

ZyWAN

Cellular Routing Modem

Rev F – April 2010 – 110150-1001F

Trademarks

All trademarks both marked and not marked appearing in this document are the property of their respective owners.

Document Revision History

REVISION	DESCRIPTION	DATE
A	Initial release.	June 2007
B	Minor updates and formatting changes.	October 2007
C	Updates for ZyWAN release 1.4. Added sections on USB, clearing browser cache, Security page, and mechanical diagrams.	October 2007
D	Updates for ZyWAN release 1.5. Added Open Ports and optional fields to Networking, HTTPS option, support for 3G and Novatel modems, and rules for default gateway/DHCP/DNS. Added configuration examples. Updated RS-485 wiring detail.	February 2008
E (rev 2.0)	Updates for ZyWAN release 1.7 and style changes. Added Modem Status pages, DNS option for Cellular, and masquerade option for port forwarding. Added sections on setting up PuTTY and WinSCP, updating ZyWAN firmware manually, and backing up and restoring configurations. Changed 'cingular' to 'att'.	June 2009
F	Minor updates and formatting changes.	April 2010

Table of Contents

Trademarks.....	2
Document Revision History	2
Table of Contents	3
Important User Information	6
Safety Notices and Warnings	6
<i>Alerts that can be found throughout this manual.....</i>	6
<i>Product Handling and Environmental Guidelines.....</i>	6
Warranty	7
WEEE	7
RoHS	7
Technical Assistance	8
Conventions.....	8
Introduction	9
Product Overview	9
<i>Features.....</i>	9
<i>ZyWAN Model Numbers</i>	10
<i>Accessories.....</i>	10
Operating Characteristics	11
<i>Electrical Characteristics.....</i>	11
<i>Temperature Range.....</i>	11
PART 1: GETTING STARTED.....	13
Chapter 1 Interfaces	14
LED Indicators	15
Power Connector	16
Ethernet	16
Antenna Connections	17
Serial Ports	18
<i>COM1, COM2, COM3 (RS-232)</i>	18
<i>COM3 (4-wire RS-485/422)</i>	18
<i>USB</i>	19
SIM Card.....	20
<i>Installing a SIM card (GPRS / 3G / IDEN).....</i>	20
Battery Link.....	21
Understanding Network Interfaces	21
Chapter 2 Accessing the ZyWAN.....	22
What You Will Need.....	22
<i>Hardware Requirements</i>	22
<i>Software Requirements</i>	22
<i>Network Requirements</i>	22
<i>Optional Equipment</i>	23
<i>Additional Documentation</i>	23
Serial Connection to COM1	24
<i>RS-232 Null Modem Cable</i>	24
Setting Up Software.....	25
<i>Windows HyperTerminal.....</i>	25

SSH Client (PuTTY)	26
SFTP/SCP Client (WinSCP)	27
Initial Connection with Single PC	30
Initial Connection Over a Network	33
Troubleshooting Connection Problems	36
Unable to Load Web Page	36
Ping the ZyWAN	36
Check the PC's Network Configuration	37
Using ZyWAN COM1 for Diagnostics	37
Check with Network Administrator	38
PART 2: SOFTWARE CONFIGURATION	39
Chapter 1 Web Configuration Page	40
Web Page Login	40
Switching Between HTTP and HTTPS	42
Clearing the Browser Cache	43
Changing a Configuration	44
Using Default Gateway, DHCP, and DNS	45
Configuration Options	45
Default Route	46
DHCP Server and NAT	46
DNS Server	46
Chapter 2 System Status	47
Status Web Page	47
Get Modem Status	48
EVDO Status	48
3G Status	51
IDEN Status	54
GPRS Status	57
Chapter 3 Cellular Configuration	61
ZyWAN-EVDO Options	61
ZyWAN-3G Options	70
ZyWAN-IDEN Options	72
ZyWAN-GPRS Options	72
Chapter 4 Ethernet configuration	74
Enable Eth0/Eth1	74
DHCP Client	74
Fixed Address	74
DHCP Server	75
Chapter 5 WiFi configuration	77
DHCP Client	78
Fixed Address	78
DHCP Server	79
Chapter 6 Networking configuration	81
Open Ports	81
Enable Port Forwarding	83
Enable NAT	84
Time Synchronization	86

Chapter 7 GPS configuration	87
Forward GPS to Physical COM Port	88
Enable GPS Terminal Server	89
GPS UDP Message Format.....	90
<i>Arcom Format for GPS Messages (UDP)</i>	92
Chapter 8 Terminal Clients	94
Host Connection Table	97
Chapter 9 Terminal Servers	100
Serial Ports Table	103
Chapter 10 Update	105
Updating Via the Web Interface.....	105
Updating Using WinSCP.....	106
<i>Starting with versions 1.2 through 1.4</i>	106
<i>Starting with version 1.5</i>	108
Chapter 11 Security	110
Chapter 12 Backing Up Configurations.....	112
Saving Configuration Files	112
Restoring Configuration Files	112
PART 3: CONFIGURATION EXAMPLES	113
Introduction	114
Configuration Example 1: Network Router	115
Cellular Setup	115
Ethernet Setup	116
WiFi Setup	117
Networking Setup	118
Checking Out Example 1	119
Configuration Example 2: WiFi Client	120
WiFi Setup	120
Configuration Example 3: Terminal Server.....	121
Terminal Server Setup.....	122
Networking Setup	122
Configuration Example 4: GPS interface	123
Cellular Setup	123
GPS Setup	123
Networking Setup	124
Appendix	125
A.1. Mechanical Specifications	125
A.2. Electromagnetic Compatibility (EMC)	127
Eurotech Worldwide Presence	129

Important User Information

In order to lower the risk of personal injury, electric shock, fire, or equipment damage, users must observe the following precautions as well as good technical judgment, whenever this product is installed or used.

All reasonable efforts have been made to ensure the accuracy of this document; however, Eurotech assumes no liability resulting from any error/omission in this document or from the use of the information contained herein. Eurotech reserves the right to revise this document and to change its contents at any time without obligation to notify any person of such revision or changes.

Safety Notices and Warnings

The following general safety precautions must be observed during all phases of operation, service, and repair of this equipment. Failure to comply with these precautions or with specific warnings elsewhere in this manual violates safety standards of design, manufacture, and intended use of the equipment. Eurotech assumes no liability for the customer's failure to comply with these requirements.

The safety precautions listed below represent warnings of certain dangers of which Eurotech is aware. You, as the user of the product, should follow these warnings and all other safety precautions necessary for the safe operation of the equipment in your operating environment.

Alerts that can be found throughout this manual

The following alerts are used within this manual and indicate potentially dangerous situations.

Warning:

Information regarding potential hazards:



- Personal injury or death could occur. Also damage to the system, connected peripheral devices, or software could occur if the warnings are not carefully followed.
 - Appropriate safety precautions should always be used. These should meet the requirements set out for the environment that the equipment will be deployed in.
-



Information and/or Notes:

Indicates important features or instructions that should be observed

Product Handling and Environmental Guidelines

Warnings:

Electric current from power and communication cables is hazardous. To avoid shock hazard when connecting or disconnecting cables, follow appropriate safety precautions. Ensure that the correct operating voltage is used when powering the device.



Do not open the equipment to perform any adjustments, measurements, or maintenance until all power supplies have been disconnected.

The ZyWAN is equipped with a certain level of protection against power surges. However, to ensure maximum protection or when using in areas susceptible to electrical disturbances and lightning, use of an external surge suppressor is strongly recommended.

Antistatic Precautions

To avoid damage caused by ESD (Electro Static Discharge), always use appropriate antistatic precautions when handling any electronic equipment.

Batteries

The ZyWAN contains a coin-type, replaceable Lithium battery to maintain its real-time clock when input power is removed. The ZyWAN is normally shipped with the battery jumper connected. If the unit will be sitting unused for lengthy periods of time, it is recommended to remove the jumper to extend the life of the battery. See [Battery Link](#) on page 21 for more details.



Warning:

To avoid possible injury:

- Do not short circuit the batteries or place in water or on a metal surface where the battery terminals could be shorted. Do not incinerate or heat to more than 100 °C (212 °F). Do not crush or otherwise disassemble the battery or attempt to repair the battery.
 - Do not recharge. The batteries are non-rechargeable. There is a danger of explosion if a lithium battery is recharged or incorrectly replaced.
 - Dispose of used batteries according to the manufacturer's instructions and local ordinances.
-

Warranty

This product is supplied with a limited warranty. The product warranty covers failure of any Eurotech manufactured product caused by manufacturing defects. Eurotech will make all reasonable effort to repair the product or replace it with an equivalent alternative. Eurotech reserves the right to replace the returned product with an alternative variant or an equivalent fit, form, and functional product. Delivery charges will apply to all returned products.

WEEE

The following information is issued in compliance with the regulations as set out in the 2002/96/CE directive, subsequently superseded by 2003/108/CE. It refers electrical and electronic equipment and the waste management of such products.

When disposing of a device, including all of its components, subassemblies, and materials that are an integral part of the product, you should consider the WEEE directive.

This symbol has been attached to the equipment or, if this has not been possible, on the packaging, instruction literature and/or the guarantee sheet. By using this symbol, it states that the device has been marketed after August 13, 2005 and implies that you must separate all of its components when possible and dispose of them in accordance with local waste disposal legislations.



- Because of the substances present in the equipment, improper use or disposal of the refuse can cause damage to human health and to the environment.
- With reference to WEEE, it is compulsory not to dispose of the equipment with normal urban refuse, and arrangements should be instigated for separate collection and disposal.
- Contact your local waste collection body for more detailed recycling information.
- In case of illicit disposal, sanctions will be levied on transgressors.

RoHS

This device, including all its components, subassemblies, and the consumable materials that are an integral part of the product, has been manufactured in compliance with the European directive 2002/95/EC known as the RoHS directive (Restrictions on the use of certain Hazardous Substances). This directive targets the reduction of certain hazardous substances previously used in electrical and electronic equipment (EEE).

Technical Assistance

If you have any technical questions, cannot isolate a problem with your device, or have any enquiry about repair and returns policies, contact your local Eurotech Technical Support Team.

See [Eurotech Group Worldwide presence](#), page 129 for full contact details.

Before returning any Eurotech supplied product, for any reason whatsoever, you must first send an e-mail to the Technical Support Team. You will receive an RMA number (Returned Material Authorization) for the return of the material.

Provide the following information in the RMA request:

- Model number
- Serial number
- Detailed fault description
- Company Details
- Contact details



Pack the product in anti-static material and ship it in a sturdy cardboard box with enough packing material to adequately protect the shipment.

Any product returned to Eurotech improperly packed will immediately void the warranty for that particular product!

Conventions

The following conventions are used throughout this manual.

Symbol / Text	Pin Definition
NC	Not Connected
Reserved	Use reserved to Eurotech, must remain unconnected

Text in `Courier font` is used to indicate commands entered or responses received at a command prompt in either the Windows or Linux operating system.

Introduction

The ZyWAN is a cellular routing modem for GSM/GPRS, EvDO/1xRTT CDMA, iDEN and 3G networks. It is ideally suited for wireless applications such as Internet access, AVL, telemetry, SCADA, mobile computing, and AMR. The ZyWAN operates as a fully configurable embedded Linux router enabling firewall, DHCP, DNS and NAT. ZyWAN provides real-time network access to any Ethernet, 802.11 or serial device for mobile and fixed data applications.

A GPS adapter provides a sophisticated tracking program and raw NMEA data strings for mapping applications. The tracking program reports the device location, speed and heading on regular intervals and caches data when out of network. To easily manage the ZyWAN configuration, a Web page presents a simple tool to quickly change settings locally or over-the-air.

This User Manual provides the basic configuration and hardware information required for getting started with the ZyWAN products. For more detailed information, see www.zywan.com for additional technical and addendum documentation.

Product Overview

Features

The features offered by the ZyWAN include:

- Rugged design – handles challenging industrial or mobile telemetry environments.
- Wireless features – provides cellular, WiFi (802.11) and GPS communication.
- Ethernet – two 10/100 base-T ports provide independent wired network ports.
- Networking – takes full advantage of IP networking technologies.
- Firewall – provides data encryption and authentication.
- Security – secure routing of IP data between the cellular network, Ethernet, and 802.11 WLAN.
- Wireless router – can act as gateway for local wired or wireless LAN to access the Internet.
- Serial communication – field equipment can connect via RS-232, RS-422/485, or LAN ports.
- Localization – GPS receiver allows applications or local devices to pinpoint exact location.
- VPN – IPSec security and PPTP VPN capabilities are available.

ZyWAN Model Numbers

The standard model numbers for the ZyWAN are determined by the hardware options which are part of the product. The list of features and model number variations are explained next.

ZyWAN	-	CCCC	####	-	Options
--------------	---	-------------	-------------	---	----------------

where,

CCCC identifies the cellular network.

GPRS = GPRS/GSM network (AT&T, T-Mobile, O2, Orange, etc.)

3G = 3G network (AT&T, T-Mobile, O2, Orange, etc.)

IDEN = IDEN network (Nextel)

EVDO = EVDO/CDMA network (Sprint)

(omitted) = base model, with no cellular option

identifies the main model variation.

1000 = Base model with COM3 as RS-232

1001 = Base model with COM3 as RS-485

Options identifies additional optional components.

-WiFi = WiFi (802.11) wireless network

-GPS = GPS receiver

In addition, project-specific model names are given to ZyWAN models, which include specific hardware or software to meet customer project requirements.

Accessories

Several accessories for the ZyWAN are listed next.

