments in 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 Source 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 Mode	Options for the Default Dial Data Mode are: • TCP • UDP Default: UDP

Table 11-1: Serial Port Configuration

Field	Description
Advanced	
Assert DSR	Assert DSR always when the device is in a data mode (UDP, TCP, etc.), or when the device is in network coverage. Options are: • Always • In Data Mode • In Coverage Default: Always
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. Options are: • Always • In Data Mode • In Coverage Default: Always
Enable CTS	Assert CTS when there is network coverage. Options: • Disable • Enable Defaulty: Disable
DTR Mode	Use DTR from the serial device, or ignore DTR (same as S211). Options: • Use DTR • Ignore DTR Default: Ignore DTR
Quiet Mode	Disable or enable display of device responses. Options: • Disable • Enable Defaulty: Disable
AT Verbose Mode	Configure AT command responses. Options: • Verbose • Numeric Defaulty: Verbose
Call Progress Result Mode	When enabled adds 19200 to CONNECT messages. Options: • Disable • Enable Defaulty: Disable.
Convert 12 digit Number to IP Address	Converts 12 digit number to an IP address 111222333444 -> 111.222.333.444. Options: • Use as Name • Use as IP Default: Use as Name.

Table 11-1: Serial Port Configuration

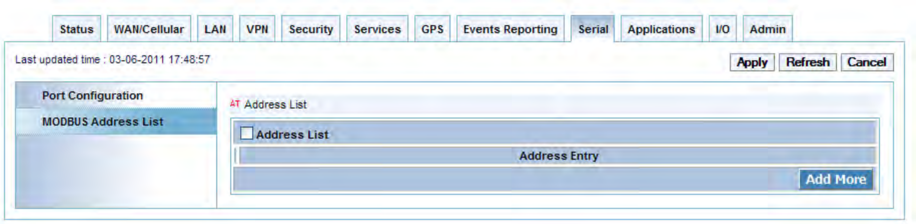
Field	Description
ATZ Reset	When set to Enable, +++ ATZ will reset the device. Options: • Disable • Enable Default: Enable
IP List Dial	This allows access to the Modbus IP Address using the first two digits of the dial string. E.g., ATDT1234567 would imply ID index 12 on the Modbus Address list and use the associated IP Address as the destination. Options: • Disable • Enable Defaulty: Disable
TCP	
TCP Auto Answer	This register determines how the AirLink 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. • Disable • Enable Default: Disable
TCP Connect Timeout (secs)	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. Options: • Minutes • secs Default: Minutes
TCP Idle Timeout Unit	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 (secs)	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
UDP	
UDP Auto Answer	Enables UDP auto answer (half-open) mode. • n=0 : Normal mode • n=2 : Enable UDP auto answer mode.
UDP Idle Timeout (secs)	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.

Table 11-1: Serial Port Configuration

Field	Description
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. • Do not change S53 • Set S53 last IP Default: Do not change S53
Allow Any Incoming IP	Allow any incoming IP address to connect when UDP auto answer is enabled (S82=2) or only S53 to connect when UDP Auto Answer mode is enabled (S82=20). This is subject to the trusted IP Address filters. Options: • Allow only S53 • Allow any IP address Default: Allow only S53.
Allow All UDP	Accepts UDP packets from all IP addresses 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. Options: • No effect • Allow all Default: No effect
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 (.1 secs)	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.

MODBUS Address List

To add an Address Entry, click on Add More.



Last updated time : 03-06-2011 17:48:57

Figure 11-2: ACEmanager: MODBUS Address List

12: Application Configuration

12

- Data Usage
- Garmin

The Application tab that displays in ACEmanager is applicable to all AirLink devices.

The Applications tab consists of a Data Usage and a Garmin application section.

Data Usage

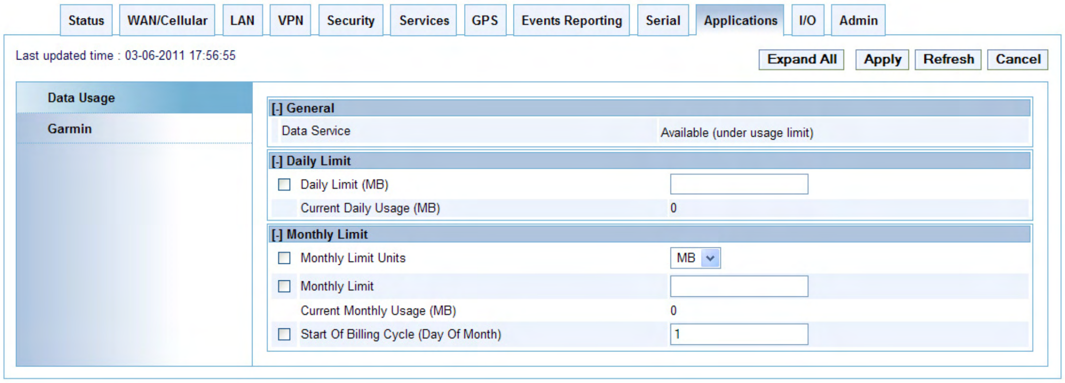
The Data Usage feature available in the Application tab provides users with a way to actively monitor cellular data usage.

A user can:

- Actively monitor the cellular data usage by configuring usage level thresholds that result in notifications being sent to the user.
- Halt device data traffic until the end of the billing period. In the event that the user decides the halt the data traffic, the management interface to ALEOS is still available.
- Set usage levels and thresholds on a monthly and/or daily limit.

To Configure Data Usage,

1. Select the Application tab and the Data Usage page, and enter the fields of data usage, such as monthly limit (in GB or MB) and the day of the month that starts the cellular billing cycle.



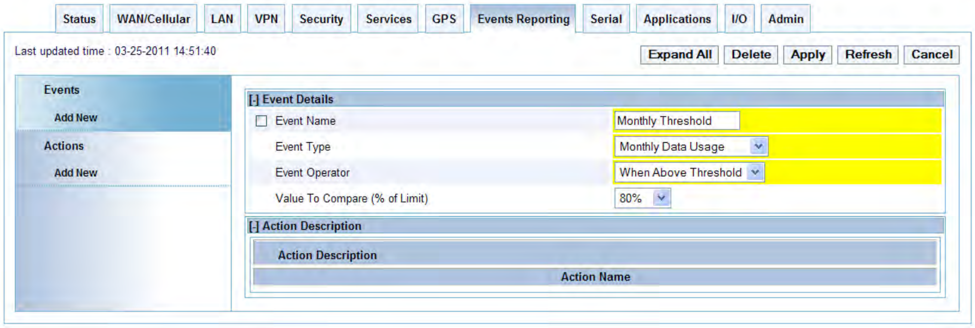
Last updated time : 03-06-2011 17:56:55

[-] General	
Data Service	Available (under usage limit)
[-] Daily Limit	
☐ Daily Limit (MB)	
Current Daily Usage (MB)	0
[-] Monthly Limit	
☐ Monthly Limit Units	MB
☐ Monthly Limit	
Current Monthly Usage (MB)	0
☐ Start Of Billing Cycle (Day Of Month)	1

Figure 12-1: ACEmanager: Applications: Data Usage

Field	Description
General	
Data Service	If Data Service is on, “Available” displays on the user interface. If data usage exceeds the configured data limit, “Not Available” displays on the screen.
Daily Limit	
Daily Limit (MB)	This is the user specified daily data usage (in MBs) limit (24 hour limit). The user can specify data usage limits on a daily or monthly basis. A limit is essentially a threshold that can trigger the software to take a user specified action if the usage goes above the threshold.
Current Daily Usage (MB)	Displays the current daily data usage (in MBs). For example, if the daily limit is 60, the current daily usage should not exceed 60. 90% is the usage limit. You cannot access the cellular world if you exceed the limit. You can, however, Telnet, OTA, etc.
Monthly Limit	
Monthly Limit Units	Select an MB or GB unit for monthly data usage. Default: MB.
Monthly Limit	This is the user specified monthly data usage limit. Data usage accumulates on a monthly basis and on the date specified by the user (the “rolling month”). Data usage will accumulate during the month until the end of the next billing period at which point the data usage totals will be reset.
Current Monthly Usage (MB)	Displays the current monthly data usage.
Start of Billing Cycle (Day of Month)	Enter the desired start of the billing cycle. For example, 3 (Day 3 of every month).

2. Select the Events Reporting tab and configure a data usage threshold. The threshold is specified as a percentage value of the monthly or daily limit. For example, if the you have specified 5 GB as the monthly limit, and the threshold is set at 80%, then the threshold is reached when 4 GB data usage is reached.

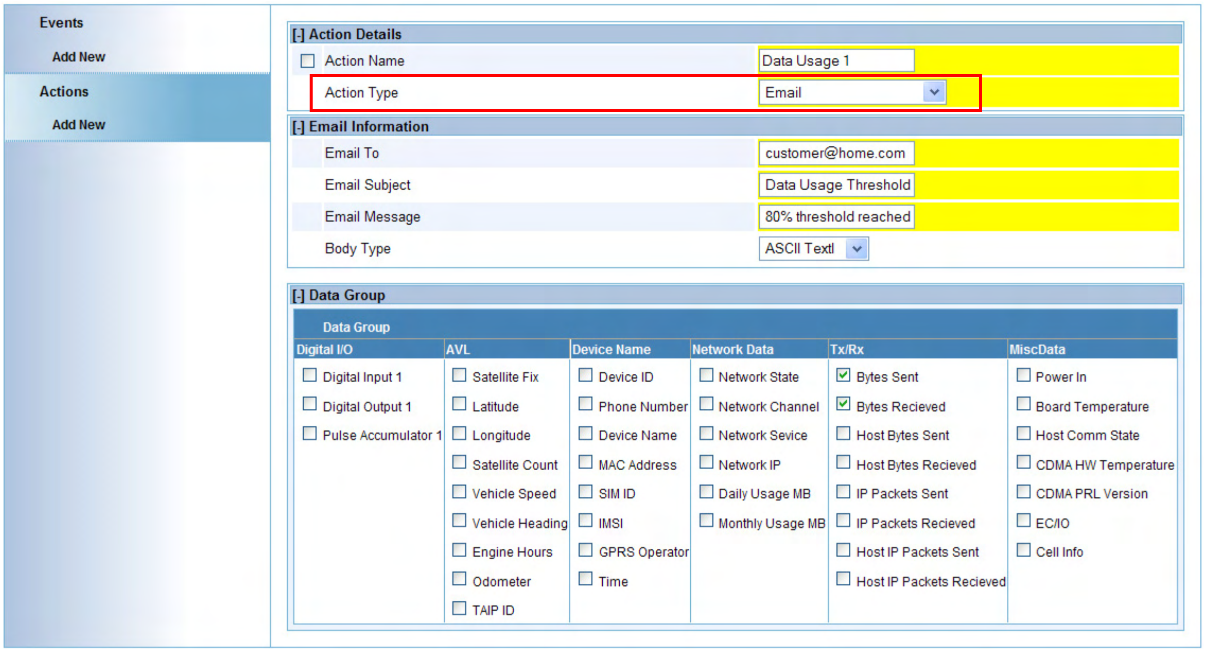


Last updated time : 03-25-2011 14:51:40

☐ Event Name	Monthly Threshold
Event Type	Monthly Data Usage
Event Operator	When Above Threshold
Value To Compare (% of Limit)	80%

Figure 12-2: ACEmanager: Events Reporting - Events

3. Select the Actions group under Events Reporting tab, and specify an action to be performed when the Event is triggered.



[-] Action Details

□ Action Name	Data Usage 1
Action Type	Email

[-] Email Information

Email To	customer@home.com
Email Subject	Data Usage Threshold
Email Message	80% threshold reached
Body Type	ASCII Text

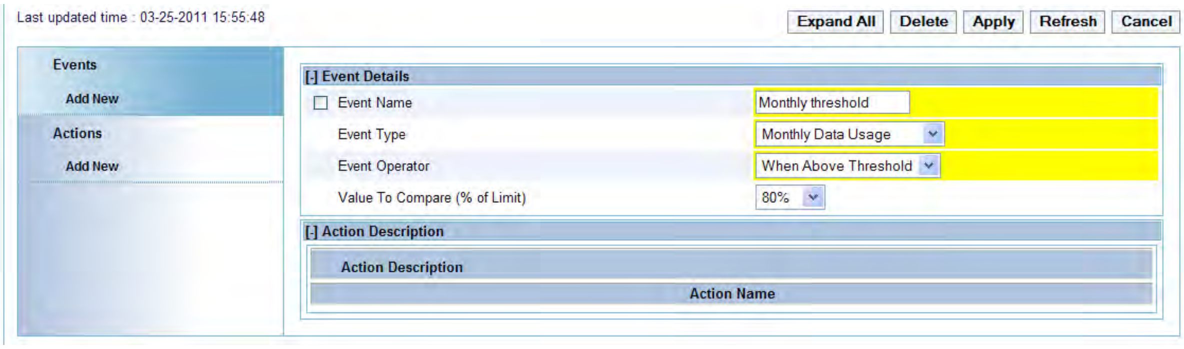
[-] Data Group

Data Group

Digital I/O	AVL	Device Name	Network Data	Tx/Rx	MiscData
□ Digital Input 1	□ Satellite Fix	□ Device ID	□ Network State	☑ Bytes Sent	□ Power In
□ Digital Output 1	□ Latitude	□ Phone Number	□ Network Channel	☑ Bytes Recieved	□ Board Temperature
□ Pulse Accumulator 1	□ Longitude	□ Device Name	□ Network Sevice	□ Host Bytes Sent	□ Host Comm State
	□ Satellite Count	□ MAC Address	□ Network IP	□ Host Bytes Recieved	□ CDMA HW Temperature
	□ Vehicle Speed	□ SIM ID	□ Daily Usage MB	□ IP Packets Sent	□ CDMA PRL Version
	□ Vehicle Heading	□ IMSI	□ Monthly Usage MB	□ IP Packets Recieved	□ EC/IO
	□ Engine Hours	□ GPRS Operator		□ Host IP Packets Sent	□ Cell Info
	□ Odometer	□ Time		□ Host IP Packets Recieved	
	□ TAIP ID				

Figure 12-3: ACEmanager: Events Reporting - Actions

4. Select the Events group page again to associate the Data Usage Action with the Data Usage Event.



Last updated time : 03-25-2011 15:55:48

[-] Event Details

□ Event Name	Monthly threshold
Event Type	Monthly Data Usage
Event Operator	When Above Threshold
Value To Compare (% of Limit)	80%

[-] Action Description

Action Description

Action Name

Figure 12-4: ACEmanager: Events Reporting - Events

Note: Daily and monthly limits will reset again at the end of the billing cycle.

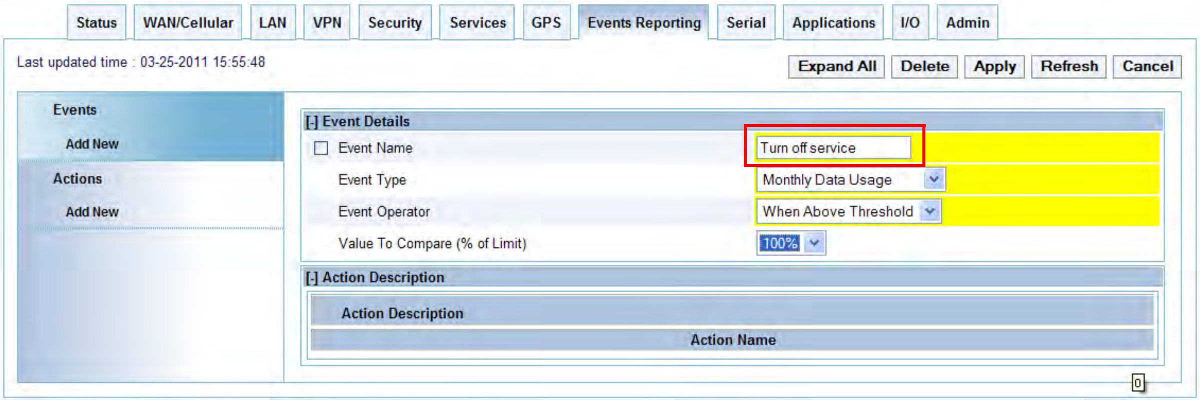
Once the data plan limit is reached, the user may desire to turn off cellular communication with the any user devices connected to the host port until the next billing cycle starts.

To configure the device to turn off services, another event and action must be configured.

If the user decides to disable the events and actions associated with the Data Usage feature, then the Data Usage Events must be deleted.

To turn off services on the data plan when the limit is reached:

1. Configure an event and an action. The event (shown below) is triggered when 100% of the monthly plan limit is reached.



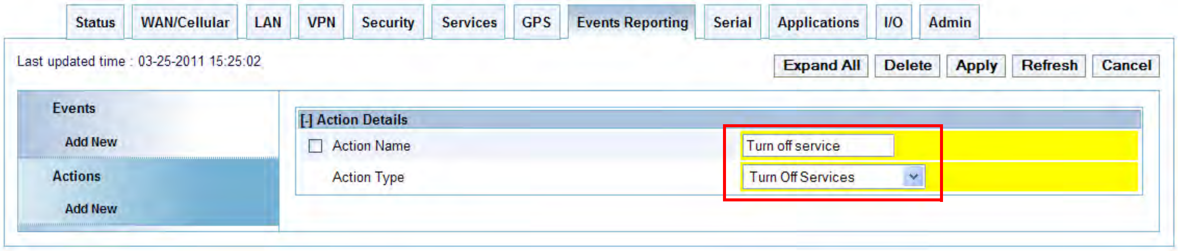
Last updated time : 03-25-2011 15:55:48

[-] Event Details

□ Event Name	Turn off service
Event Type	Monthly Data Usage
Event Operator	When Above Threshold
Value To Compare (% of Limit)	100%

Figure 12-5: ACEmanager: Events Reporting - Events -Turn off Service

2. Create an action to turn off the services. When triggered, this action will prevent cellular communication to any user device connected to a host port.



Last updated time : 03-25-2011 15:25:02

[-] Action Details

□ Action Name	Turn off service
Action Type	Turn Off Services

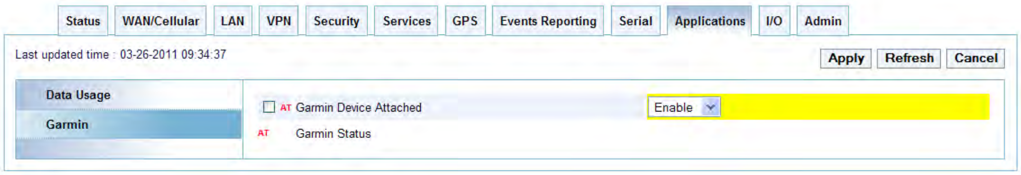
Figure 12-6: ACEmanager: Events Reporting - Actions - Add New

Garmin

Garmin provides navigation devices for versatile fleet monitoring solutions. AirLink devices provide 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.

To configure Garmin in ACEmanager:

1. Enable Garmin. Under the **Applications - Garmin** tab, set Garmin Device Attached to Enabled.

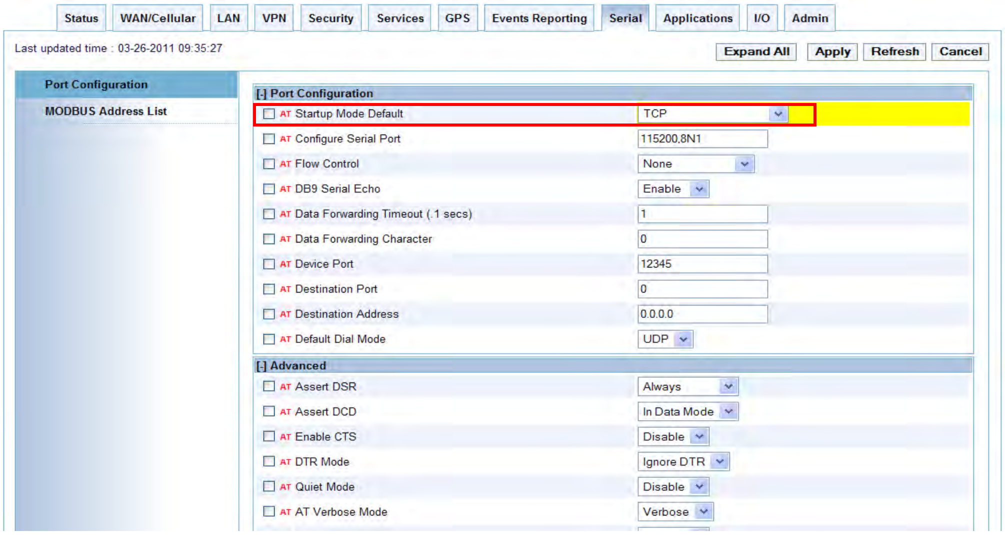


Last updated time : 03-26-2011 09:34:37

□ AT Garmin Device Attached	Enable
AT Garmin Status	

Figure 12-7: ACEmanager: Applications - Garmin

2. Set the Host Mode to TCP. Under the **Serial – Port Configuration** tab, set the Startup Mode Default parameter to TCP.