ZW-AC-PSU	ZyWAN AC Power Supply and Power Cord
ZW-Null-Modem	RS232 Null Modem Cable
ZW-RJ45-Xover	Crossover RJ45 Ethernet cable
ZW-Pwr cable	ZyWAN Power Cable -10ft (Included w/ base unit)
ZW-CD	ZyWAN CD (Manual, App notes)
ZW-Starter Kit	ZyWAN Starter KIT (CD, Null modem, Xover, AC PSU)

Operating Characteristics

Electrical Characteristics

General

FEATURE	DESCRIPTION
Processor/clock:	520MHz PXA270 processor
Dimensions:	238.5mm (9.4") x 141mm (5.6") x 65mm (2.6")
Weight:	1.25 kg (2.75 lbs)
Mounting:	Panel mount aluminium enclosure
Memory:	64Mbytes SDRAM and 32Mbytes Flash
Serial ports:	(2) RS-232 and (1) optional RS-232 or RS-422/485
LAN:	(2) RJ45 10/100baseT
USB	(2) USB 1.1 ports (one or both used internally on some models)
Wireless WAN:	GSM, IDEN, or EVDO cellular data network, and 802.11b option, depending on product model
GPS	Fastrax iTrax 03 GPS receiver

Power

FEATURE	DESCRIPTION
Input power:	+10 to +26 VDC
Overvoltage/reverse voltage protection:	100 VDC
Ignition sense input:	12 VDC protected
Power consumption:	2 W (excluding 802.11b, cellular and other peripheral devices)
	5 W (approximate, including 802.11b and cellular)
	Power consumption for communication devices varies depending on the amount of transmission time. Typical values for maximum power consumption are listed (assuming full transmit power over a sustained period). Realistically, the total power consumption is much less because the module does not transmit continuously.
	GSM (GR64) cellular module: 7.5 W (max)
	IDEN (iO270) cellular module: 4.8 W (max)
	GPRS (MC5725) cellular module: 6.6 W (max)
	802.11b: 2 W (max)

Temperature Range

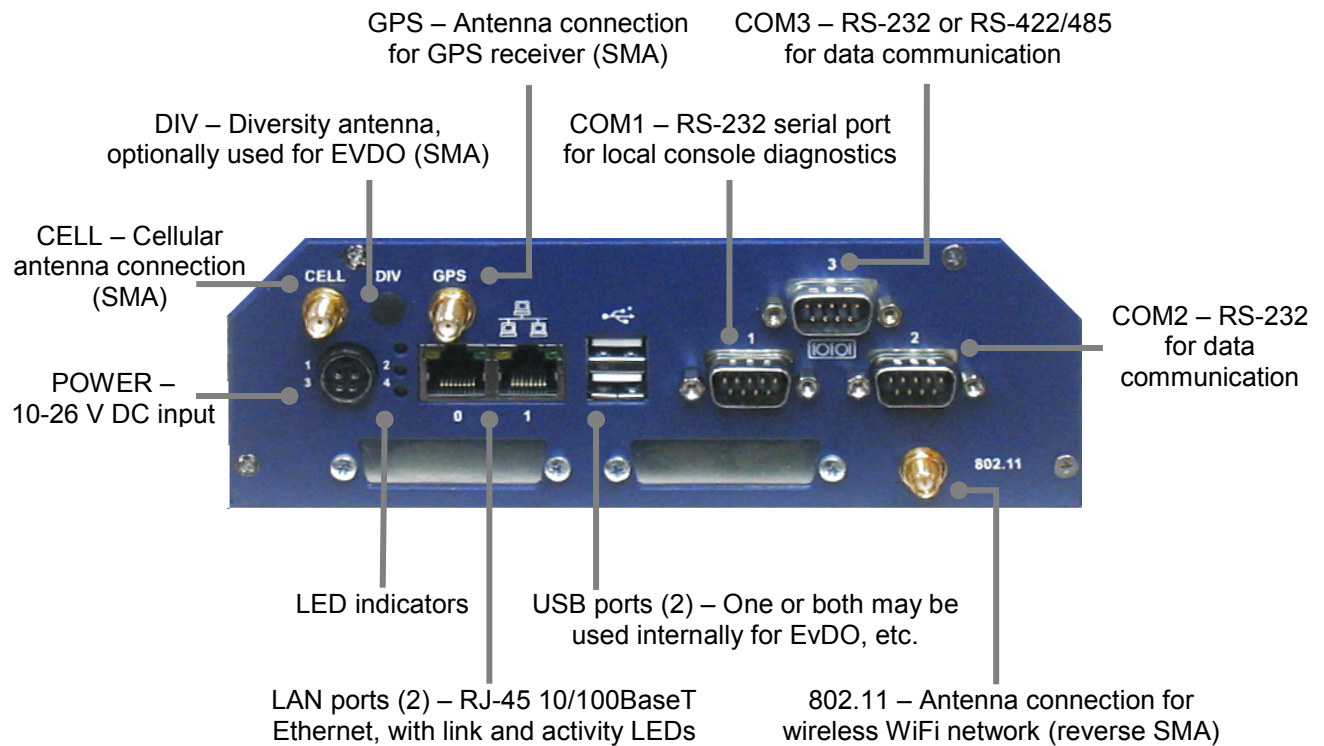
FEATURE	DESCRIPTION
Temperature:	
Operating:	-20 to +65 C Note: Certain models of cellular modems or WiFi cards may have a lower operating temperature range. Contact your local Eurotech representative for more details.
Storage:	-40 to +85 C
Humidity:	10% to 90% relative humidity (non-condensing)

(This page intentionally blank)

PART 1: GETTING STARTED

Chapter 1 Interfaces

The front panel of the ZyWAN contains the following ports and indicators:



Further information about these ports and connectors is provided in the following sections.

LED Indicators

The ZyWAN has three LED lights which indicate the following:

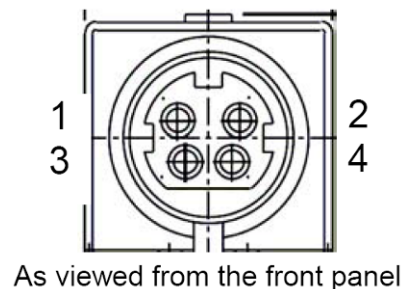
POSITION	INDICATES	DISPLAY EXPLANATION
Top	Power and GPS	Off = ZyWAN is not powered.
		On = On during startup of ZyWAN.
		Slow blink = ZyWAN is running, but there is no GPS lock. (Slow blink is approximately one blink every 2 seconds.)
		Fast blink = ZyWAN running, and GPS position lock obtained.
Middle	Cellular Connection Status	Off = Cellular interface not started (ppp0 not present).
		On = Cellular interface started, and network communication ability probable. (This does not necessarily guarantee that communication can occur. For instance, when the interface is established but the device goes out of range of cellular coverage, the light may still indicate a solid On condition.)
		Slow blink = Received data activity detected on cellular network.
Bottom	WiFi Connection Status	Off = WiFi interface not started (wlan0 not present).
		On = WiFi interface started, and network communication ability probable. (This does not necessarily guarantee that communication can occur. For instance, when the interface is established but the device goes out of range of WiFi coverage, the light may still indicate a solid On condition.)
		Slow blink = Received data activity detected on WiFi network.

Power Connector

The ZyWAN can be powered from 10 to 26 VDC. Power to the ZyWAN is supplied via the 4-pin power socket (mating connector: Kycon KPPX-4P plug). The power plug must be inserted with the flat part of the plug facing up (toward the top of the ZyWAN front panel). The pin configuration is as follows:

PIN	SIGNAL NAME
1	+ Power
2	Ignition sense
3	- Power (GND)
4	GND

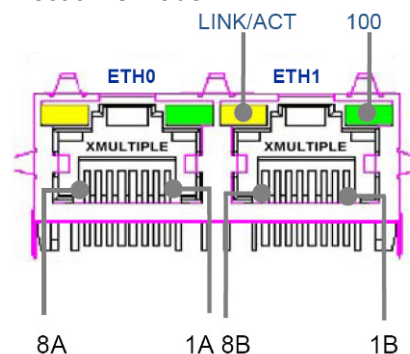
The ignition sense input is intended for sensing the on/off condition of a vehicle's ignition, but it is not yet supported in the ZyWAN application software.



Ethernet

The pin assignments for the Ethernet LAN connection are shown in the following table. The yellow LED is a Link/Activity light, which illuminates when a 10/100Base-T connection is made and flashes when there is data activity. The green LED illuminates when a 100 MB/s connection is made.

PIN	SIGNAL NAME
1	Transmit +
2	Transmit -
3	Receive +
4	Reserved
5	Reserved
6	Receive -
7	Reserved
8	Reserved



Antenna Connections

The “CELL” connector on the front of the ZyWAN is typically a standard polarity SMA (female) connector. The cellular antenna to be connected here must be rated for operation within one or more of the ranges required by the ZyWAN model/cellular type, as given in the following table.

CELLULAR TYPE	FREQUENCIES
EVDO	US Cellular (824-894 MHz) North America PCS (1850-1990 MHz)
3G	GSM 850 (824-894 MHz) EGSM 900 (880-960 MHz) GSM 1800 (1710-1880 MHz) GSM 1900 (1850-1990 MHz)
IDEN	IDEN 800 (806-870 MHz) IDEN 900 (896-941 MHz)
GPRS	GSM 850 (824-894 MHz) EGSM 900 (880-960 MHz) GSM 1800 (1710-1880 MHz) GSM 1900 (1850-1990 MHz)

The “DIV” connector is a standard polarity SMA connector used for a diversity antenna. This is an option used with EVDO models to enhance signal reception, and it uses the same EVDO frequencies.

The “GPS” connector is a standard polarity SMA connector, which connects to a GPS antenna with a typical frequency of 1575.42 MHz (L1). Typically, GPS antennas must have line of sight to a wide area of the sky in order to receive signals from multiple positioning satellites.

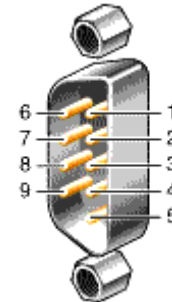
The “802.11” connector is a reverse polarity SMA (male) connector. It connects to a WiFi antenna, with a typical range of 2.4-2.485 GHz.

Serial Ports

The following tables show pin assignments for the serial ports.

COM1, COM2, COM3 (RS-232)

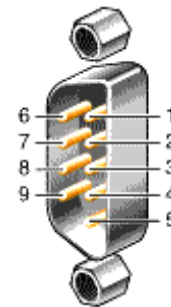
PIN	SIGNAL NAME
1	Data Carrier Detect (DCD)
2	Receive Data (RX)
3	Transmit Data (TX) *
4	Data Terminal Ready (DTR) *
5	Ground
6	Data Set Ready (DSR)
7	Request To Send (RTS) *
8	Clear To Send (CTS)
9	Ring Indicator (RI)



* = output signals

COM3 (4-wire RS-485/422)

PIN	SIGNAL NAME
1	NC
2	NC
3	RS-485/422 TX-
4	RS-485/422 RX-
5	GND
6	NC
7	RS-485/422 TX+
8	RS-485/422 RX+
9	GND



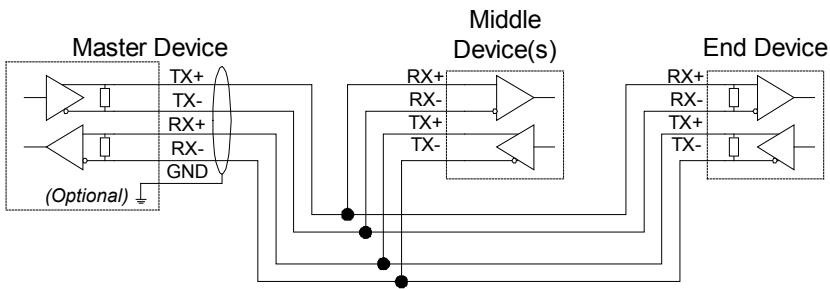
RS-485 / RS-422 wiring diagrams

When connecting RS-485 or RS-422 devices in a multidrop configuration, there must usually be a 120Ω termination resistor at one or both end devices in the network but NOT on any devices in the middle of the loop. The ZyWAN provides a 4-wire RS-485/422 interface.

In RS-485 or RS-422 systems, the ground connection is optional. Typically, it is used to connect the cable shield for a shielded, twisted pair cable. In the ZyWAN, the RS-485/422 ground is common with the RS-232 grounds, but it is isolated from the metal case. In order to avoid ground loops, connect the cable shield to the RS-485/422 GND AT ONLY ONE POINT in the network.

The following wiring diagrams show the correct device connection arrangements.

4-wire RS-485/422 Device Connections

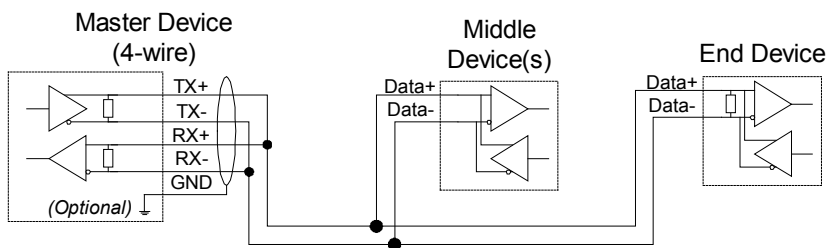


End device (and RS-485 Master) may need 120 ohm termination resistor, optional middle device(s) must not have resistor.

Drawing is labeled as if devices are DTE. Direction of arrows is correct, regardless of RX/TX labeling on a given device.

Drg. S15037-02b

4-wire to 2-wire RS-485/422 Device Connections



End device (and RS-485 Master) may need 120 ohm termination resistor, optional middle device(s) must not have resistor.

Drawing is labeled as if devices are DTE. Direction of arrows is correct, regardless of RX/TX labeling on a given device.

Drg. S15037-02c

USB

One or both of the USB ports may be used internally for EvDO or WiFi. EvDO uses the top USB port internally, and it is unavailable externally. An older WiFi option used the bottom USB port internally, but the WiFi option now uses an internal PCMCIA card. If the ZyWAN includes either of these hardware options, the external USB socket will be plugged to indicate the port is in use, and it must not be used for external equipment.

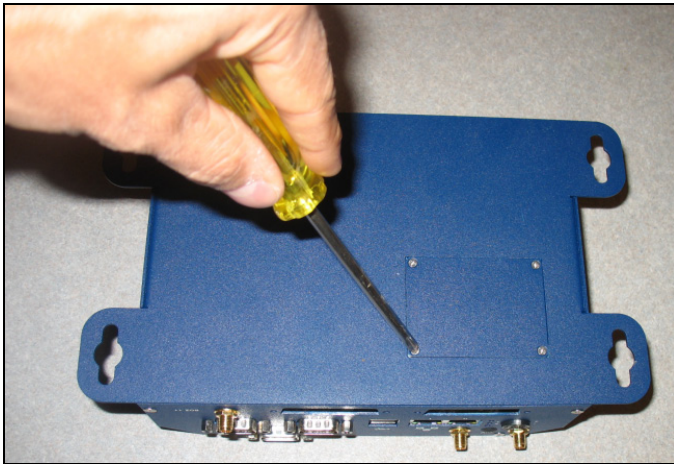
SIM Card

The ZyWAN for a GPRS, 3G, or IDEN network requires a SIM card from the network provider in order to operate on the cellular data network. The SIM card is accessible through an access panel on the bottom of the ZyWAN.

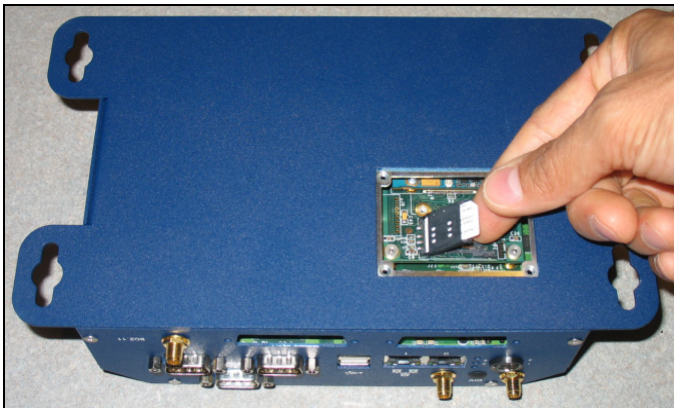
Installing a SIM card (GPRS / 3G / IDEN)

To change or install the SIM card, complete the following steps:

1. Remove the power connector, and then remove other connectors from the ZyWAN.
2. Unscrew the four screws and remove the access panel on the bottom.



3. Slide the black SIM card holder, and remove the existing SIM card.



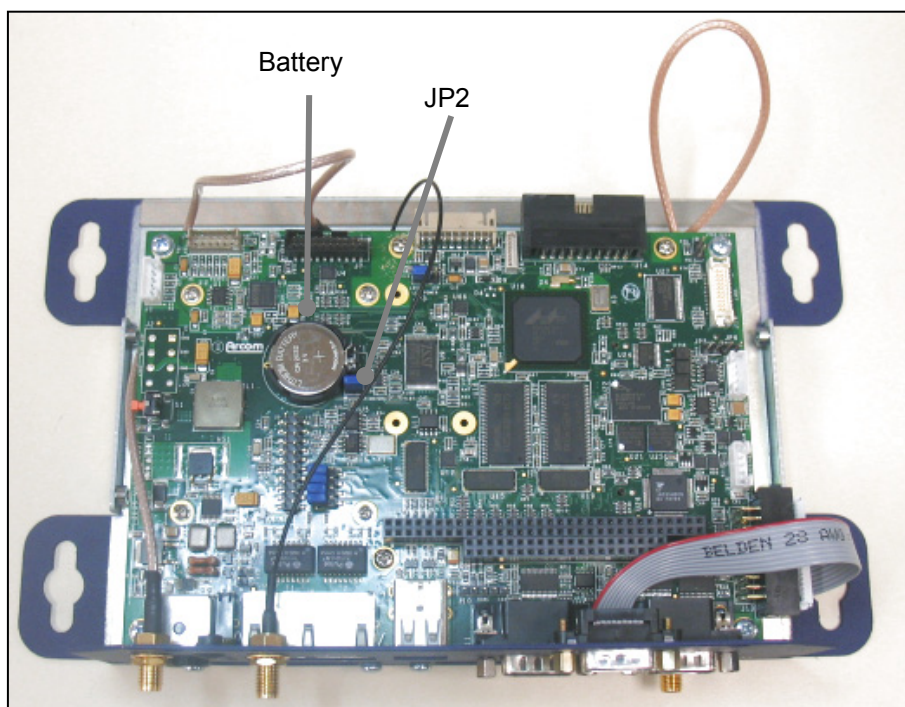
4. Install the new SIM card and replace the access panel.
5. Restore all connectors reconnecting the power cable last.