Last updated time : 03-26-2011 09:35:27

[-] Port Configuration

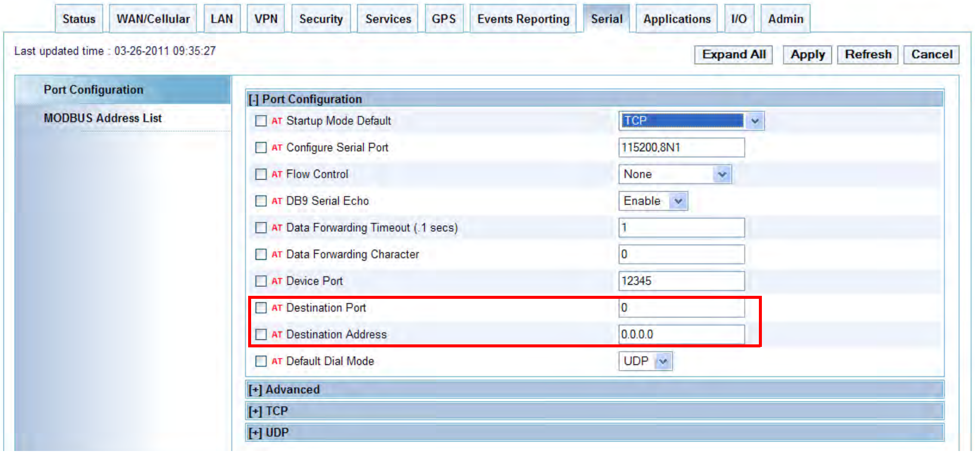
□ AT Startup Mode Default	TCP
□ AT Configure Serial Port	115200,8N1
□ AT Flow Control	None
□ AT DB9 Serial Echo	Enable
□ AT Data Forwarding Timeout (.1 secs)	1
□ AT Data Forwarding Character	0
□ AT Device Port	12345
□ AT Destination Port	0
□ AT Destination Address	0.0.0.0
□ AT Default Dial Mode	UDP

[-] Advanced

□ AT Assert DSR	Always
□ AT Assert DCD	In Data Mode
□ AT Enable CTS	Disable
□ AT DTR Mode	Ignore DTR
□ AT Quiet Mode	Disable
□ AT AT Verbose Mode	Verbose

Figure 12-8: ACEmanager: Serial - Port Configuration

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



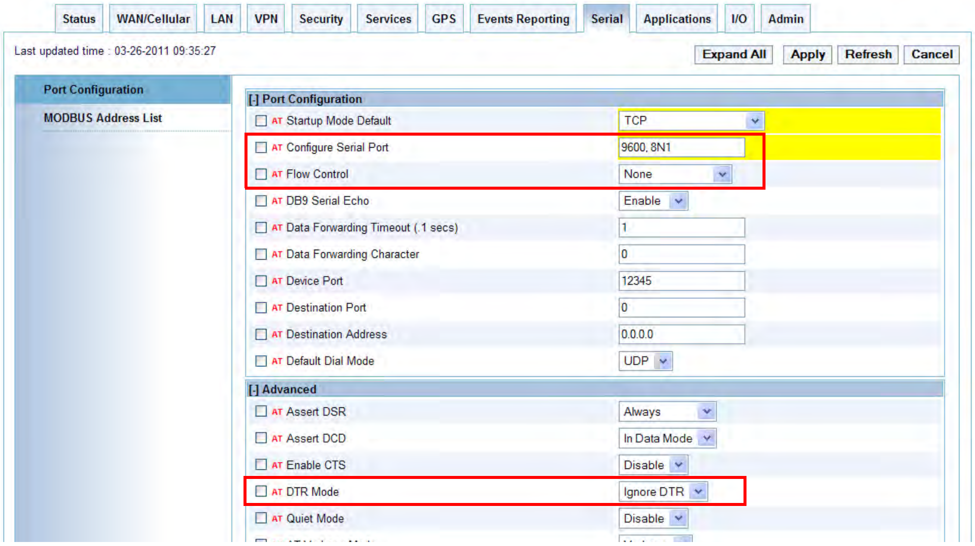
Last updated time : 03-26-2011 09:35:27

[-] Port Configuration

□ AT Startup Mode Default	TCP
□ AT Configure Serial Port	115200,8N1
□ AT Flow Control	None
□ AT DB9 Serial Echo	Enable
□ AT Data Forwarding Timeout (1 secs)	1
□ AT Data Forwarding Character	0
□ AT Device Port	12345
□ AT Destination Port	0
□ AT Destination Address	0.0.0.0
□ AT Default Dial Mode	UDP

Figure 12-9: ACEmanager: Serial - Port Configuration

4. Configure the serial port. To communicate with Garmin:
   - Input **9600, 8N1** in Startup Mode Default
   - Select **None** in Flow Control
   - Select **Ignore DTR** in DTR Mode.



Last updated time : 03-26-2011 09:35:27

[-] Port Configuration

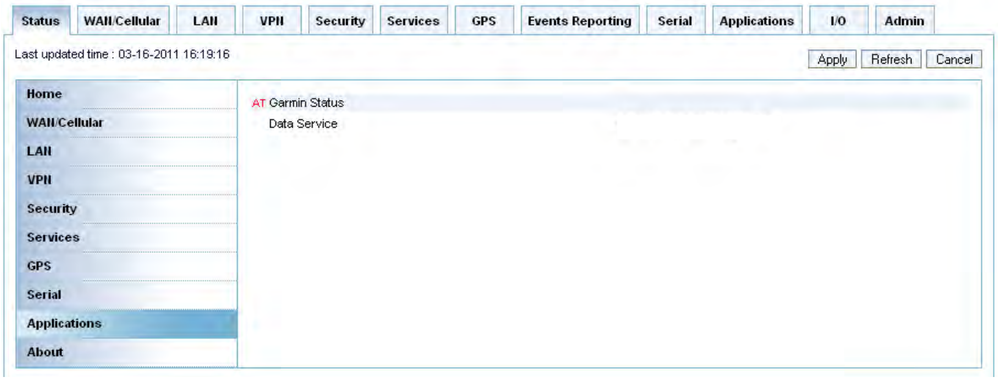
□ AT Startup Mode Default	TCP
□ AT Configure Serial Port	9600, 8N1
□ AT Flow Control	None
□ AT DB9 Serial Echo	Enable
□ AT Data Forwarding Timeout (.1 secs)	1
□ AT Data Forwarding Character	0
□ AT Device Port	12345
□ AT Destination Port	0
□ AT Destination Address	0.0.0.0
□ AT Default Dial Mode	UDP

[-] Advanced

□ AT Assert DSR	Always
□ AT Assert DCD	In Data Mode
□ AT Enable CTS	Disable
□ AT DTR Mode	Ignore DTR
□ AT Quiet Mode	Disable

Figure 12-10: ACEmanager: Serial - Port Configuration parameters

5. Check the Garmin’s communications status under the **Status - Applications** tab. Garmin data service states are:
    - Not Connected - Not acknowledged by the AVL server
    - Connected - Acknowledged by the AVL server.



Last updated time : 03-16-2011 16:19:16

AT Garmin Status

Data Service

Figure 12-11: ACEmanager: Status - Applications - Garmin Status

6. **Reboot** the AirLink device to apply the changes. The “Garmin Status” now displays:
    - Connected - Acknowledged by the AVL server.

*Note: The Garmin Status field displays **only** if the Garmin application is Connected.*

13: I/O Configuration

13

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

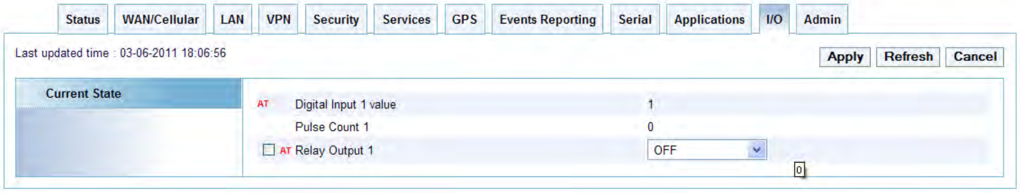
This group includes configuration commands for the digital inputs and outputs as applicable to an AirLink device. Some of the values shown as a part of this group are not changeable but reflect the current status. Only those devices with available inputs and outputs will display this group.

Refer to the Inputs, Relay Outputs, and Power Status chapter in the respective Hardware Users Guide 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). The current state of the Relay or Digital Output is displayed and can be changed directly.



Last updated time : 03-06-2011 18:06:56

AT Digital Input 1 value 1

Pulse Count 1 0

□ AT Relay Output 1 OFF

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

Table 13-1: I/O: Current State

Command	Description
Digital Input 1 value	Query individual digital inputs. The digital inputs report either a 0 (open) or 1 (closed). • n= 1 Input number
Pulse Count 1	On devices with a digital input that can be configured for use as a digital output, the pulse counts will also reflect output changes.
Relay Output 1	Set or query the relay output. Options: • OFF • Drive Action Low

Pulse Count

Following are some Pulse Count details:

- The AirLink device has one digital input and one pulse count.
- Pulses are counted on falling edge (high - >low). This can be added.
- 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.

14: Admin

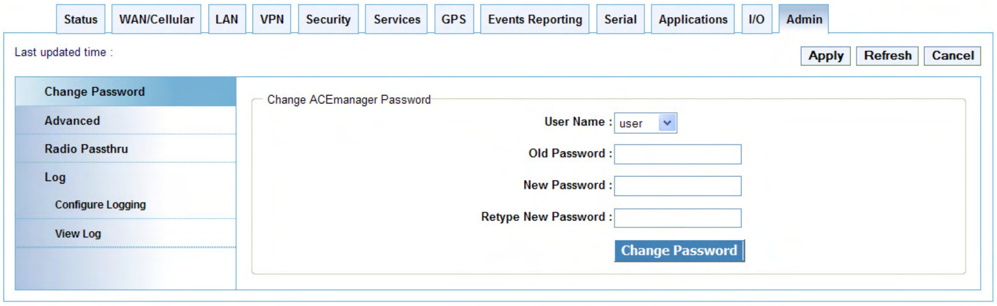
14

The Admin tab that displays in ACEmanager is applicable to all Sierra Wireless AirLink GX400 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.



User Name : user

Old Password :

New Password :

Retype New Password :

Figure 14-1: ACEmanager: Admin

To change the default password,

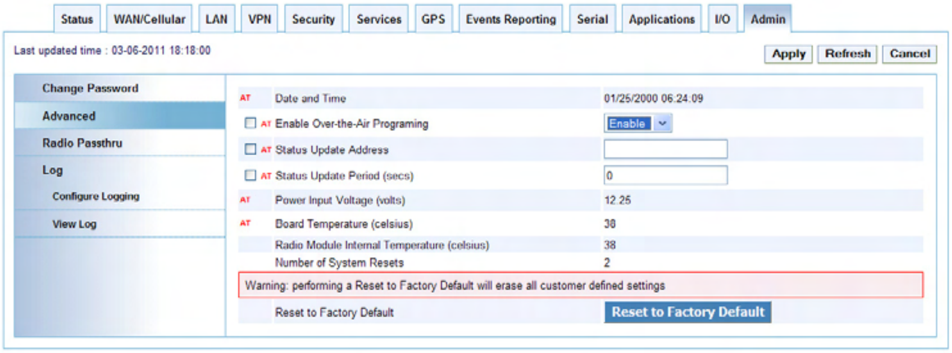
1. Select the User Name: user or viewer
2. Enter the old password
3. Enter the new password twice
4. Click on Change Password.

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

Note: There are two user levels in the User Name drop down menu. The 'user' has full admin rights and can edit the configuration; the 'viewer' can only view the configuration and status of the device. Viewer can change the 'viewer' password. User can change both.

Advanced

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



Last updated time : 03-06-2011 18:18:00

AT	Date and Time	01/25/2000 06:24:09
□ AT	Enable Over-the-Air Programing	Enable
□ AT	Status Update Address	
□ AT	Status Update Period (secs)	0
AT	Power Input Voltage (volts)	12.25
AT	Board Temperature (celsius)	38
	Radio Module Internal Temperature (celsius)	38
	Number of System Resets	2

Warning: performing a Reset to Factory Default will erase all customer defined settings

Reset to Factory Default

Figure 14-2: ACEmanager: Admin - Default

Field	Description
Date and Time	Queries the internal clock. The date and time are always specified in 24-hour notation (UTC). • mm/dd/yyyy= date in month/day/year notation • hh:mm:ss= time in 24-hour notation.
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. • Enable • Disable Default: Enable
Status Update Address	Device Status Update Address where Name/Port is the domain name (or IP address) and port of the machine where the device status updates will be sent. This report can be sent to a LAN connected host (e.g., 192.168.13.100/1122) or to a remote location (e.g., newb.eairlink.com/17000). The status parameters are sent in an XML format. • name= domain name or IP address • port= port
Status Update Period (secs)	The time interval (in seconds) when a status update should be sent.
Power Input Voltage (volts)	Displays the power input voltage in volts.
Board Temperature (celsius)	Displays the board temperature in degrees (celsius).
Radio Module Internal Temperature (celsius)	Displays the temperature of the internal radio module in degrees (celsius).

Field	Description
Number of System Resets	Counter of the number of system resets over the life of the device or since the configuration was reset.
Reset to Factory Default	Resets all settings (passwords, LAN and WAN configuration, security settings, etc.) to the original factory settings.

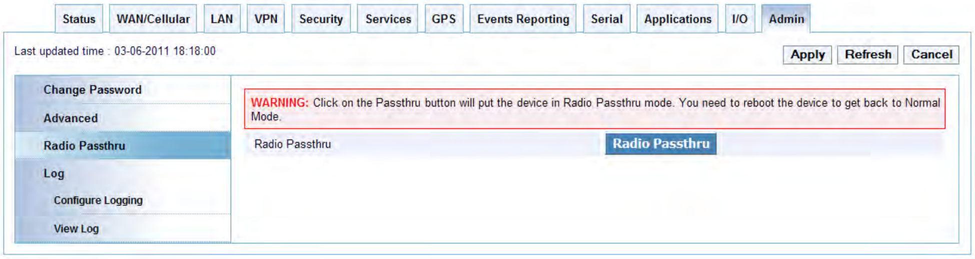
Radio Passthru

Radio Passthru allows a direct connection, using USB, to the internal radio. Normal cellular radio operation is suspended while Radio Passthru is enabled.

Radio Passthru is generally used only in certain troubleshooting scenarios.

The hardware bypass will remain in effect until the ALEOS software resets either via ACEmanager command or the hardware Reset button.

Note: Special drivers are required to connect to the radio. Additionally, while it is possible to send AT commands to the radio using a terminal connection, there are software applications designed to communicate with the radio directly. If you need to use Radio Passthru, contact your Sierra Wireless AirLink representative to obtain the needed drivers and/or software application.



Last updated time : 03-06-2011 18:18:00

WARNING: Click on the Passthru button will put the device in Radio Passthru mode. You need to reboot the device to get back to Normal Mode.

Radio Passthru

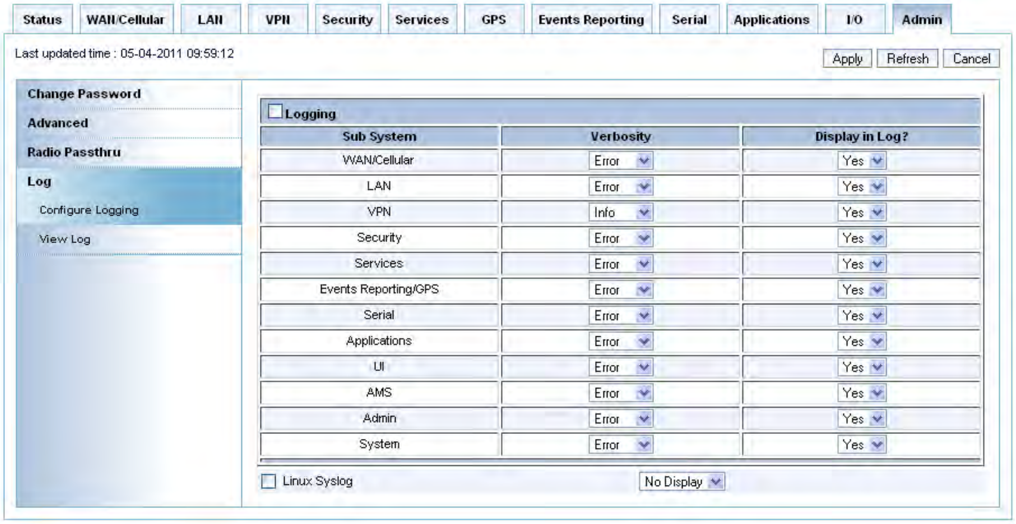
Figure 14-3: ACEmanager: Admin - Radio Passthru

Log

The Log file is a system log of the AirLink device.

The Logging configuration screen enables the user to configure log verbosity and display filtering. The View Log screen enables the user to view and save logs. The logs are in clear text.

The Configure Logging group is organized by Subsystems. Separate filters, based on subsystem and severity, are applied when the messages are generated and when the messages are displayed. Four severity levels are supported for filtering: Critical, Error, Info, and Debug. Select one of these levels from the Verbosity column drop-down lists.



Last updated time : 05-04-2011 09:59:12

☐ Logging

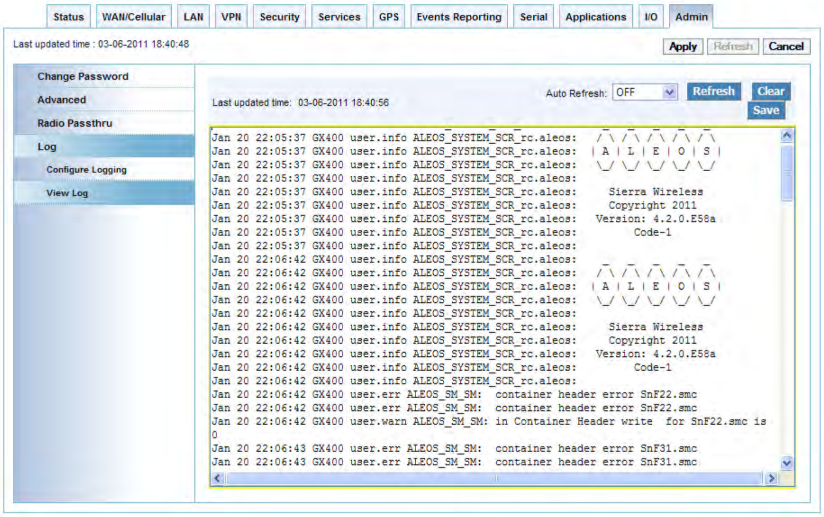
Sub System	Verbosity	Display in Log?
WAN/Cellular	Error	Yes
LAN	Error	Yes
VPN	Info	Yes
Security	Error	Yes
Services	Error	Yes
Events Reporting/GPS	Error	Yes
Serial	Error	Yes
Applications	Error	Yes
UI	Error	Yes
AMS	Error	Yes
Admin	Error	Yes
System	Error	Yes

☐ Linux Syslog: No Display

Figure 14-4: ACEmanager: Admin - Log, Configure Logging

Field	Description
Logging	Logging enables the user to configure log verbosity and display filtering for various subsystems. Sub System fields are: • WAN/Cellular • LAN • VPN • Security • Services • Events Reporting/OPS • Serial • Applications • UI • AMS • Admin • System Separate filters, based on subsystem and severity, are applied when the messages are generated and when the messages are displayed. Four severity levels are supported for filtering in the drop-down lists for Verbosity: Critical, Error, Info (information), and Debug. (Note: The VPN Sub System only allows for Info and Debug.) The user also has the option (Yes or No) of which Sub System fields to display in the log.
Linux Syslog	A Linux Syslog can be displayed. Options: • No Display • Display Default: No Display

Use View Log for troubleshooting purposes (e.g., when setting up the IPsec 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.