Battery Link

The ZyWAN contains a coin-type replaceable Lithium battery (CR2032, 3V) to maintain its real-time clock when input power is removed. A user jumper on the main circuit board enables this battery. The ZyWAN is normally shipped with the battery jumper connected. If the unit will be sitting unused for lengthy periods of time (months or years), it is recommended to remove the jumper to extend the life of the battery. When the device is running in a normally powered state or when it will be off for short periods of time, there is no need to remove the jumper.

To change the setting of the battery jumper or to replace the battery, remove power and all connectors from the ZyWAN and remove it from its installed location. Ensure that anti-static precautions are taken when handling the device. Remove the four screws on the front plate and the two screws from either side of the enclosure lid. In some cases, it may also be necessary to remove the four screws from the back plate.

Remove the lid and locate the battery and battery jumper (JP2). The battery is enabled when the jumper is fitted. To replace the battery, remove it from its holder and replace it with an equivalent (CR2032) battery. Dispose of the used battery according to the manufacturer's instructions and local ordinances.



Carefully replace the lid, ensuring that all internal cables remain in place. Replace mounting screws and external cabling to their correct locations.

Understanding Network Interfaces

The ZyWAN contains at least four possible IP network connections or 'interfaces'. These interfaces are mentioned throughout this manual and on the ZyWAN configuration page. The ZyWAN system assigns each interface a name. The last character of each interface name is a number, 0 (zero) or 1, as listed in the following table. When these interface names are used in the Web configuration page, they must be entered exactly as written (case sensitive).

NAME	INTERFACE DESCRIPTION
eth0	Ethernet port 0
eth1	Ethernet port 1
ppp0	Cellular network (for all cellular technologies and providers)
wlan0	802.11 WiFi network

Chapter 2 Accessing the ZyWAN

This section describes several ways to gain access to the ZyWAN for diagnostic and system maintenance purposes and some utility software that may be useful for troubleshooting.

What You Will Need

Hardware Requirements

The ZyWAN must be connected to a stand-alone computer and/or a network, so that the initial configuration may be loaded via the Web configuration page.

In order to perform the initial configuration via a stand-alone computer, you need the following hardware:

- ZyWAN unit
- Power supply
- Computer with 10base-T Ethernet network port and Web browser
- Ethernet crossover cable

In order to perform the initial configuration via an existing network, you need the following hardware:

- ZyWAN unit
- Power supply
- Network equipment and cables to connect ZyWAN
- Computer with network connection, RS-232 serial port, and Web browser
- Serial crossover cable (or some other means of identifying the DHCP-assigned address of the ZyWAN after it powers on)

Software Requirements

The computer used to perform the ZyWAN configuration must have the following software:

- Windows operating system (Windows 2000 or Windows XP)
- Web browser: Mozilla Firefox ver. 2 (recommended), or Internet Explorer ver. 6 or ver. 7
- Serial terminal program, such as Windows HyperTerminal

Other operating systems or Web browsers may be used, but they may not work as described in this document.

Network Requirements

The network used to perform the ZyWAN configuration must have the following requirements:

- Either a direct connection (via Ethernet crossover) or existing network LAN connection from the computer to the ZyWAN for the initial setup
- Network configuration of wired LAN, wireless 802.11 WAN, and/or cellular networks depending on the network used after initial configuration
- Knowledge of the final networking address requirements in order to configure the ZyWAN
- If using cellular services, a registered cellular data account for this ZyWAN

Optional Equipment

Several optional components may be used with the ZyWAN, including GPS Receiver and the Wireless LAN 802.11b card. These modules are plugged into internal sockets of the ZyWAN. Cellular and 802.11 antennas must conform to the requirements on page 127 in order to ensure compliance with FCC regulations.

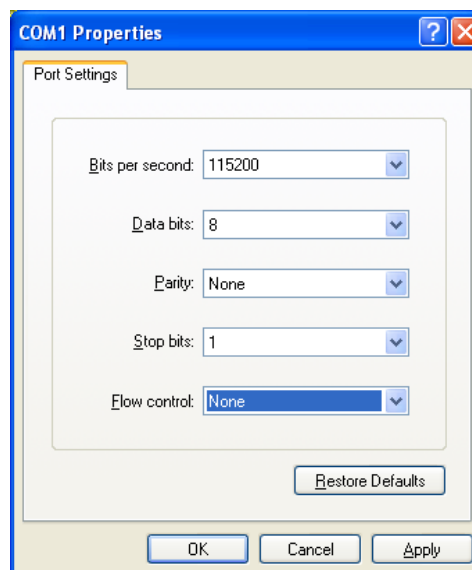
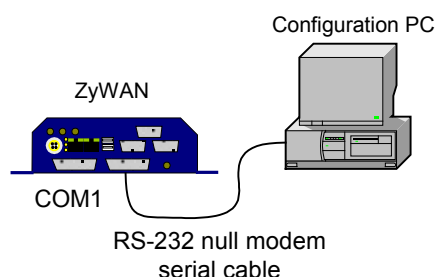
Additional Documentation

In addition to this manual, there are several Application Notes giving further documentation on specific subjects relating to the ZyWAN configuration. These can be found on the ZyWAN software CD or upon request. These Application Notes include:

- ZyWAN Application Note – Modem Diagnostics
- ZyWAN Application Note – Security and System Diagnostics
- ZyWAN Application Note – IPSec Security and PPTP VPN

Serial Connection to COM1

The COM1 port of the ZyWAN is used for a serial console. Typically, this allows a local administrative ('root') login to the ZyWAN using a null modem serial cable. The next section describes the settings for Windows HyperTerminal. The settings for this connection are 115,200 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

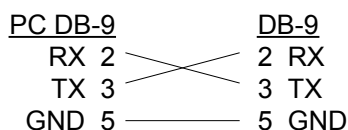


Press the **Enter** key to get a login prompt. The default login is `root` and the default password is `arcom` (case-sensitive).

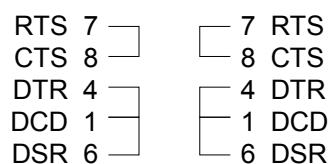
RS-232 Null Modem Cable

To connect the ZyWAN to another computer (DTE) device, such as on COM1 for the console diagnostic port, a null modem serial cable must be used. The pinout for this cable is shown next.

RS-232 Null Modem Cable



optional (loopbacks required if hardware handshaking enabled)



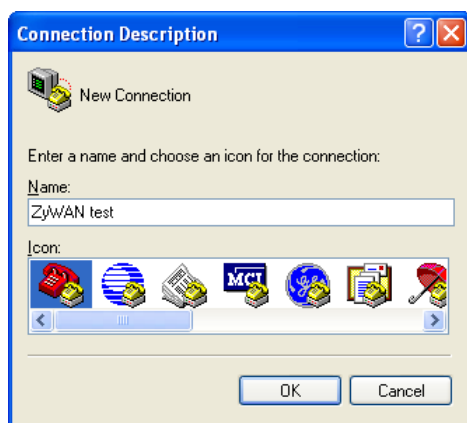
Drg. S15037-03b

Setting Up Software

Windows HyperTerminal

Windows provides a serial terminal program, HyperTerminal, for serial communications. This can be used to access the console port of the ZyWAN for diagnostics. The following steps are the setup instructions for Windows HyperTerminal.

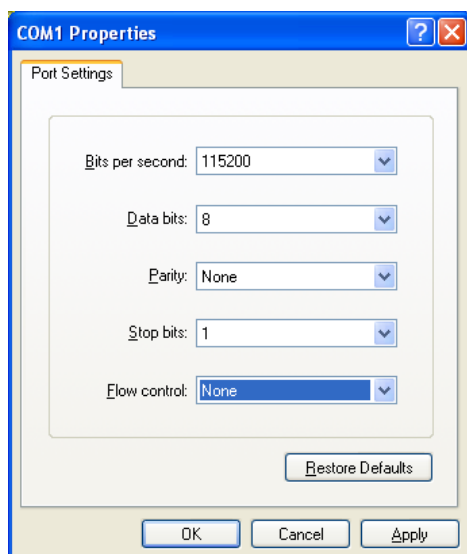
1. In the Windows *Start* menu, select *Programs>Accessories>Communications>HyperTerminal*. The *Connection Description* window is displayed.
2. Enter a name for this HyperTerminal configuration, as shown next.



3. Set the *Connect using* option to *COM1* or whatever free RS-232 port exists on this PC.



- Make the following settings for the serial communication, then click the **OK** button.



- If the ZyWAN is already started, press the **Enter** key to get a login prompt. The default login is `root` and the default password is `arcom` (case-sensitive).

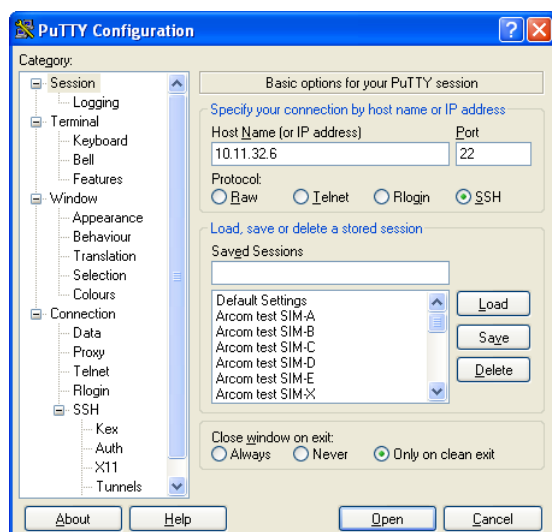
SSH Client (PuTTY)

The ZyWAN allows remote console logins using Secure Shell (SSH), which requires SSH client software. Unencrypted Telnet to the ZyWAN is not an option.

For Linux systems, the 'ssh' command is available as an SSH client.

For Windows systems, the PuTTY program is available as a free SSH client. Download and install PuTTY (choose the Windows installer version) from <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

Once the PuTTY application is installed on the Windows computer, run the application and enter the IP address of the ZyWAN. Set the protocol to "SSH" and the port to 22 (unless the port has been changed on the ZyWAN from its factory default). Click the **Open** button to connect.



The first time a connection is made with PuTTY, a security warning is given as PuTTY tries to authenticate with the ZyWAN. Click **Yes** to continue, as long as you are sure that this is the correct ZyWAN device. Then log in with the correct username and password. The default administrative login is `root` and the default password is `arcom` (case-sensitive).

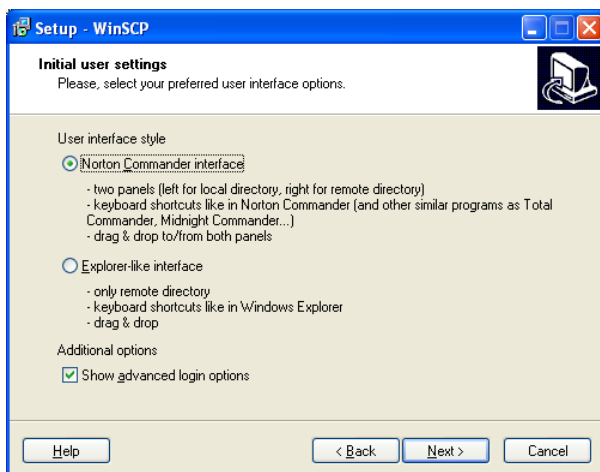


SFTP/SCP Client (WinSCP)

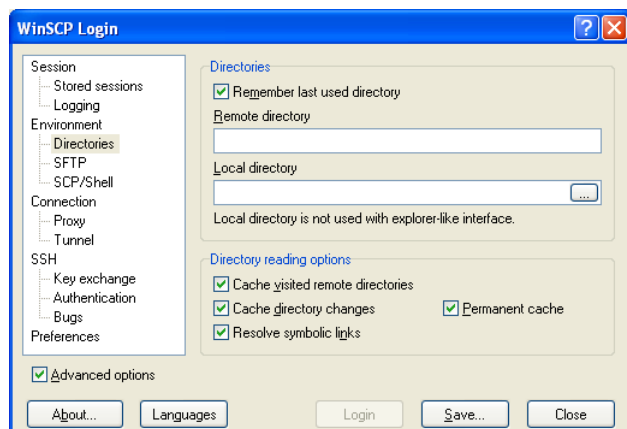
There may be occasions when you must upload or download files to/from the ZyWAN. Unencrypted FTP is not an option. This requires the SFTP or SCP (Secure FTP or Secure Copy) protocol, which use an encrypted SSH network connection.

For Linux systems, the 'sftp' and 'scp' commands are available for file transfers to the ZyWAN.

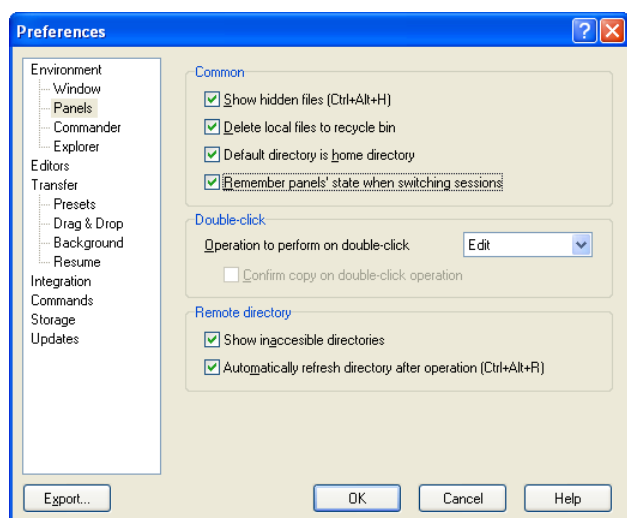
For Windows systems, the WinSCP application is available as a free download for SFTP/SCP file transfers. This is available from www.winscp.net. Download and install the latest version of WinSCP from this site. One option presented during installation is the user interface style. Either style can be used, but it is recommended to choose the Norton Commander interface that allows display of both the local and remote directories.



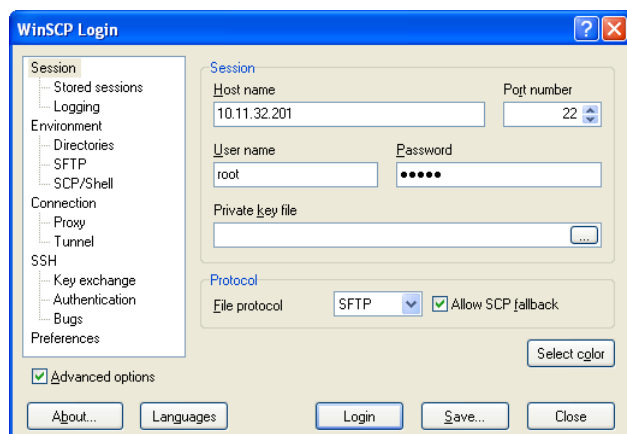
Run WinSCP after installing it. It may be useful to set the option “Remember last used directory” under the *Environment>Directories* menu.