Last updated time : 03-06-2011 18:40:48

Last updated time: 03-06-2011 18:40:56

Auto Refresh: OFF

```
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:   / \ / \ / \ / \ / \
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:  | A | L | E | O | S |
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:   \_/ \_/ \_/ \_/ \_/
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:     Sierra Wireless
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:     Copyright 2011
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:   Version: 4.2.0.E58a
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:         Code-1
Jan 20 22:05:37 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:    _   _   _   _   _
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:   / \ / \ / \ / \ / \
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:  | A | L | E | O | S |
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:   \_/ \_/ \_/ \_/ \_/
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:     Sierra Wireless
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:     Copyright 2011
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:   Version: 4.2.0.E58a
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:         Code-1
Jan 20 22:06:42 GX400 user.info ALEOS_SYSTEM_SCR_rc.aleos:
Jan 20 22:06:42 GX400 user.err ALEOS_SM_SM:  container header error SnF22.smc
Jan 20 22:06:42 GX400 user.err ALEOS_SM_SM:  container header error SnF22.smc
Jan 20 22:06:42 GX400 user.warn ALEOS_SM_SM: in Container Header write  for SnF22.smc is
0
Jan 20 22:06:43 GX400 user.err ALEOS_SM_SM:  container header error SnF31.smc
Jan 20 22:06:43 GX400 user.err ALEOS_SM_SM:  container header error SnF31.smc
```

Figure 14-5: ACEmanager: Admin - Log, View Log

To view a log:

1. Select a Verbosity severity level, and choose “Yes” from Display in Log?
2. Apply Refresh.
3. Go to the View Log menu item, and select Refresh.
4. Select Save. A window appears with a text file.

User action options on the View Log screen include:

- Auto Refresh - The drop-down menu allows the user to set up an automatic log page refresh, and the interval between refreshes: 30 secs, 1 minute, or 2 minutes.
- Refresh button - Initiates a manual page refresh.
- Clear button - Clears out the tunnels.
- Save button - Creates a text file of the log.

A: Modbus/BSAP Configuration

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

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 an AirLink 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.

1. Configure the ports.

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.

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: 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.

*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.*

1. 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.

2. Configure other RTU settings.

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

3. 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.

B: PPP over Ethernet (PPPoE)

Configuring a PPPoE Connection in Windows

Note: These directions listed are for Windows XP.

1. Create a new network connection

   a. Select *Start* > *Connect To* > *Show All Connections*. This will open the Network Connections window.

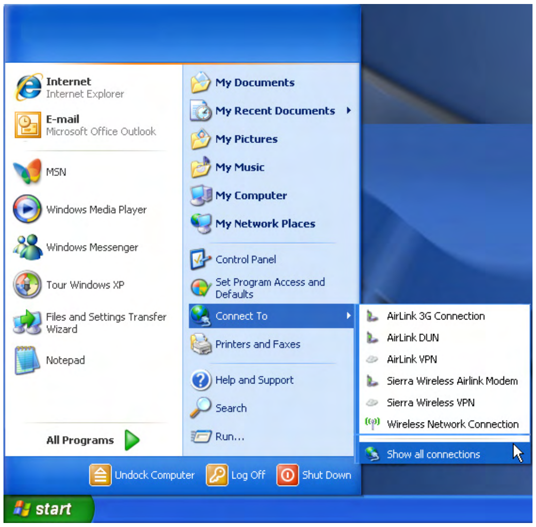


Figure B-1: Windows: Start menu

   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.

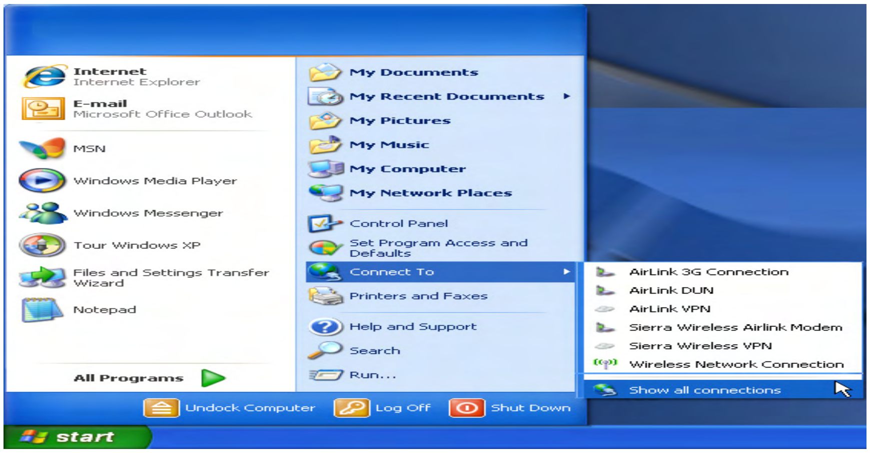
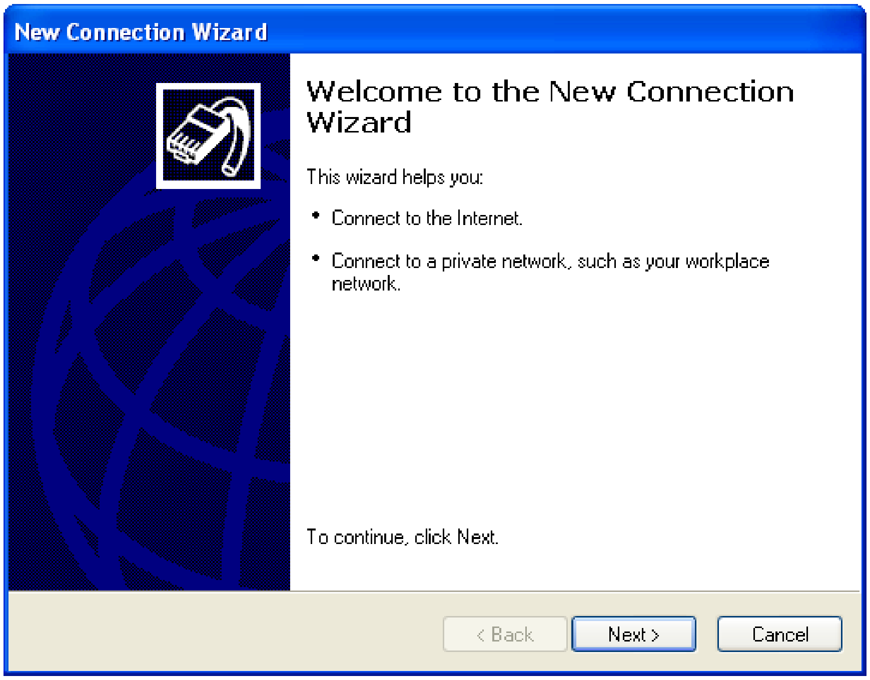


Figure B-2: Windows: Network Connections

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

d. *Next.*


New Connection Wizard

Welcome to the New Connection Wizard

This wizard helps you:

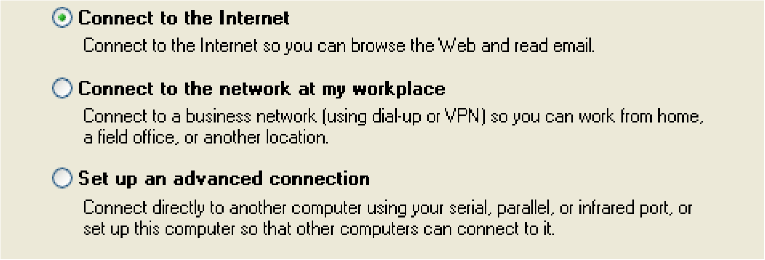
- Connect to the Internet.
- Connect to a private network, such as your workplace network.

To continue, click Next.

Figure B-3: New Connection Wizard

e. Select *Connect to the Internet*.

f. Select *Next*.



● **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

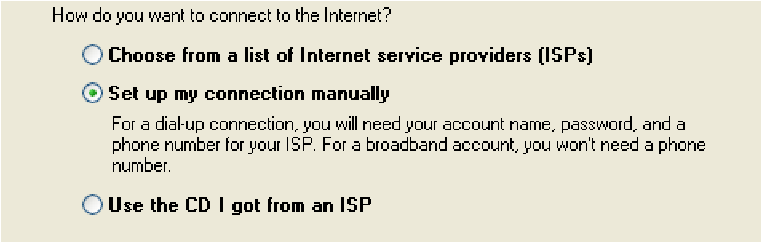
○ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

Figure B-4: New Connection: Type

g. Select *Set up my connection manually.*

h. Select *Next*.



How do you want to connect to the Internet?

○ **Choose from a list of Internet service providers (ISPs)**

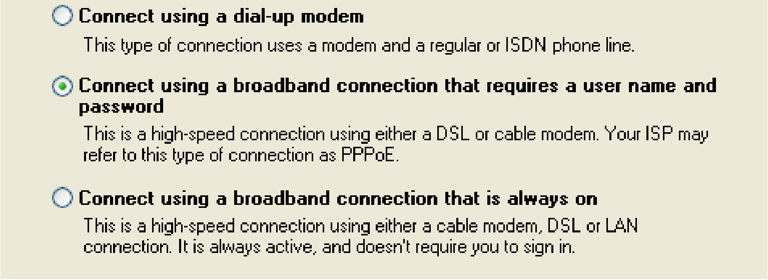
● **Set up my connection manually**
For a dial-up connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number.

○ **Use the CD I got from an ISP**

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

i. Select *Connect using a broadband connection*.

j. Select *Next*.



○ **Connect using a dial-up modem**
This type of connection uses a modem and a regular or ISDN phone line.

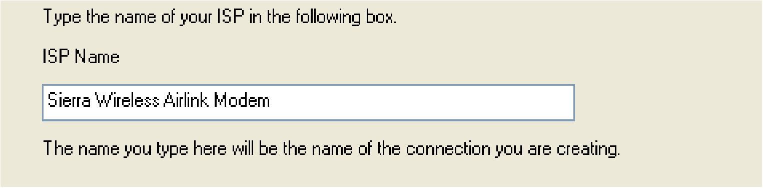
● **Connect using a broadband connection that requires a user name and password**
This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.

○ **Connect using a broadband connection that is always on**
This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.

Figure B-6: New Connection: Connect using broadband

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

l. Select *Next*.



Type the name of your ISP in the following box.

ISP Name

Sierra Wireless Airlink Modem

The name you type here will be the name of the connection you are creating.

Figure B-7: New Connection: Connection Name

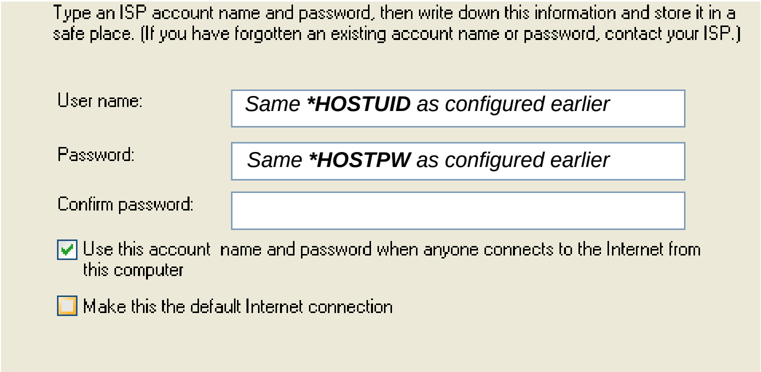
Tip: *The name provided here will not effect the connection in any way. It is only a label for the icon. It can be the name of your wireless service provider (Provider), your modem (AirLink device), or any other designation for the connection.*

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.*



Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)

User name: *Same* ****HOSTUID** *as configured earlier*

Password: *Same* ****HOSTPW** *as configured earlier*

Confirm password:

☑ Use this account name and password when anyone connects to the Internet from this computer

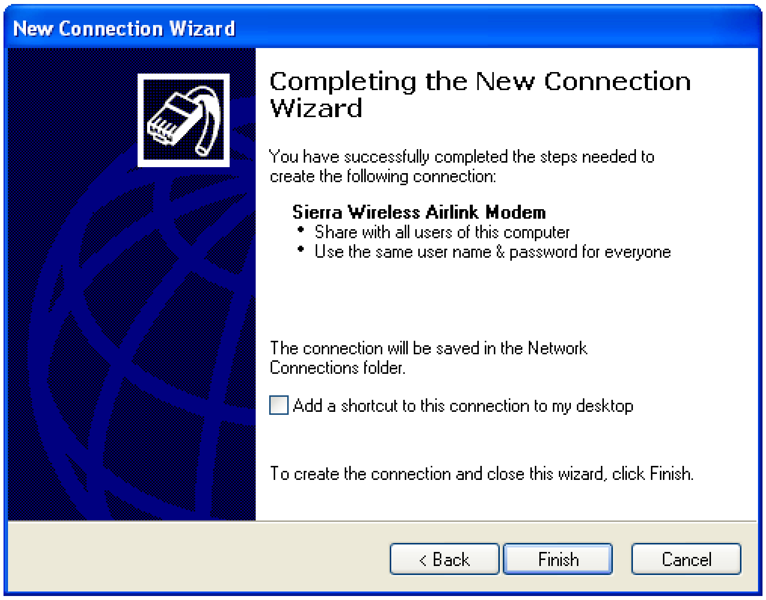
□ Make this the default Internet connection

Figure B-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.



New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

Sierra Wireless Airlink Modem
- Share with all users of this computer
- Use the same user name & password for everyone

The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

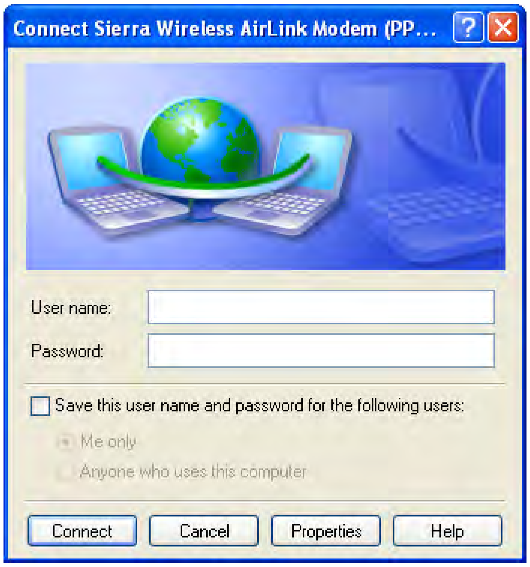
To create the connection and close this wizard, click Finish.

Figure B-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*.



Connect Sierra Wireless AirLink Modem (PP...

User name:

Password:

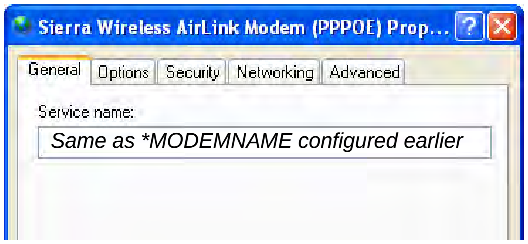
□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Figure B-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.

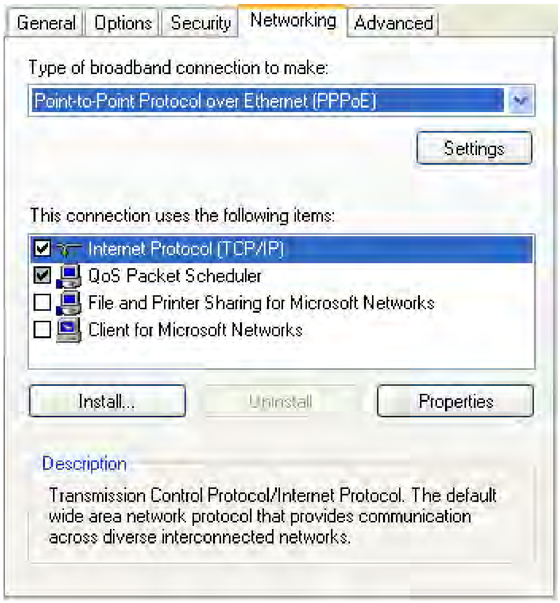


Service name: *Same as *MODEMNAME configured earlier*

Figure B-11: PPPoE Connection: Service Name

c. Select *Networking*.

d. Select *Settings*.



Type of broadband connection to make: Point-to-Point Protocol over Ethernet (PPPoE)

This connection uses the following items:

☑ Internet Protocol (TCP/IP)
☑ QoS Packet Scheduler
☐ File and Printer Sharing for Microsoft Networks
☐ Client for Microsoft Networks

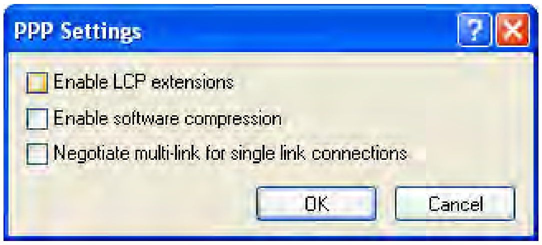
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure B-12: PPPoE: Networking

e. Remove the checks from all three PPP settings.

f. Select *OK*.



☐ Enable LCP extensions
☐ Enable software compression
☐ Negotiate multi-link for single link connections

Figure B-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.

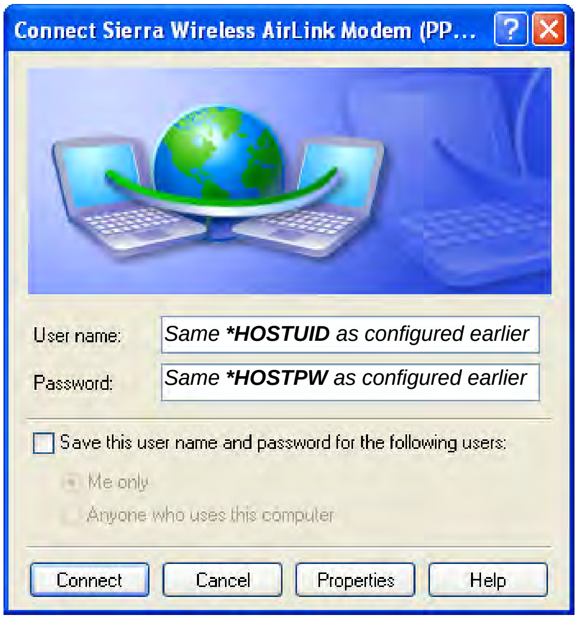
Connecting to the Internet with PPPoE

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.



User name: *Same ***HOSTUID** as configured earlier*

Password: *Same ***HOSTPW** as configured earlier*

□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Figure B-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.

C: SNMP : Simple Network Management Protocol

Management Information Base (MIB)

The ALEOS 4.2 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.

The MIB complies with:

- RFC 1213 and MIB-II
- RFC 2863 - The Interfaces Group MIB
- RFC 2665 - Ethernet-Like Interface Types

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 traps when the network connection becomes available.