Also, click on the *Preferences* option, and the *Preferences* button. It may be useful to set the “Remember panels’ state when switching sessions” option in the *Environment>Panels* menu.

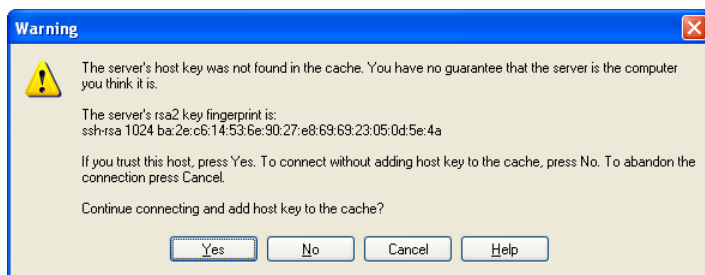


In the main window of WinSCP, click on the *Session* menu. In the “Host name” field, enter the IP address of the ZyWAN. The username and password can also be entered at this time. Individual session configurations may be saved, if repeated connections need to be made to the same address. These will appear in the *Stored sessions* menu of the WinSCP menu.



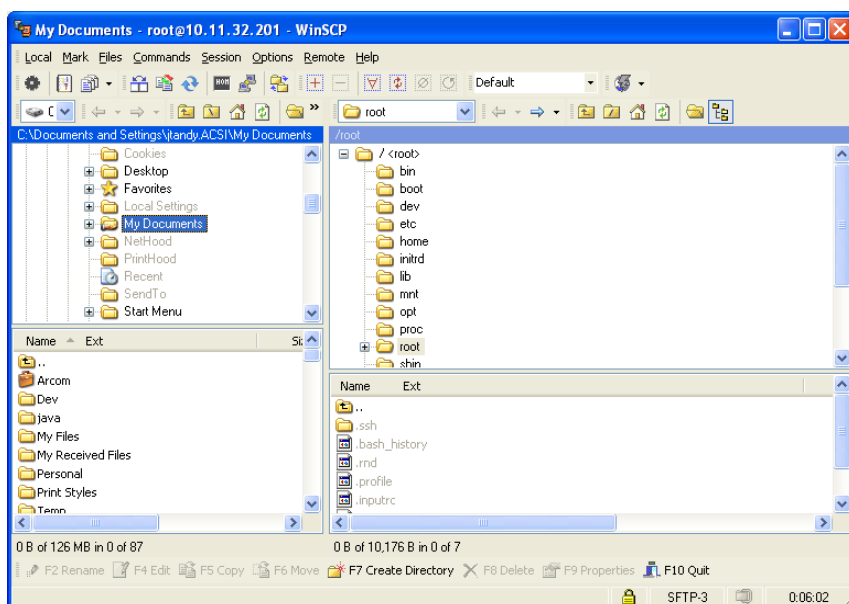
Click **Login** to connect.

The first time a connection is made with WinSCP, a security warning is given as WinSCP tries to authenticate with the ZyWAN. Click **Yes** to continue.



Once connected, WinSCP shows the local directories and files in the left panes. The right panes show the directories and files on the ZyWAN (using WinSCP's Norton Commander interface only). If all four panes are not visible, they can be displayed by choosing the *Options>Local Panel>Tree* and *Options>Remote Panel>Tree* menu options.

You can drag and drop files between the panes or other Windows Explorer windows. Navigate through the local or remote directory structures in the upper panes, as needed.



Initial Connection with Single PC

The ZyWAN typically comes factory loaded with default settings, which need to be configured for the network on which it will ultimately be used. The instructions in the following two sections describe how to set up the hardware and software necessary to perform this initial configuration.



Note:

Ethernet port '0' is used in this section, which typically comes with standard settings of address 192.168.1.1, subnet mask 255.255.255.0, and operating as a DHCP server. In some cases, the ZyWAN may come factory loaded with different settings. The instructions given here may or may not apply, depending on the customer configuration.

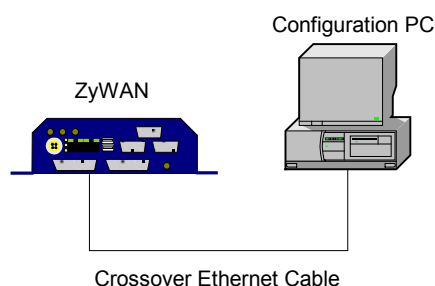
The simplest way to start the ZyWAN and perform an initial configuration is to use a direct connection to another computer (PC). To make a direct connection, complete the following steps:

1. Connect the configuration PC using a crossover Ethernet cable.
2. Apply power to the ZyWAN.
3. Set up the PC's network settings.
4. Configure the ZyWAN via its Web page.

The following sections provide detailed explanations of these actions.

1. Connect the Configuration PC

Connect a crossover Ethernet cable from the network port labeled '0' on the ZyWAN to an Ethernet port on the PC as shown in the following diagram.



The crossover Ethernet cable may be purchased from Eurotech, or it may be obtained from a network equipment supplier.

2. Apply Power

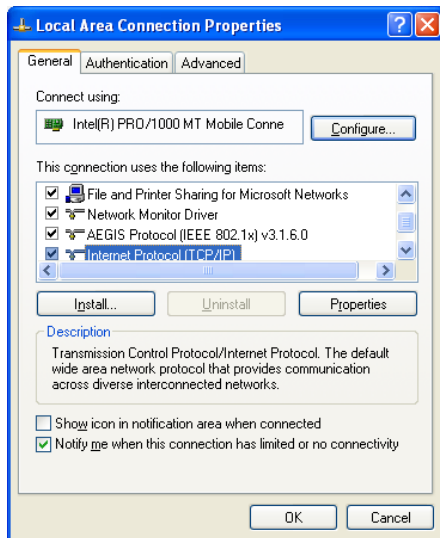
Connect the power supply to a wall outlet and to the 4-position power connector on the ZyWAN. See [Power Connector](#) on page 16 for the power input socket pin configuration details.

3. Set Up the Network

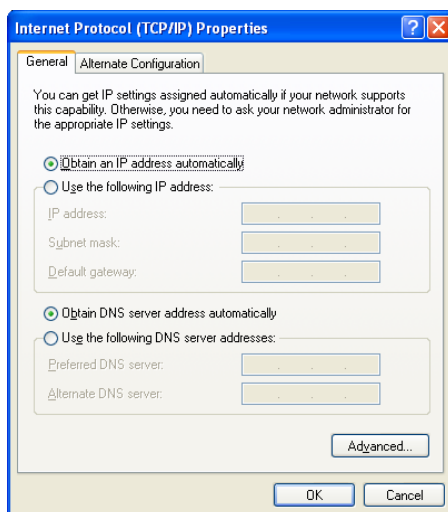
The PC must be set up to obtain its network address from the ZyWAN for this test. After initial configuration of the ZyWAN, the PC can be changed back to its normal network settings.

To configure the network as mentioned previously, complete the following steps:

1. In the Windows *Start* menu, select *Control Panel>Network Connections*. Look at the properties of the *Local Area Connection*.



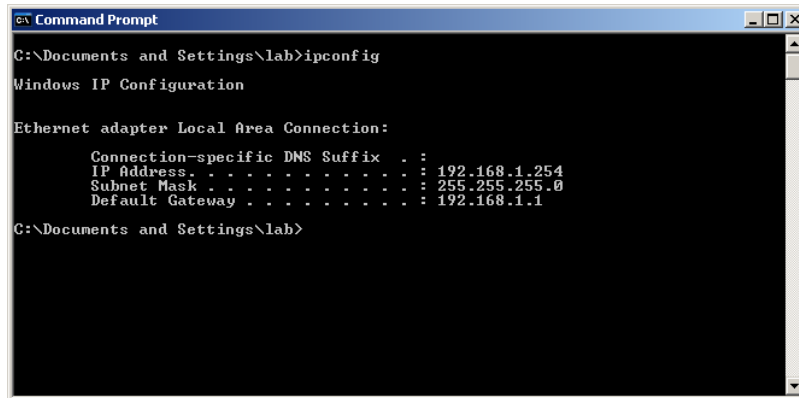
2. Open the properties for the *Internet Protocol (TCP/IP)*. Select the *Obtain an IP address automatically* and *Obtain DNS Server address automatically* checkboxes as shown in the following screen capture.



3. Record the existing settings, then make the changes to obtain the IP address and DNS server automatically.
4. Click **OK** to close the *Local Area Connection* properties, and reboot the PC if prompted to do so.

The PC automatically obtains its address from the ZyWAN. To check the address, complete the following steps:

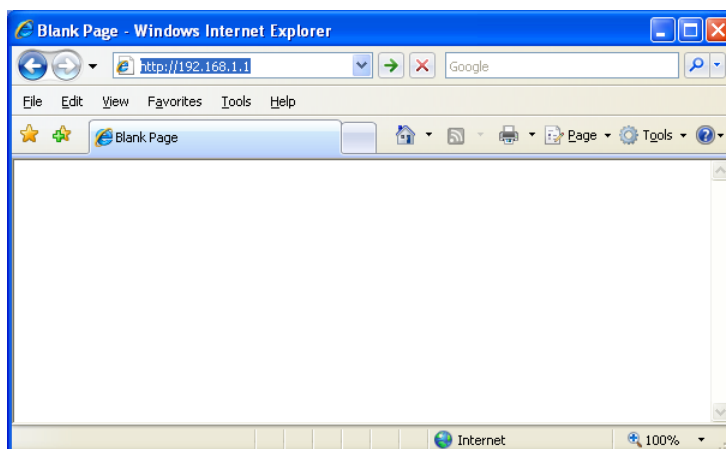
1. In the Windows *Start* menu, select *Accessories>Command Prompt*. The *Command Prompt* window is displayed.
2. Enter the command `ipconfig`. Under *Local Area Connection*, the address is 192.168.1.x, where x is a number between 2 and 254.



4. Browse ZyWAN Configuration Page

To browse the ZyWAN configuration page, complete the following steps:

1. Open a Web browser and enter the address `http://192.168.1.1` into the address bar.



A dialog box is displayed asking for the username and password.

2. Enter your username and password. The default username is `arcom` and default password is `arcom`. The ZyWAN configuration page is displayed. See [Web Configuration Page](#) on page 40, for further instructions on configuration.

Initial Connection Over a Network

An alternate way to start the ZyWAN and to perform an initial configuration is to connect it to an existing network which also contains the configuration computer (PC).

**Note:**

Ethernet port '1' is used in this section, which typically comes configured to obtain its address automatically from a network using DHCP. In some cases, the ZyWAN may come factory loaded with different user settings. These instructions may or may not apply, depending on the customer configuration.

To connect the ZyWAN to an existing network which also contains the configuration computer, complete the following instructions:

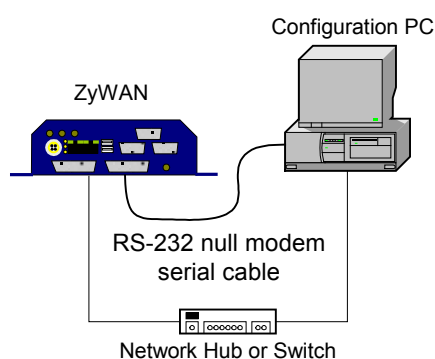
1. Connect ZyWAN to an existing Ethernet network and to the PC serial port.
2. Apply power to the ZyWAN.
3. Determine ZyWAN network address.
4. Configure the ZyWAN via its Web page.

The following sections provide detailed explanations of these actions.

1. Connect ZyWAN to the Network

To connect ZyWAN to the network, complete the following steps:

1. Connect the null modem serial cable from the PC to COM1 of the ZyWAN.
2. Connect the ZyWAN network port labeled '1' to an existing network, using a standard 10base-T Ethernet cable as shown in the following diagram.

**Note:**

The PC must exist on the same network. Consult a network administrator for assistance, if necessary.

2. Apply Power

Connect the power supply to a wall outlet and to the 4-position power connector on the ZyWAN. See [Power Connector](#) on page 16 for the power input socket pin configuration details.

3. Determine ZyWAN Network Address (DHCP)

Port 1 on the ZyWAN is typically set to acquire its address automatically using DHCP. Since the address is dynamically assigned, the ZyWAN address must be determined before it can be configured.

One way to check the ZyWAN network address is to use a crossover (null modem) serial cable between the PC and the ZyWAN. The null modem cable can be purchased from Eurotech, or it may be obtained from an electronics supply store.



Tip:

If your network administrator can determine the DHCP assigned address after the ZyWAN starts up, the serial cable is not needed. Skip to [Browse ZyWAN Configuration Page](#) on page 35.

To determine the ZyWAN network address (DHCP), complete the following steps:

1. Use Windows HyperTerminal to establish communication to the ZyWAN on COM1 at 115,200 baud. See [Windows HyperTerminal](#) on page 25, for help with this step.
2. If the ZyWAN is already started, press the **Enter** key to get a login prompt. The default login is `root` and the default password is `arcom` (case-sensitive).
3. After logging into the ZyWAN, type the command `ifconfig eth1` at the command prompt. The current network address which has been assigned to the ZyWAN by the network is displayed.

```

ZyWAN test - HyperTerminal
File Edit View Call Transfer Help

Arcom Embedded Linux v4i2a <ttyS0>
zeus login: root
Password:
root@zeus root# ifconfig eth1
eth1
Link encap:Ethernet HWaddr 00:80:66:04:2E:B3
inet addr:10.1.1.30 Bcast:10.1.255.255 Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:6828 errors:0 dropped:0 overruns:0 frame:0
TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:580487 (566.8 KiB) TX bytes:64089 (62.5 KiB)
Interrupt:145 Base address:0xe000

root@zeus root#
  
```

Note:

If the `ifconfig` command does not show an `inet addr` address, it may be that the network does not have a DHCP server or that security policies prohibit the ZyWAN from obtaining its address. An address can be manually set if necessary by issuing the following command:



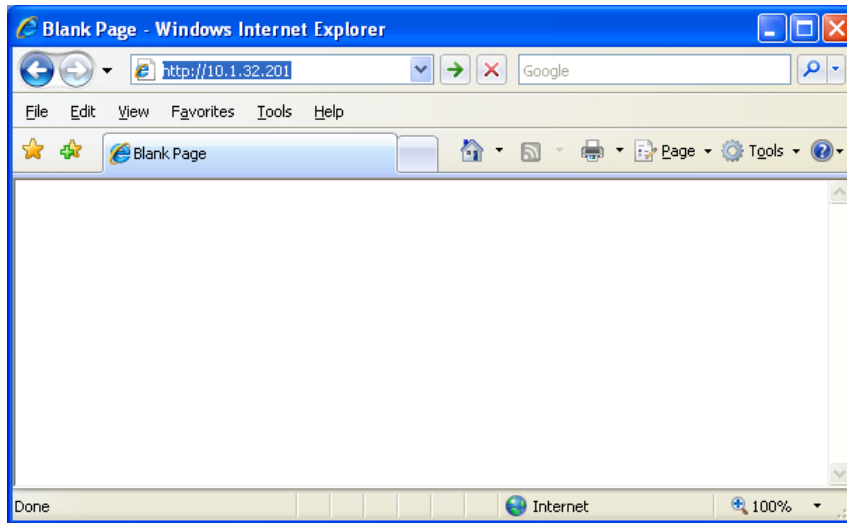
```
ifconfig eth1 ip_address netmask subnet
```

where `ip_address` is the actual address on the network, and `subnet` is the subnet mask in dotted notation (such as 255.255.0.0).

4. Browse ZyWAN Configuration Page

To browse the ZyWAN configuration page, complete the following steps:

1. Open a Web browser and enter the address of the ZyWAN into the address bar.



A dialog box is displayed asking for the username and password.

2. Enter your username and password. The default username is `arcom` and default password is `arcom`. The ZyWAN configuration page is displayed. See [Web Configuration Page](#) on page 40, for further instructions on configuration.

Troubleshooting Connection Problems

If the Web configuration page does not come up with the instructions given in the last two sections, there are several things which can be done to troubleshoot connection problems.

Unable to Load Web Page

If the Web configuration page fails to load, the following are common reasons why this might happen.

1. Due to network configuration, the computer making the connection may not be able to reach the ZyWAN. Check connection to the Web page by doing a ping command (see [Ping the ZyWAN](#), on page 36).
However, if trying to connect over the Internet and cellular connection, a ping may fail because it is blocked by the cellular network. In this case, try making an SSH connection with the PuTTY application (see [SSH Client \(PuTTY\)](#) on page 26 for help installing PuTTY), because the SSH connection should work if a connection can be made to the ZyWAN.
2. Over the Sprint network, it may be that port 80 is blocked. In the Web browser, enter the full HTTPS address of the ZyWAN (https://ip_address/cgi-bin/php/main.php), which may work instead to load the Web page.

Ping the ZyWAN

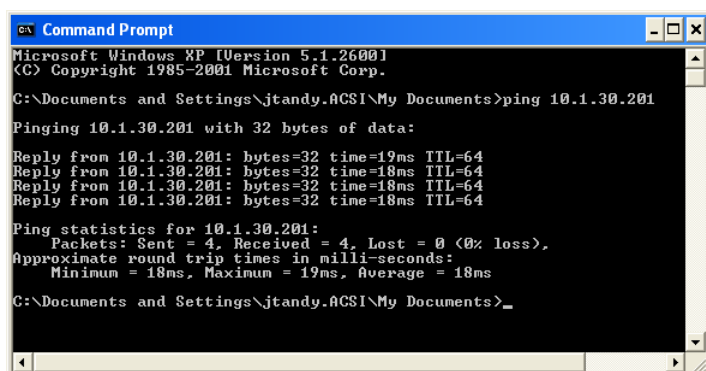
To ping the ZyWAN, complete the following steps:

1. In the Windows *Start* menu, select *Accessories>Command Prompt*. The *Command Prompt* window is displayed.
2. Type the command:

```
ping address
```

where *address* is the numeric address of the ZyWAN.

A diagnostic message is sent to the ZyWAN to check communication. If successful, the Ping response receives the following reply.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jtandy.ACSI\My Documents>ping 10.1.30.201

Pinging 10.1.30.201 with 32 bytes of data:

Reply from 10.1.30.201: bytes=32 time=19ms TTL=64
Reply from 10.1.30.201: bytes=32 time=18ms TTL=64
Reply from 10.1.30.201: bytes=32 time=18ms TTL=64
Reply from 10.1.30.201: bytes=32 time=18ms TTL=64

Ping statistics for 10.1.30.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 19ms, Average = 18ms

C:\Documents and Settings\jtandy.ACSI\My Documents>_
```

Check the PC's Network Configuration

To check the PC's network configuration, type the command `ipconfig /all` in the *Command Prompt* window. The network interface of the PC is displayed.

```

C:\Documents and Settings\jtandy.ACSI\My Documents>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : jtandywxxp
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  : 
    Description . . . . . : Intel(R) PRO/1000 MT Mobile Connection
    Physical Address. . . . . : 00-10-C6-DF-32-19
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.1.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Documents and Settings\jtandy.ACSI\My Documents>

```

If using the ZyWAN as a DHCP Server to the PC:

- Make sure the PC *Dhcp Enabled* is set to *Yes*.
- Make sure that the PC has been given a proper address from the ZyWAN, according to how it's configured.

If using the PC in a fixed address mode, check the address and make sure that it is compatible with the address and subnet necessary to communicate on the network or direct to the ZyWAN, depending on the test being performed.

If the ZyWAN is acting as a DHCP Server to the PC and is configured to serve the DNS addresses, these are displayed in the `ipconfig` settings.

Using ZyWAN COM1 for Diagnostics

When using a null modem serial cable connected to COM1, as described in [Initial Connection Over a Network](#) on page 33, several commands can be issued to the ZyWAN to diagnose network configuration or operation.

To check network configuration or availability, use the command

```
ipconfig
```

To set a temporary network address on an interface, use the command:

```
ipconfig eth1 ip_address netmask subnet
```

where *ip_address* is the actual address on the network, and *subnet* is the subnet mask in dotted notation (such as 255.255.0.0).

To send a diagnostic message to another device on a network, use the command:

```
ping address
```

where *address* is the numeric or named address of another device. Press **Ctrl-C** to stop the ping.

To check the route table of the ZyWAN, use the command:

```
route -n
```

To make a TCP/IP connection to a port on a device, use the command

```
nc ip_address ip_port
```

where *ip_address* is the device address on the network or 127.0.0.1 for the ZyWAN itself, and *ip_port* is the network port.

Check with Network Administrator

If you are still unable to get the ZyWAN to connect to an existing network, check with a network administrator for additional support.

PART 2: SOFTWARE CONFIGURATION

Chapter 1 Web Configuration Page

Web Page Login

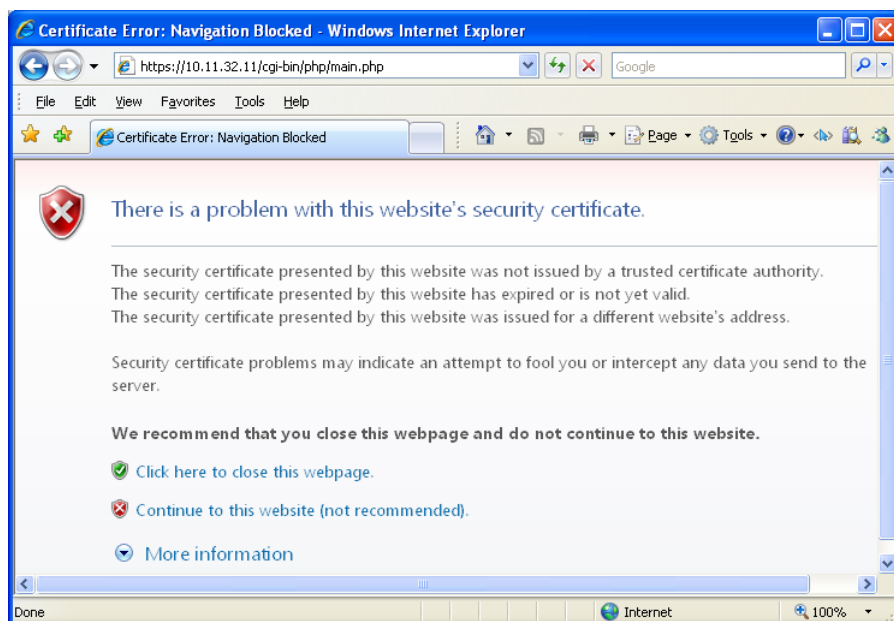
Configuration of the ZyWAN is done using a Web browser, either Mozilla Firefox or Internet Explorer. Other Web browsers have not been tested and may not be fully compatible with the ZyWAN configuration Web page. This section gives detailed explanations of each configuration parameter. Some typical configuration examples are given later in this manual (page 113).

Make sure the ZyWAN is connected to the network. To log on to a web page, complete the following steps:

1. Enter the appropriate address preceded by 'http://'. If the ZyWAN has never been configured, see [Initial Connection with Single PC](#) on page 30 or [Initial Connection Over a Network](#) on page 33. For instance, typically the default Web address on Ethernet port 0 is <http://192.168.1.1>.

If the ZyWAN has been previously configured for a different network configuration, its current numeric IP address should be used. The Web configuration page may be accessed via any available network (cellular, WiFi, Ethernet), unless Web access for that network interface has been disabled.

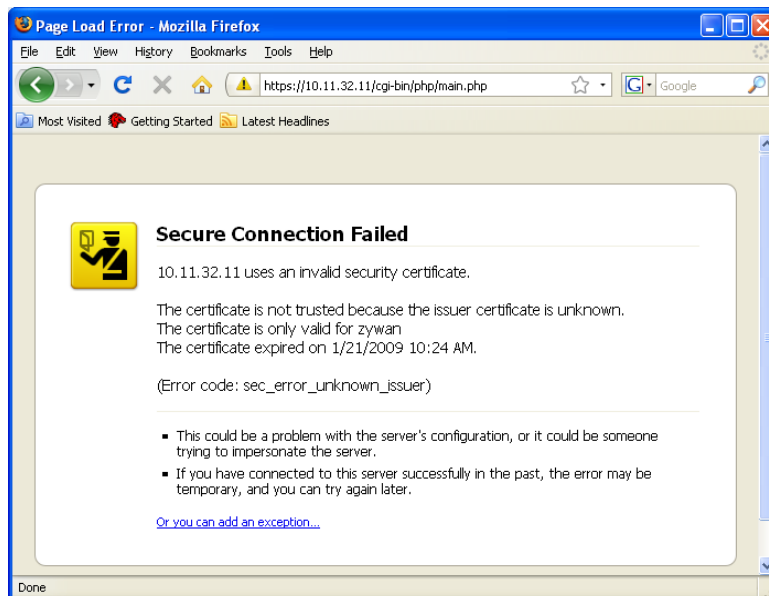
2. By default, the ZyWAN uses HTTPS for secure transfer of configuration data. The browser will display a warning about the certificate. In Internet Explorer, click on the message "Continue to this website".



In Mozilla Firefox version 2, select one of the “Accept this certificate” checkboxes, and then click **OK**.



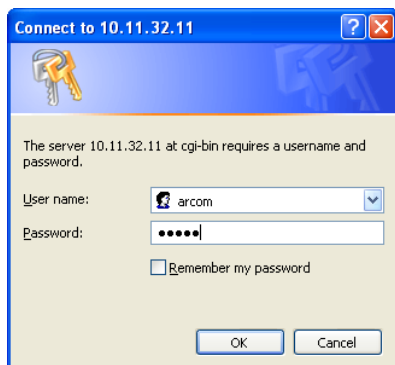
In Mozilla Firefox version 3, click “Or you can add an exception...”, and then click **Add Exception**.



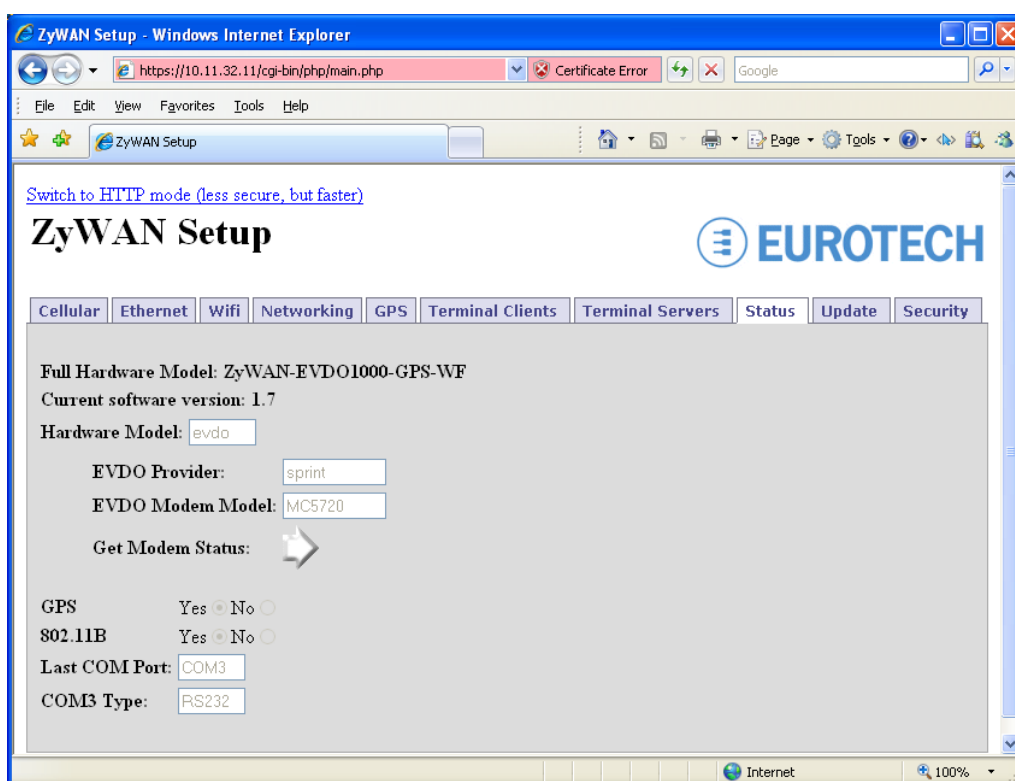
In the following dialog box, click **Get Certificate** and **Confirm Security Exception**.



3. Enter your login details when prompted. The default username is `arcom` and default password is `arcom`.



After logging in, the configuration page is displayed, as shown in the following screen capture.



The tabs across the top (*Cellular*, *Ethernet*, etc.) identify each section or page of the configuration. The current settings for any page are read from the ZyWAN whenever a tab is clicked. Clicking on the tab of a page that is currently displayed reloads the existing configuration.

Switching Between HTTP and HTTPS

By default, the ZyWAN uses Secure HTTP (HTTPS) for displaying its Web pages. This uses network IP port 443 and encrypts the data transferred between the computer and the ZyWAN. This can be switched to standard HTTP (unencrypted, IP port 80) by clicking on the link at the top, "Switch to HTTP mode (less secure, but faster)". The address URL changes to http://ip_address/cgi-bin/php/main2.php.

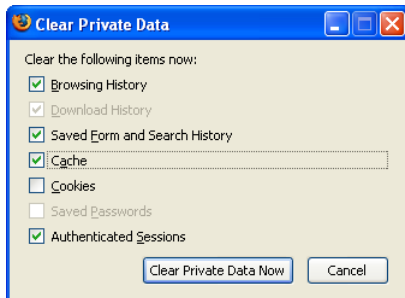
Switch back to HTTPS by clicking on the link "Switch to HTTPS mode (more secure, but slower)". The address URL will change back to http://ip_address/cgi-bin/php/main.php.

Clearing the Browser Cache

**Note:**

Web browsers (Internet Explorer, Firefox) can store cached copies of downloaded Web pages. If unexpected results occur in displaying the Web configuration, it may be due to the browser caching a copy of the files that control the Web interface. To correct this error, delete *Temporary Internet Files*, close all instances of the Web browser, and then re-open the ZyWAN Web page. The following section describes this procedure.

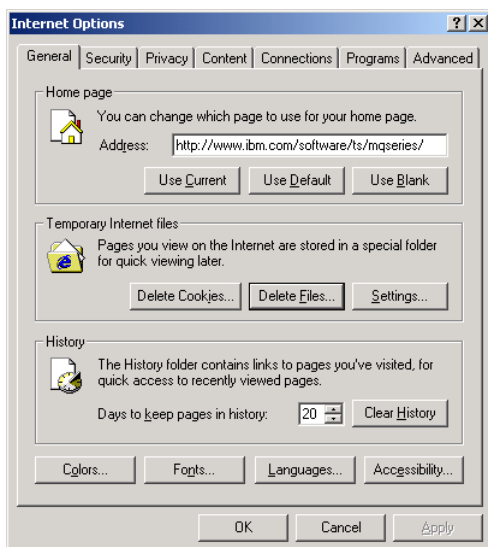
To clear the browser cache in Mozilla Firefox, select *Tools>Clear Private Data*. Make sure the “Cache” box is checked, and then click the **Clear Private Data Now** button.



To clear the browser cache in Internet Explorer version 7, select *Tools>Internet Options*, and then click the **Delete...** button under “Browsing history”. Click the **Delete files...** button to clear temporary Internet files.



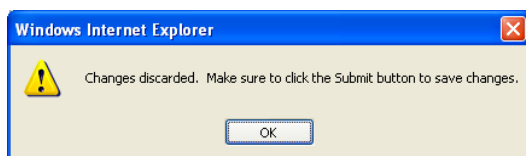
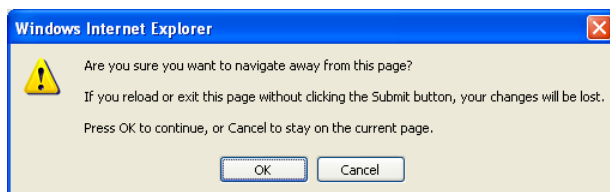
To clear the browser cache in Internet Explorer version 6, select *Tools>Internet Options*, and then click the **Delete Files...** button.



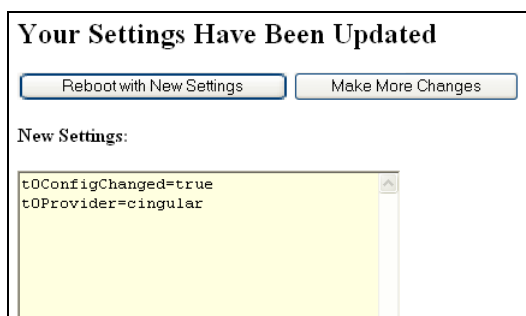
Changing a Configuration

The following sections describe the configuration details for each Web page. To make changes on any page of the configuration, complete the following steps:

1. Enter the changes you want to make, and then click the **Submit New Configuration** button. Changes must be submitted, or they will be lost. One of the following error messages will be displayed before closing the browser, moving to another page, or clicking on another tab without submitting changes.



2. Click on any tab or close the browser. The names and values of the properties are displayed in a box with the heading *New Settings*.



By submitting the configuration, the values of all properties on the displayed page only are stored in a properties file in permanent memory of the ZyWAN.

3. If there are more changes to be made on a different page of the configuration, click the **Make More Changes** button. The *Cellular* tab is displayed again so that another page may be selected and modified.



Important:

If the ZyWAN is not rebooted after all changes have been made, some settings will not take effect until the next reboot.

4. After all changes have been made, click the **Reboot with New Settings** button after submitting changes on any page. The ZyWAN then reboots so that the changes can take effect. The ZyWAN shuts down and restarts, which may take over a minute. The Web page automatically attempts to reload at the same IP address after 90 seconds.

Rebooting ZyWAN... Please wait up to 89 seconds.

New Settings:

```
reboot=true
```



Tip:

Even if no new changes have been made, the ZyWAN may be rebooted via the Web page by clicking the **Submit New Configuration** button on any page, then clicking the **Reboot with New Settings** button.

Using Default Gateway, DHCP, and DNS

The ZyWAN provides two Ethernet (eth0, eth1), WiFi (wlan0), and cellular (ppp0) interfaces. Each of these interfaces can potentially have a Default Gateway address, DHCP, and DNS server addresses. One of these interfaces will be made the default route to reach addresses not otherwise available on its local networks.

Configuration Options

The Ethernet interfaces can be configured to be a DHCP client on an existing network (the *Use Dhcp?* option set to Yes). The WiFi interface can be configured in similar manner (in “managed mode”). In this case, it is likely that the ZyWAN will obtain a Default Gateway and DNS server from the network to which it is attached.

Static IP addresses may also be configured. This allows the Ethernet or WiFi to be configured with a Default Gateway and two DNS Server addresses for the interface. These items may be left blank if there is no server available or if it does not make sense to include them in the configuration.

When configured with a static IP address, the Ethernet interface may be configured to *Run a DHCP Server*. This will allow the ZyWAN to deliver an IP address to other devices on the network. When operating in this mode, there is also an option to *Pass DNS servers to DHCP clients*. The WiFi interface in “master” or “ad-hoc” modes provides these same options to wireless clients.

Default Route

The ZyWAN will make one of its interfaces the default route based on the configuration and the availability of each network. The order of preference for the default route is:

- Ethernet 0 (eth0)
- Ethernet 1 (eth1)
- WiFi (wlan0)
- Cellular (ppp0)

The first interface which has a Default Gateway (static configuration in Web page, or dynamically obtained with DHCP) will be the one used for the ZyWAN's default gateway. If the network cable is unplugged or the WiFi becomes unavailable, the list of interfaces is checked again, and the first available interface will be selected dynamically as the default route, in order of preference.

This means, for instance, that if an application requires the cellular network to be the default gateway for network traffic, any static Default Gateway (in the ZyWAN Web configuration) or gateway obtained from DHCP will interfere with the intended operation.

DHCP Server and NAT

If either the Ethernet or WiFi (master or ad-hoc mode) is running a DHCP server, then the ZyWAN will reply to any device on the network that asks for an IP address using DHCP protocol. The ZyWAN will give the device an address in accordance with the list of addresses specified in the ZyWAN Web configuration. The device will be supplied the ZyWAN's network address as its Default Gateway.

The ZyWAN is able to act as a gateway, but in order to route traffic from one interface to another, there must also be a NAT entry configured on the *Networking* page to route from the source network to the destination network. The "Open Ports" section on the *Networking* page must include UDP port 67 to allow DHCP traffic to the ZyWAN.

DNS Server

As a DHCP Server, the ZyWAN may also be configured to pass DNS server addresses to other devices, so they can resolve named addresses (URL or FQDN). When this happens, the ZyWAN will provide its own IP address as the DNS server. The ZyWAN acts as a DNS proxy, so that any DNS requests from the client device are passed to the one of the DNS servers known to the ZyWAN, and the resulting IP address is returned to the client device.


In order to resolve DNS addresses, the ZyWAN needs to have a list of known DNS server(s). It obtains the list of these servers in the same way as it obtains its default route. The ZyWAN checks its interfaces in the preferred order: eth0, eth1, wlan0, and ppp0. The first active interface which contains one or more DNS servers (static address configured via the Web page, or obtained by the ZyWAN using DHCP) is used. This list of address(es) is used by the DNS proxy. If the Ethernet cable is unplugged or the WiFi becomes unavailable, the list of interfaces is checked again, and the first available interface will be selected dynamically as the location for DNS servers, in order of preference.

The "Open Ports" section on the *Networking* page must include UDP port 53, to allow DNS requests to the ZyWAN.

Chapter 2 System Status

The following diagram shows the *Status* tab.

Cellular Ethernet Wifi Networking GPS Terminal Clients Terminal Servers **Status** Update Security

Full Hardware Model: ZyWAN-EVDO1000-GPS-WF
 Current software version: 1.7
 Hardware Model:
 EVDO Provider:
 EVDO Modem Model:
 Get Modem Status: 
 GPS: Yes ☒ No ☐
 802.11B: Yes ☒ No ☐
 Last COM Port:
 COM3 Type:

Status Web Page

The *Status* tab includes several items which give the current status and hardware configuration. The hardware configuration is done in factory configuration and is provided here for information.

The following table lists the fields and options offered on the *Status* tab.

FIELD/OPTION	EXPLANATION
Full Hardware Model	The <i>Full Hardware Model</i> gives the model number of the ZyWAN, based on the types of options that were included from the factory. See ZyWAN Model Numbers on page 10, for information on the ZyWAN model numbers based on hardware configuration.
Current software version	The <i>Current software version</i> gives the current installed version of ZyWAN software.
Hardware Model	The <i>Hardware Model</i> gives the type of cellular modem installed. Options are indicated as: <i>gprs</i> , <i>3G</i> , <i>iden</i> , and <i>evdo</i> .
EVDO Provider	Since the EvDO cellular provider has to be specified with the modem provided with the ZyWAN, this is set as part of the factory configuration (applies only to ZyWAN-EVDO models). Possible options for EvDO provider are: <i>Sprint</i> , <i>Verizon</i> , <i>Bell Mobility</i> , and <i>Telus</i> .
EVDO Modem Module	The <i>EVDO Modem Module</i> gives the type of modem model used for EVDO (MC5720, MC5725, MC5727, E725).
GPS	This option indicates whether or not GPS hardware is installed.
802.11B	This option indicates whether or not an 802.11b WiFi module is installed.
Last COM Port	This option indicates what is the last available COM port on the ZyWAN, which is used in all other configuration menus where a selection of COM ports is allowed. Typically this is <i>COM3</i> .
COM3 Type	The COM3 port may be factory configured to be either RS-232 or RS-485/422. Options are indicated as: <i>RS-232</i> or <i>RS-485</i> .
Get Modem Status	Click the arrow icon next to <i>Get Modem Status</i> to open a window which gives status information on the cellular modem. See the next section for details on the contents of the status pages.

Get Modem Status



Click the arrow on the *Status* page to get modem and communication diagnostics for the cellular module. Before doing this action, the cellular configuration needs to be set, as described in [Cellular Configuration](#) on page 61.

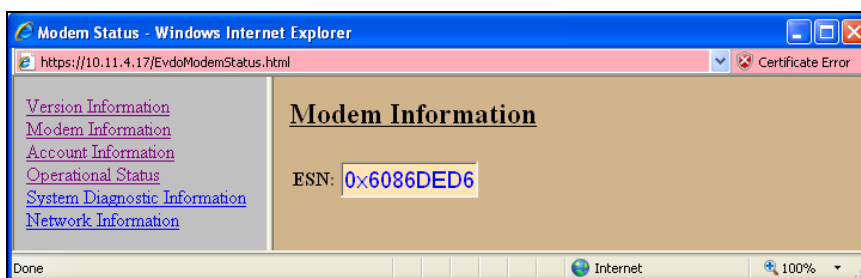
EVDO Status

Click the *Version Information* link to show version details on the EVDO cellular module.



FIELD/OPTION	EXPLANATION
	Version Information
Firmware Version	Firmware version in cellular module
Firmware Date	Date of firmware version in cellular module
PRL Version	Version of the PRL (Preferred Roaming List) stored in the cellular module

Click the *Modem Information* link to show modem settings for the EVDO cellular module.



FIELD/OPTION	EXPLANATION
	Modem Information
ESN	ESN (electronic serial number) of cellular module

Click the *Account Information* link to show account details for the EVDO cellular module.

The screenshot shows a web browser window titled "Modem Status - Windows Internet Explorer" with the address bar displaying "https://10.11.4.17/EvdoModemStatus.html". A "Certificate Error" icon is visible in the address bar. The left sidebar contains a list of links: "Version Information", "Modem Information", "Account Information", "Operational Status", "System Diagnostic Information", and "Network Information". The main content area is titled "Account Information" and displays the following fields:

Active NAM:	0
IP Address:	174.158.75.207
Activation Status:	activated
Activation Date:	2009-03-27
Phone Number:	801-865-3375
MDN:	801-865-3375
MIN:	801-953-6295

FIELD/OPTION	EXPLANATION
	Account Information
Active NAM	Selected profile, NAM0 or NAM1 (MC5725 only)
IP Address	Public IP address assigned by the cellular network
Activation Status	Status of whether the account is activated or not
Activation Date	Date that the cellular module was provisioned and activated on the network
Phone Number	Telephone number of the cellular module
MDN	MDN (Mobile Directory Number) of the cellular module
MIN	MIN (Mobile Station Identification Number) of the cellular module