SNMP MIB Definition Sample

```
SIERRA-MIB DEFINITIONS ::= BEGIN

IMPORTS
  OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY,
  Integer32, Opaque, enterprises, Counter32, Unsigned32
    FROM SNMPv2-SMI

  TEXTUAL-CONVENTION, DisplayString, TruthValue
FROM SNMPv2-TC;

sierrawireless MODULE-IDENTITY
  LAST-UPDATED "201008190000Z"
  ORGANIZATION "Sierra Wireless Inc"
  CONTACT-INFO
"Sierra Wirelss Inc
```

```
     "

   DESCRIPTION
"This file defines the private Sierra MIB extensions."

   ::= { enterprises 20542 }

sharks OBJECT IDENTIFIER ::= { sierrawireless  9}

-- MIB versions

mibversion1 OBJECT IDENTIFIER ::= { sharks  1}

--  GUI Tabs for Sharks

statustab OBJECT IDENTIFIER ::= { mibversion1  1}
cellulartab OBJECT IDENTIFIER ::= { mibversion1  2}
lantab OBJECT IDENTIFIER ::= { mibversion1  3}
vpntab OBJECT IDENTIFIER ::= { mibversion1 4}
securitytab OBJECT IDENTIFIER ::= { mibversion1  5}
servicestab OBJECT IDENTIFIER ::= { mibversion1  6}
gpstab OBJECT IDENTIFIER ::= { mibversion1  7}
eventsreportingtab OBJECT IDENTIFIER ::= { mibversion1  8}
serialtab OBJECT IDENTIFIER ::= { mibversion1  9}
IOtab OBJECT IDENTIFIER ::= { mibversion1  10}
admintab OBJECT IDENTIFIER ::= { mibversion1  11}
snmpconfig OBJECT IDENTIFIER ::= { mibversion1  12}

--  status elements

home   OBJECT IDENTIFIER ::= { statustab  1}
cellular OBJECT IDENTIFIER ::= { statustab  2}
lan  OBJECT IDENTIFIER ::= { statustab  3}
vpn     OBJECT IDENTIFIER ::= { statustab  4}
security     OBJECT IDENTIFIER ::= { statustab  5}
services     OBJECT IDENTIFIER ::= { statustab  6}
gps     OBJECT IDENTIFIER ::= { statustab  7}
serial     OBJECT IDENTIFIER ::= { statustab  8}
about     OBJECT IDENTIFIER ::= { statustab  9}


--  home status elements

phoneNumber OBJECT-TYPE
SYNTAX DisplayString (SIZE (10))
MAX-ACCESS read-only
STATUS current
::= { home 17 }

ipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
```

```
STATUS current
::= { home 301 }

networkState OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 259 }

RSSI OBJECT-TYPE
SYNTAX INTEGER(-125..-50)
MAX-ACCESS read-only
STATUS current
::= { home 261 }

gprsnetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 770 }

cdmanetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 644 }

gprsECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 772 }

cdmaECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 643 }

powerIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 266 }

boardTemprature OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { home 267 }

networkServiceType OBJECT-TYPE
```

```
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 264}

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

netChannel OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { home 260 }

cellularBytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { home 283 }

cellularBytesRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { home 284 }


deviceName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { home 1154 }

--  cellular status elements

ipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
::= { cellular 301 }

electronicID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { cellular 10 }

IMSI OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-only
STATUS current
::= { cellular 785 }

keepAliveIpAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
::= { cellular 1105 }

keepAlivePingTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 1104 }

DNSServer1 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { cellular 1082 }

DNSServer2 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { cellular 1083 }

wanUseTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 5046 }

errorRate OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 263 }

bytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 283 }

bytesRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 284 }
```

```
packetsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 281 }

packetsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 282 }

prlVersion OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 642 }

prlUpdateStatus OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { cellular 646 }

SID OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 648 }

NID OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { cellular 649 }

pnOffset OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { cellular 650 }

baseClass OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { cellular 651 }

--  LAN status elements

usbMode OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-only
STATUS current
::= { lan 1130 }


vrrpEnabled OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { lan 9001 }

lanpacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { lan 279 }

lanpacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { lan 280 }

--  VPN status elements


incomingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3177 }

outgoingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3178 }

outgoingHostOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3179 }


vpn1Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3176 }

vpn2Status OBJECT-TYPE
```

```
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3205 }

vpn3Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3231 }

vpn4Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3257 }

vpn5Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { vpn 3283 }

--  Security status elements

DMZ OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { security 5113 }

portForwarding OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { security 5112 }

portFilteringIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { security 3505 }

portFilteringOut OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { security 3506 }

trustedHosts OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
```

```
STATUS current
::= { security 1062 }

macFiltering OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { security 3509 }

badPasswdCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { security 385 }

ipRejectCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { security 386 }

ipRejectLog OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { security 387 }

--  Services status elements

aceNet OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { services 5026 }

aceManager OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { services 1149 }

dynamicDnsService OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { services 5011 }

fullDomainName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { services 5007 }
```

```
-- GPS status elements

gpsFix OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { gps 900 }

satelliteCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { gps 901 }

latitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { gps 902 }

longitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { gps 903 }

heading OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { gps 904 }

speed OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { gps 905 }

engineHours OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { gps 906 }

-- Serial status elements

serialPortMode OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { serial 1043 }
```

```
tcpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { serial 1048 }

udpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { serial 1054 }

serialPacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { serial 273 }

serialPacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
::= { serial 274 }

-- About status elements

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


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

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

deviceID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { about 25 }
```

```
macAddress OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
::= { about 66 }

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

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

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

-- Read Write values

snmpenable OBJECT-TYPE
SYNTAX INTEGER {
        disabled(0),
        enabled(1)}
MAX-ACCESS read-write
STATUS current
::= { snmpconfig 10040 }

snmpversion OBJECT-TYPE
SYNTAX INTEGER {
        snmpv2c(2),
        snmpv3(3)}
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10041 }

snmpport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10042 }

snmpContact OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
```

```
::= { snmpconfig  2730 }

snmpName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  2731 }

snmpLocation OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  2732 }

rocommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10063 }

rouser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10045 }

rosecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
        noauthnopriv(0),
        authnopriv(1),
        authpriv(2)}
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10046 }

roauthtype OBJECT-TYPE
SYNTAX INTEGER {
        MD5(0),
        SHA(1) }
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10047 }

roauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10048 }

roprivtype OBJECT-TYPE
SYNTAX INTEGER {
        AES(0),
        DES(1) }
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10049 }

roprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10050 }


rwcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10064 }

rwuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10051 }

rwsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
        noauthnopriv(0),
        authnopriv(1),
        authpriv(2)}
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10052 }

rwauthtype OBJECT-TYPE
SYNTAX INTEGER {
        MD5(0),
        SHA(1) }
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10053 }

rwauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10054 }


rwprivtype OBJECT-TYPE
SYNTAX INTEGER {
        AES(0),
        DES(1) }
```

```
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10055 }

rwprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10056 }


trapipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
::= { snmpconfig 1166 }

trapport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10043 }

engineid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10044 }

trapcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10065 }

trapuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10057 }

trapsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
        noauthnopriv(0),
        authnopriv(1),
        authpriv(2)}
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10058 }

trapauthtype OBJECT-TYPE
SYNTAX INTEGER {
        MD5(0),
        SHA(1) }
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10059 }

trapauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10060 }


trapprivtype OBJECT-TYPE
SYNTAX INTEGER {
        AES(0),
        DES(1) }
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10061 }

trapprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  10062 }


rebootmodem OBJECT-TYPE
SYNTAX INTEGER {
        nop(0),
        reboot(1) }
MAX-ACCESS read-write
STATUS current
::= { snmpconfig  65001 }






--  Notifications starting at 1000

modemNotifications OBJECT IDENTIFIER ::= { mibversion1  1000 }


Value OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION
      "value of MSCIID that triggered this event"
```

```
::= { modemNotifications 500 }

DigitalInput1 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Digital Input 1 MSCIID 851"
::= { modemNotifications 1 }


DigitalInput2 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Digital Input 1 MSCIID 852"
::= { modemNotifications 2 }

DigitalInput3 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Digital Input 1 MSCIID 853"
::= { modemNotifications 3 }

DigitalInput4 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Digital Input 1 MSCIID 854"
::= { modemNotifications 4 }

PulseAccumulator1 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 1 MSCIID 4002"
::= { modemNotifications 5 }


PulseAccumulator2 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 2 MSCIID 4003"
::= { modemNotifications 6 }

PulseAccumulator3 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 3 MSCIID 4004"
::= { modemNotifications 7 }
```

```
PulseAccumulator4 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 1 MSCIID 4005"
::= { modemNotifications 8 }

AnalogInput1 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 1 MSCIID 855"
::= { modemNotifications 9 }


AnalogInput2 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 2 MSCIID 856"
::= { modemNotifications 10 }

AnalogInput3 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 3 MSCIID 857"
::= { modemNotifications 11 }

AnalogInput4 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 4 MSCIID 858"
::= { modemNotifications 12 }

ScaledAnalogInput1 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 1 MSCIID 4041"
::= { modemNotifications 13 }


ScaledAnalogInput2 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 2 MSCIID 4042"
::= { modemNotifications 14 }
```

```
ScaledAnalogInput3 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog Input 3 MSCIID 4043"
::= { modemNotifications 15 }

ScaledAnalogInput4 NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog Input 4 MSCIID 4044"
::= { modemNotifications 16 }

GPSFix NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "GPS Fix MSCIID 900"
::= { modemNotifications 17 }

VehicleSpeed NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Vehicle Speed MSCIID 905"
::= { modemNotifications 18 }

EngineHours NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Engine Hours MSCIID 906"
::= { modemNotifications 19 }

HeadingChange NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Heading Change MSCIID 904"
::= { modemNotifications 20 }

RSSI NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "RSSI MSCIID 261"
::= { modemNotifications 21 }

NetworkState NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Network State MSCIID 259"
::= { modemNotifications 22 }

NetworkService NOTIFICATION-TYPE
   OBJECTS     { Value }
   STATUS     current
   DESCRIPTION
      "Network Service 264"
::= { modemNotifications 23 }

NetworkErrorRate NOTIFICATION-TYPE
   OBJECTS     { Value }
   STATUS     current
   DESCRIPTION
      "Network Error Rate MSCIID 263"
::= { modemNotifications 24 }

PeriodicReports NOTIFICATION-TYPE
   OBJECTS     { Value }
   STATUS     current
   DESCRIPTION
      "Periodic Reports MSCIID 270"
::= { modemNotifications 25 }

PowerIn NOTIFICATION-TYPE
   OBJECTS     { Value }
   STATUS     current
   DESCRIPTION
      "Power In  MSCIID 266"
::= { modemNotifications 26 }

BoardTemp NOTIFICATION-TYPE
   OBJECTS     { Value }
   STATUS     current
   DESCRIPTION
      "Board Temperature MSCIID 267"
::= { modemNotifications 27 }

CDMATemp NOTIFICATION-TYPE
   OBJECTS     { Value }
   STATUS     current
   DESCRIPTION
      "CDMA Temperature MSCIID 641"
::= { modemNotifications 28 }


dailyDataUsage NOTIFICATION-TYPE
   OBJECTS     { Value }
   STATUS     current
   DESCRIPTION
      "Daily Data Usage MSCIID 25001"
```

```
::= { modemNotifications 29 }

monthlyDataUsage NOTIFICATION-TYPE
   OBJECTS    { Value }
   STATUS     current
   DESCRIPTION
      "Monthly Data Usage MSCIID 25002"
::= { modemNotifications 30 }

END
```

D : 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

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

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 Configuring 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.