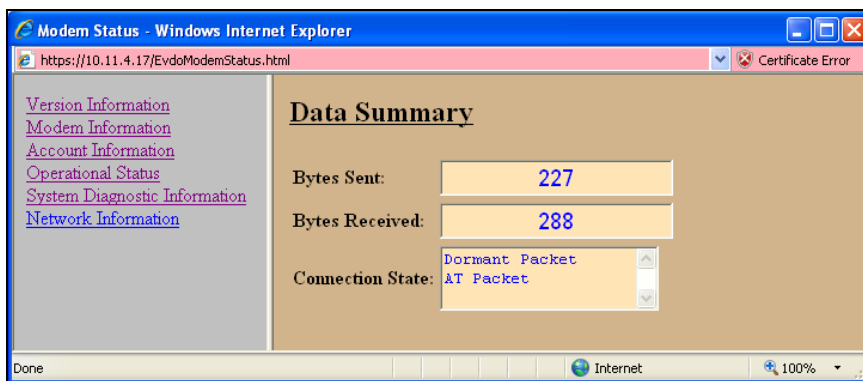
Click the *Operational Status Information* link to show current operational details, such as the EVDO cellular signal strength.

The screenshot shows the same web browser window, but the "Operational Status" link is selected in the sidebar. The main content area is titled "Operational Status" and displays the following fields:

Signal Strength (dBm):	-69
Channel Number:	50
Channel State:	Acquired
Current Band Class:	PCS

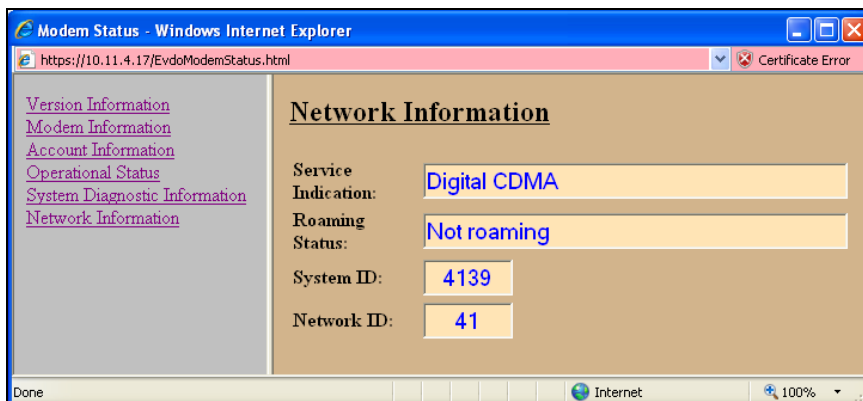
FIELD/OPTION	EXPLANATION
	Operational Status Information
Signal Strength	Received signal strength (RSSI), in dBm
Channel Number	Current 1xRTT active channel number or zero if digital service is not available
Channel State	Current 1xRTT channel acquisition state with possible states of acquired, not acquired, and scanning for channel
Current Band Class	Current tuning band of the modem (cellular or PCS)

Click the *System Diagnostic Information* link to show diagnostic data for the EVDO cellular module.



FIELD/OPTION	EXPLANATION
	System Diagnostic Information
Bytes Sent	Total number of bytes sent while a data call is active (The Sent and Received counters are reset after the call ends.)
Bytes Received	Total number of bytes received while a data call is active
Connection State	

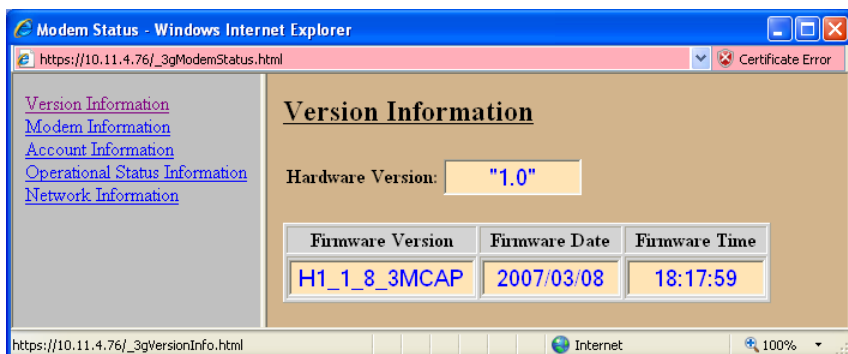
Click the *Network Information* link to show information about the EVDO cellular network.



FIELD/OPTION	EXPLANATION
	Network Information
Service Indication	Which type of service is currently available to the modem (No service, Digital CDMA, or GPS service)
Roaming Status	Status of whether roaming is available (Not roaming, Roaming with guaranteed SIDs, Roaming without guaranteed SIDs)
System ID	Current system identifier (SID) of the network providing service
Network ID	Current network identifier (NID) of the station providing service

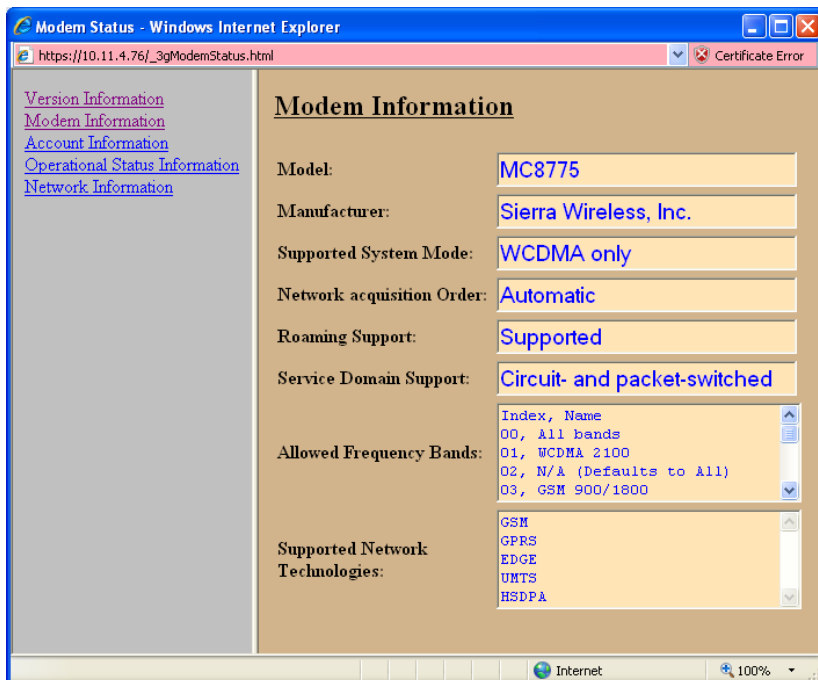
3G Status

Click the *Version Information* link to show version details on the 3G cellular module.



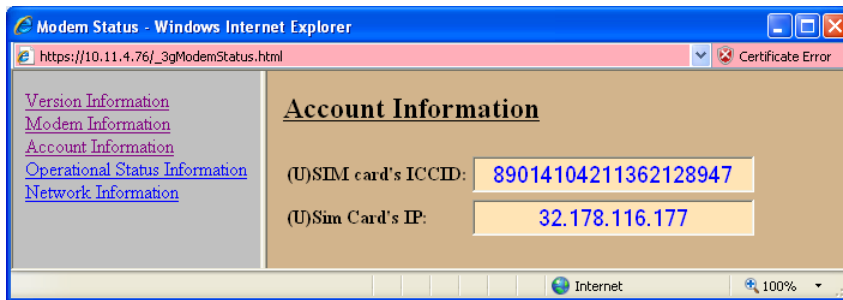
FIELD/OPTION	EXPLANATION
	Version Information
Hardware Version	Hardware version of cellular module
Firmware Version	Firmware version in cellular module
Firmware Date / Time	Date of firmware version in cellular module

Click the *Modem Information* link to show modem settings for the 3G cellular module.



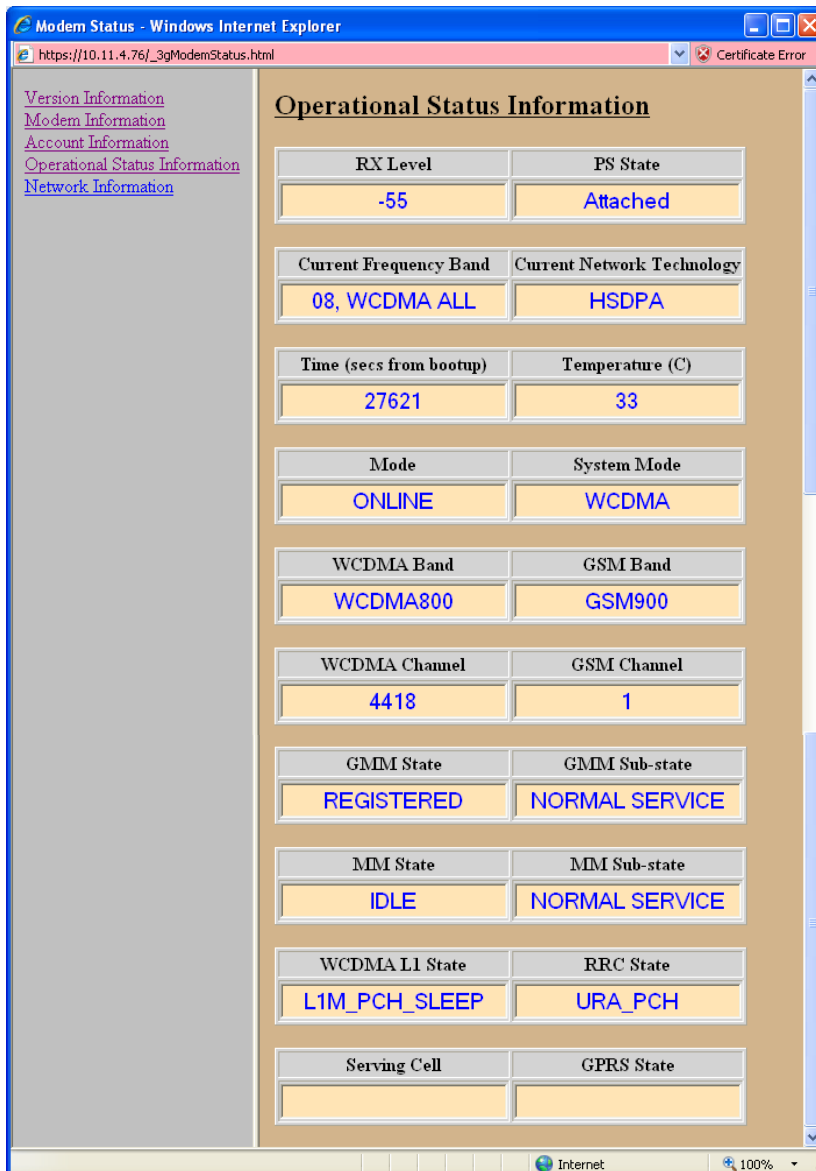
FIELD/OPTION	EXPLANATION
	Modem Information
Model	Hardware model of cellular module
Manufacturer	Manufacturer of cellular module
Supported System Mode	System modem (GSM or WCDMA) supported by module
Network acquisition Order	Order of acquiring GSM or WCDMA networks (or automatic)
Roaming Support	Whether roaming is supported in cellular module
Service Domain Support	Circuit or packet-switched domain support, or both
Allowed Frequency Bands	Frequency bands supported by cellular module
Supported Network Technologies	Network technologies supported by cellular module

Click the *Account Information* link to show account details for the 3G cellular module.



FIELD/OPTION	EXPLANATION
	Account Information
(U)SIM card's ICCID	Integrated Circuit Card ID of the installed SIM card
(U)Sim Card's IP	IP address obtained on cellular network

Click the *Operational Status Information* link to show current operational details, such as the 3G cellular signal strength.



FIELD/OPTION	EXPLANATION
	Operational Status Information
RX Level	Received cellular signal level (dBm)
PS State	State of packet-switch (data) connection to cellular network
Current Frequency Band	Frequency band currently in use
Current Network Technology	Network technology currently used by cellular module
Time	Current time, in seconds from power-up of the cellular module
Temperature	Approximate temperature, in degrees C
Mode	Current mode of the cellular module operation
System Mode	Current system mode acquired by cellular module
WCDMA Band / Channel	Current WCDMA band and channel number being accessed
GSM Band / Channel	Current GSM band and channel number being accessed
GMM State / Sub-state	Current GMM state
MM State / Sub-state	Current MM state
WCDMA L1 State	Current WCDMA L1 state, if in CDMA mode
RRC State	Current WCDMA RRC state, if in CDMA mode
Serving Cell	Serving cell, if in GSM/GPRS mode
GPRS State	Current GPRS state, if in GSM/GPRS mode

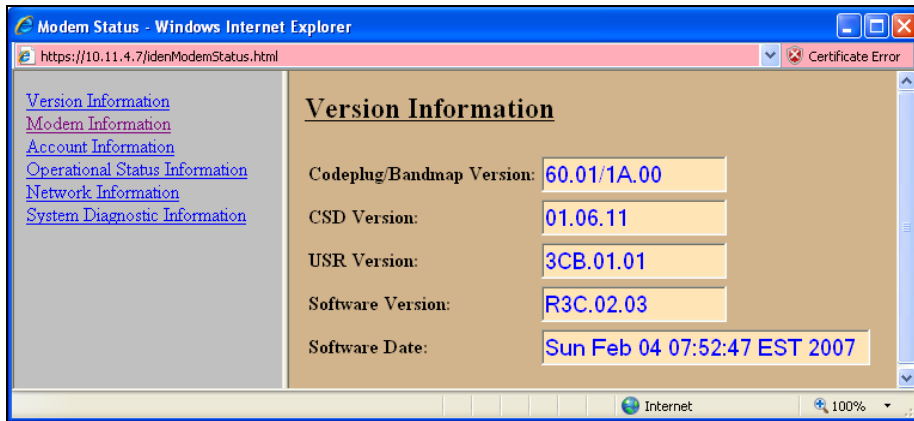
Click the *Network Information* link to show information about the 3G cellular network.



FIELD/OPTION	EXPLANATION
	Network Information
Service Status	Service availability (Service, No service, Limited service, Limited regional service)
Service Domain	Current service domain (circuit or packet switched, or both)
Roaming Status	Roaming status indicator
System Mode	Current system mode (No service, GSM/GPRS mode, WCDMA mode)
SIM Status	Availability of SIM card
Available Network Technologies	Technologies available on current network

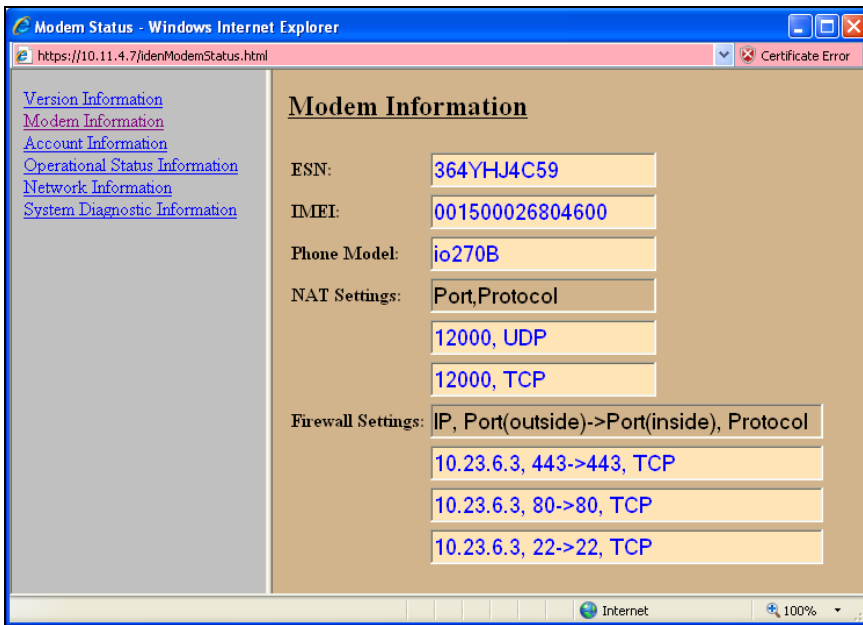
IDEN Status

Click the *Version Information* link to show version details on the IDEN cellular module.



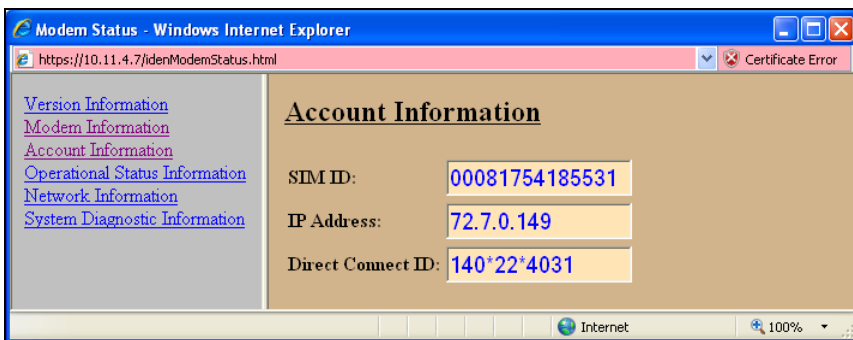
FIELD/OPTION	EXPLANATION
	Version Information
Codeplug/Bandmap Version	Codeplug and bandmap version loaded in iO270 cellular module, in the format AA.BB/CC.DD, where AA.BB is the codeplug revision, and CC.DD is the bandmap revision
CSD Version	CSD version, in the format EE.FF.GG, where EE is the bandmap version (type), FF is the structure version, and GG is the data version
USR Version	USR version, in the format HHc.JJ.KK, where HH is product identifier, c is sub ID, JJ is carrier ID, and KK is USR file version number
Software Version	iO270 software version, in the format cLL.MM.NN, where c is the load type, LL is the product identifier, and MM.NN is the revision
Software Date	Release date of Software Version

Click the *Modem Information* link to show modem settings for the IDEN cellular module.



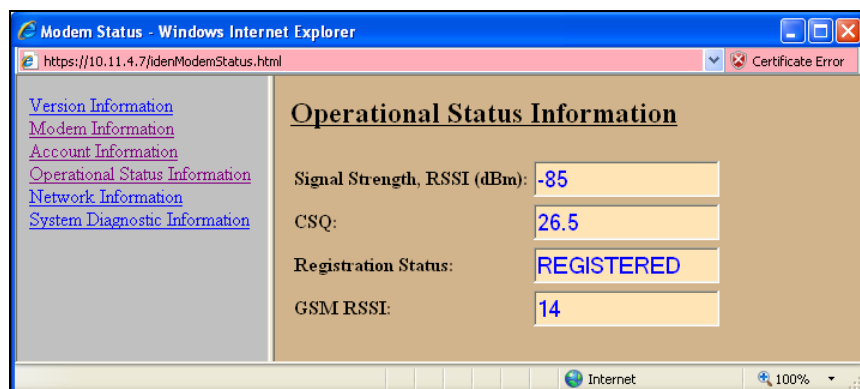
FIELD/OPTION	EXPLANATION
	Modem Information
ESN	ESN (electronic serial number) of io270 cellular module
IMEI	IMEI (International Mobile Equipment Identifier) of the cellular module
Phone Model	Model name of the cellular module
NAT Settings	NAT settings in the io270 cellular module cause outgoing packets to change their source port. This setting allows some packets to retain their original source port, using the specified protocol (TCP, UDP).
Firewall Settings	The io270 cellular module provides a network firewall for incoming connections. Any port to which a connection must be made from the cellular network must have a port opened in the firewall, for a specified protocol (TCP, UDP). The ZyWAN opens ports 443, 80, and 22 (TCP) by default, plus any ports which are listed in the <i>Networking</i> page of its configuration (see page 81).

Click the *Account Information* link to show account details for the IDEN cellular module.



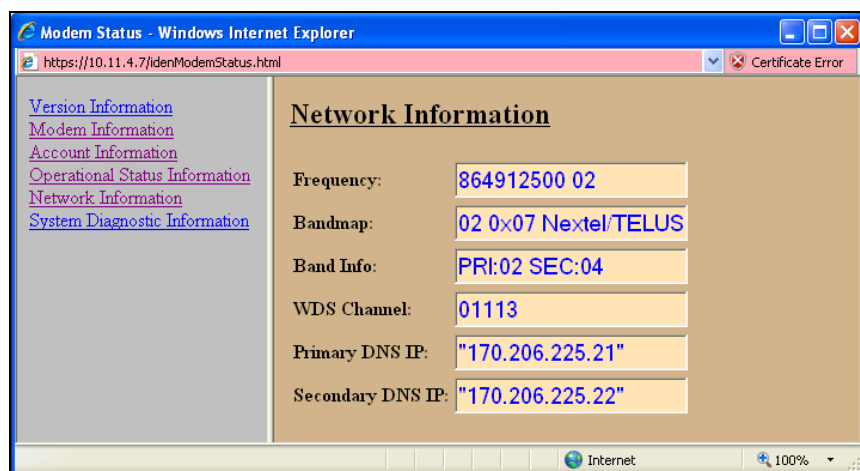
FIELD/OPTION	EXPLANATION
	Account Information
SIM ID	SIM card number
IP Address	IP address, if the cellular module is able to connect to the network
Direct Connect ID	Direct Connect ID (Push-to-Talk number) programmed in the SIM card

Click the *Operational Status Information* link to show current operational details, such as the IDEN cellular signal strength.



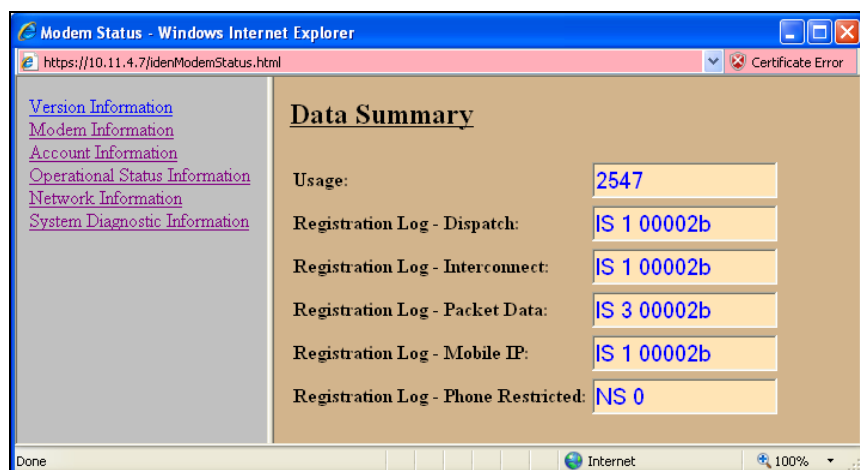
FIELD/OPTION	EXPLANATION
	Operational Status Information
Signal Strength, RSSI	Received signal strength of IDEN signal, in dBm
CSQ	IDEN cellular signal quality indication (SQE, higher number is better)
Registration Status	Status whether the cellular module is registered on the cellular network
GSM RSSI	Received signal strength of GSM carrier, 0-31 (31 is best)

Click the *Network Information* link to show information about the IDEN cellular network.



FIELD/OPTION	EXPLANATION
	Network Information
Frequency	Current frequency (in Hz) and frequency band to which the iO270 cellular module is connected
Bandmap	Bandmap information being used by the iO270
Band Info	Primary and secondary bands in use in the iO270
WDS Channel	Channel number of wireless data system (WDS)
Primary DNS IP Secondary DNS IP	Addresses of DNS server provided by the cellular network

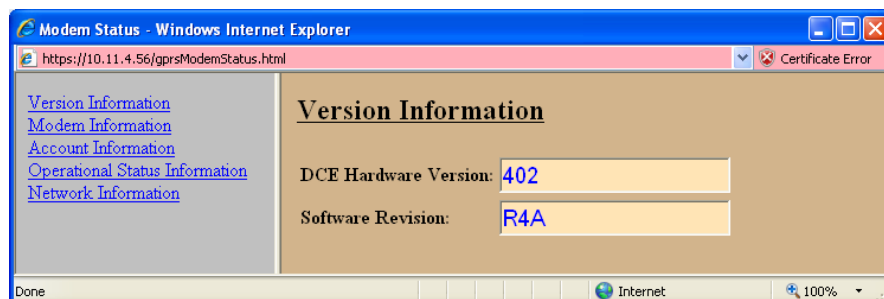
Click the *System Diagnostic Information* link to show diagnostic data for the iDEN cellular module.



FIELD/OPTION	EXPLANATION
	System Diagnostic Information
Usage	The total sum of minutes used for dispatch, interconnect and circuit data calls on an iDEN network
Registration Log – Dispatch, Interconnect, Packet Data, Mobile IP, & Phone Restricted	Registration log of various services in the iO270 cellular module (These are normally only of value in cases of rare problems in cellular registration, where these numbers can be reported to the cellular provider for diagnostics.)

GPRS Status

Click the *Version Information* link to show version details on the GPRS cellular module.



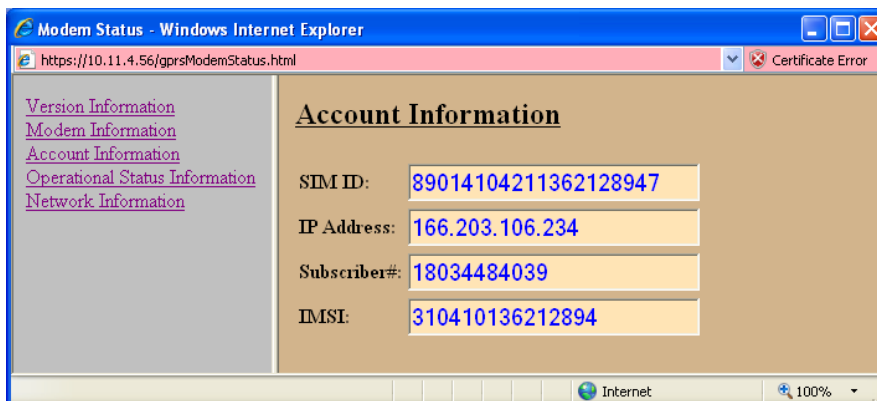
FIELD/OPTION	EXPLANATION
	Version Information
DCE Hardware Version	Hardware version of the cellular module