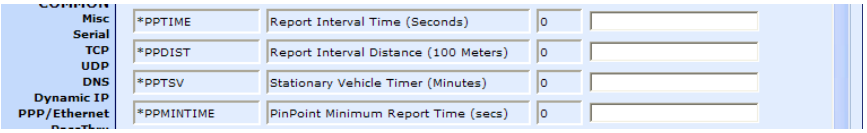
When the AirLink device is first powered on (or reset), it will send a Set Window message to sync up with the server for the current “window”.

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).



*PPTIME	Report Interval Time (Seconds)	0	
*PPDIST	Report Interval Distance (100 Meters)	0	
*PPTSV	Stationary Vehicle Timer (Minutes)	0	
*PPMINTIME	PinPoint Minimum Report Time (secs)	0	

*Figure D-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.

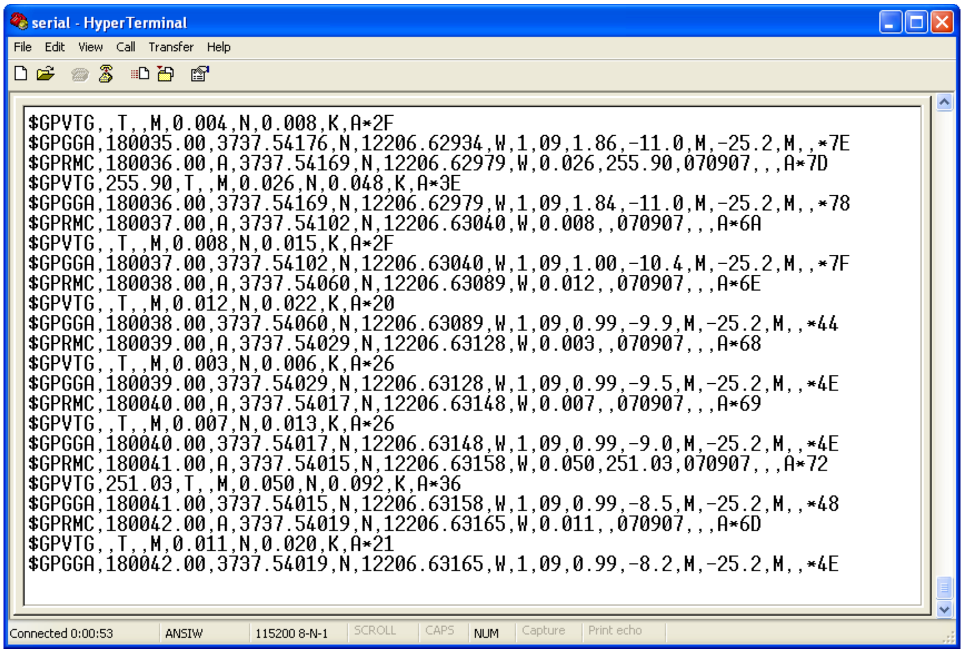
- **E0** - NMEA GGA and VTG sentences.
- **E1** - NMEA GGA, RMC, and VTG sentences.

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).



```
$GPVTG,,T,,M,0.004,N,0.008,K,A*2F
$GPGGA,180035.00,3737.54176,N,12206.62934,W,1,09,1.86,-11.0,M,-25.2,M,,*7E
$GPRMC,180036.00,A,3737.54169,N,12206.62979,W,0.026,255.90,070907,,,A*7D
$GPVTG,255.90,T,,M,0.026,N,0.048,K,A*3E
$GPGGA,180036.00,3737.54169,N,12206.62979,W,1,09,1.84,-11.0,M,-25.2,M,,*78
$GPRMC,180037.00,A,3737.54102,N,12206.63040,W,0.008,,070907,,,A*6A
$GPVTG,,T,,M,0.008,N,0.015,K,A*2F
$GPGGA,180037.00,3737.54102,N,12206.63040,W,1,09,1.00,-10.4,M,-25.2,M,,*7F
$GPRMC,180038.00,A,3737.54060,N,12206.63089,W,0.012,,070907,,,A*6E
$GPVTG,,T,,M,0.012,N,0.022,K,A*20
$GPGGA,180038.00,3737.54060,N,12206.63089,W,1,09,0.99,-9.9,M,-25.2,M,,*44
$GPRMC,180039.00,A,3737.54029,N,12206.63128,W,0.003,,070907,,,A*68
$GPVTG,,T,,M,0.003,N,0.006,K,A*26
$GPGGA,180039.00,3737.54029,N,12206.63128,W,1,09,0.99,-9.5,M,-25.2,M,,*4E
$GPRMC,180040.00,A,3737.54017,N,12206.63148,W,0.007,,070907,,,A*69
$GPVTG,,T,,M,0.007,N,0.013,K,A*26
$GPGGA,180040.00,3737.54017,N,12206.63148,W,1,09,0.99,-9.0,M,-25.2,M,,*4E
$GPRMC,180041.00,A,3737.54015,N,12206.63158,W,0.050,251.03,070907,,,A*72
$GPVTG,251.03,T,,M,0.050,N,0.092,K,A*36
$GPGGA,180041.00,3737.54015,N,12206.63158,W,1,09,0.99,-8.5,M,-25.2,M,,*48
$GPRMC,180042.00,A,3737.54019,N,12206.63165,W,0.011,,070907,,,A*6D
$GPVTG,,T,,M,0.011,N,0.020,K,A*21
$GPGGA,180042.00,3737.54019,N,12206.63165,W,1,09,0.99,-8.2,M,-25.2,M,,*4E
```

Figure D-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. 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.

- *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.

E1 - TAIP GGA, RMC, and VTG sentences.

E: AT Commands

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.

Note: Some of the configuration commands listed here are only available as AT commands and some commands require having the device in Passthru mode.

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 E-1: Info Commands

Command	Description
***ETHMAC?**	The MAC address of the Ethernet port.
***NETPHONE?**	The device's phone number, if applicable or obtainable.

Table E-1: Info Commands (Continued)

Command	Description
***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.
***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 E-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 E-2: Status: Network (Continued)

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 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 network frame for CDMA or EV-DO.
***NETSERV?**	The type of service being used by the device, e.g., Tech EV-DO Rev A.

CDMA Info

Table E-3: Status: CDMA Info

Command	Description
+PRL	Preferred Roaming List (PRL) version.
***PRLSTATUS**	The status of the most recent PRL Update. • 0 : None • 1 : In Progress • 2 : Success • Any other value: Failure.
CDMA ECIO	Indicates the signal-to-noise ratio, i.e., the quality of the signal.

CPU Status

Table E-4: 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 E-5: Common: Misc

Command	Description
General	
***DATE**	Queries the internal clock. Either the date and time can be specified, or just one of the two, in which case the unspecified value will remain unchanged. The date and time are always specifiedin a 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 is used to set the time, and any date/time specified by this command will be ignored.*

Table E-5: Common: Misc (Continued)

***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)
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.

Table E-5: Common: Misc (Continued)

***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 connection and copies to *NETUID and *NETPW.

USB

Table E-6: Common: USB

Command	Description
***USBDEVICE**	USB Device Mode This parameter alters the default startup data mode.

Serial

Table E-7: 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).

Table E-7: Common: Serial (Continued)

Command	Description

&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
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

Table E-7: Common: Serial (Continued)

Command	Description
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 E-8: 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

Table E-8: Common: TCP (Continued)

Command	Description
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 E-9: 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 E-9: Common: UDP (Continued)

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 E-10: Common: DNS

Command	Description
***DNS1**	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.
***DNS2**	

Table E-10: 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 E-11: 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 E-11: Common: Dynamic IP (Continued)

Command	Description
*IPMANAGER1	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.
*IPMANAGER2	
*IPMGRUPDATE1	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.
*IPMGRUPDATE2	
*IPMGRKEY1	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]
*IPMGRKEY2	

PPP/Ethernet

Table E-12: 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 E-12: Common: PPP/Ethernet (Continued)

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 E-13: 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 E-13: Common: PassThru (Continued)

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 E-14: 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 E-15: 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 Keep Alive. 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 Keep Alive Ping will trigger the Keep Alive Ping at the configured interval even if valid packets have been received.
***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.

Table E-15: Common: Other (Continued)

Command	Description
***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
***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 E-16: 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 the VTLG power down event happens until the device enters the low power mode. If VLTG is 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.*
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 E-17: 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.
FO (F1, F2, ... F9)	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.

Logging

This group includes commands specific to the internal log.

Table E-18: 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
***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 E-19: 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 1.61 kilometers. • n=0 : Disabled • n=1-65535
***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.*

Table E-19: GPS: Server 1 (Continued)

Command	Description
***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
***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.

Table E-19: GPS: Server 1 (Continued)

Command	Description
***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 E-20: 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
***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

Table E-20: GPS: Misc (Continued)

Command	Description
***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 E-21: 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 E-21: GPS: Serial Port (Continued)

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.*
*PGPSF	Persistent GPS frequency • n= number of seconds per report Max Value: 65535 up to 18 hours

CDMA

This group includes commands specific to 1x and EV-DO.

Table E-22: 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.*

Table E-22: CDMA (Continued)

Command	Description
~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.*
***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

I/O includes configuration commands for the digital inputs and relay outputs. Some 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 E-23: 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**	
***RELAYOUT1**	Set or query the relay outputs. • n=1-2 Input number • s=OPEN or CLOSED
***RELAYOUT2**	

SMS

Table E-24: 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 access 2 - Will disable the ALEOS Ports for OTA and Local Access 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