Software Revision	Software revision of the cellular module

Click the *Modem Information* link to show modem settings for the GPRS cellular module.



FIELD/OPTION	EXPLANATION
	Modem Information
ESN	ESN (electronic serial number) of the cellular module
IMEI	IMEI (International Mobile Equipment Identifier) of the cellular module
Phone Model	Model name of the cellular module
Phone Manufacturer	Manufacturer of the cellular module

Click the *Account Information* link to show account details for the GPRS cellular module.



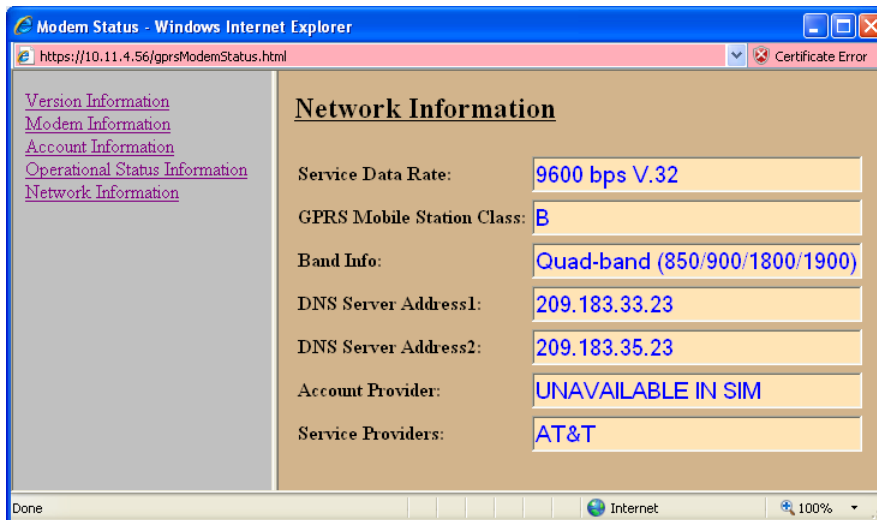
FIELD/OPTION	EXPLANATION
	Account Information
SIM ID	SIM card number
IP Address	IP address, if the cellular module is able to connect to the network
Subscriber#	Telephone number associated with the SIM card, if available
IMSI	IMSI (International Mobile Subscriber Identity) of the cellular module

Click the *Operational Status Information* link to show current operational details, such as the GPRS cellular signal strength.



FIELD/OPTION	EXPLANATION
	Operational Status Information
Signal Strength, RSSI	Received signal strength, in dBm, calculated from CSQ value
CSQ, BER	CSQ is an indication of GSM received signal strength, 0-31 (31 is best). BER is the channel bit error rate, 0-7 (0 is best).
GSM Registration Status	Registration status on cellular network Options are: Not registered, not searching Registered, home network Not registered, but searching for operator to register with Registration denied Not detailed Registered, roaming
GPRS Registration Status	Registration status on GPRS data network Options are: Not registered, not searching Registered, home network Not registered, but searching for operator to register with Registration denied Unknown Registered, roaming

Click the *Network Information* link to show information about the GPRS cellular network.



FIELD/OPTION	EXPLANATION
	Network Information
Service Data Rate	Data rate of the bearer service, used when data calls are originated or received
GPRS Mobile Station Class	Normally should be Class 'B' Other options include: CG – Class C in GPRS only mode CC – Class C in circuit switched mode only
Band Info	Current frequency band used in operation Options are: GSM & EGSM (900) GSM 1800 Dual-band 900/1800 PCS 1900 GSM 850 Dual-band 1900/850 Tri-band (900/1800/1900) Tri-band (850/1800/1900) Quad-band (850/900/1800/1900)
DNS Server Address1 DNS Server Address2	Addresses of DNS server provided by the cellular network
Account Provider	Service provider name stored in SIM, if available
Service Providers	Current GSM network service provider (Note: This does not show all available providers, only the provider currently being used).

Chapter 3 Cellular Configuration

The *Cellular* properties, and therefore the ZyWAN base model, are determined by what model of cellular modem is installed. This is configured at the factory. See [System Status](#) on page 47 to find out the ZyWAN model. The options for ZyWAN model and cellular modem are listed in the following table.

ZyWAN BASE MODEL	CELLULAR MODEM
ZyWAN-EvDO	Sierra Wireless MC5725, MC5727, or Novatel E725
ZyWAN-3G	Sierra Wireless MC8775
ZyWAN-IDEN	Motorola iO270
ZyWAN-GPRS	Wavecom GR64

On the *Cellular* tab, the items must be configured in order to enable the cellular data connection. After setting all the *Cellular* properties, click the **Submit New Configuration** button before switching to a new tab or closing the window. The available options are different depending on the ZyWAN model.

ZyWAN-EVDO Options

The following screen capture shows the *Cellular* tab on the ZyWAN-EVDO.

The following options may be configured to set up EVDO cellular network.

OPTION	EXPLANATION
Obtain DNS from Service Provider?	Normally, the cellular provider supplies one or more addresses of a DNS server to use while connected to the carrier, so this option should be set to <i>Yes</i> . If there is a case where the DNS server needs to be explicitly specified instead, set this to <i>No</i> and enter numeric IP addresses in the <i>Preferred</i> and (optional) <i>Alternate DNS Server</i> fields.
Activate EVDO Modem?	If the modem has not been activated on the cellular carrier's network, click <i>Yes</i> and continue with the activation instructions described next. Normally, this should have to be done only once.

EvDO modem modules contain the account activation information stored in the modem rather than a removable SIM card. Generally this is the responsibility of the customer to activate a module to put it into service. These operations can be done via the ZyWAN Web configuration page. The account activation process is different, depending on which modem module is installed. The modem installed in the ZyWAN can be seen by displaying the *Status* page. See [System Status](#) on page 47 for additional details.

Modem Activation of MC5727

Activate the EvDO account using the following steps:

1. To provision the account on the network, click the **IOTA/OMA-DM Provision** button. This must be done in an EvDO coverage area in the service provider's network area. IOTA stands for the 'Internet Over-the-Air' protocol, used for the MC5725. OMA-DM stands for 'Open Mobile Alliance – Device Management', used for the MC5727.
2. On the Sprint network, this should be all that is necessary to activate because the account settings will be automatically obtained from the cellular provider. It is possible that on other networks the account information needs to be manually written into the modem before doing the provisioning. If this is the case, follow the instructions for the MC5725 modem (note, the MC5727 only has one NAM account available).
3. After doing the IOTA/OMA-DM provisioning, the ZyWAN will automatically reboot.

Modem Activation of MC5725

Activate the EvDO account using the following steps:

1. Obtain the activation code (Master Subsidy Lock) and other NAM profile account information for a data account on an EvDO network. The network service provider provides this information.
2. Configure the modem module with the NAM profile information. On the ZyWAN, this is done by filling in the correct fields and clicking the **Set NAM Profile** button.
3. Provision the account profile to be active on the network, by clicking the **IOTA/OMA-DM Provision** button. This must be done in an EvDO coverage area in the service provider's network area.
4. After both setting the NAM profile and after the IOTA provisioning, the ZyWAN will automatically reboot. If doing both, allow time for the reboot after Set NAM Profile before doing the IOTA Provision option.



Important:

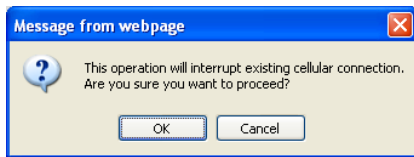
The EVDO network provider must be specified at the time of order so that the correct modem can be installed from the factory, so this is not given as a user configuration option. The service provider can be viewed on the *Status* page, see [System Status](#) on page 47 for more information.

The following table gives some information which may help with activation on several EVDO networks. These should be considered recommended settings in the absence of specific information from the cellular carrier. In the event that any problem is experienced in using these settings, contact the cellular carrier to verify this information. The items marked "provided" must be provided by the carrier for each modem.

Provider	MDN, MTN	MIN,MSID	SID	NID	MSL,OTSL, SPC	IOTA Provisioning
Sprint	provided	provided	0	65535	provided	as described next
Bell Mobility	same as MIN	provided	4139	41	provided	N/A - Not required
Verizon	provided	provided	41	65535	000000	as described next

Activate EVDO Modem?

Activation of an EvDO module may require information to be input by the user, as described previously. After selecting *Yes* to *Activate EVDO Modem?*, the following prompt is displayed.



The activation process or changing of accounts on the module interrupts any existing cellular connection, if currently active.

The following screen capture shows the *Cellular* tab if the Sierra Wireless MC5727 module is installed.

Cellular Ethernet **Wifi** Networking GPS Terminal Clients Terminal Servers Status Update Sec

Obtain DNS from Service Provider? Yes ☒ No ☐

For Service Provider Information, Please Refer to the "Status" Tab

Activate EVDO Modem? Yes ☒ No ☐

MSL,OTSL,SPC:

NAM Profiles						
NAM Profile	MDN,MTN	MIN,MSID	System ID	Network ID	Clear	
NAM 0 <input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>	

The following screen capture shows the *Cellular* tab if the MC5725 is installed.

Cellular Ethernet **Wifi** Networking GPS Terminal Clients Terminal Servers Status Update Secu

Obtain DNS from Service Provider? Yes ☒ No ☐

For Service Provider Information, Please Refer to the "Status" Tab

Activate EVDO Modem? Yes ☒ No ☐

MSL,OTSL,SPC:

NAM Profiles						
NAM Profile	MDN,MTN	MIN,MSID	System ID	Network ID	Clear	
NAM 0 <input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>	
NAM 1 <input type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Clear"/>	

The following screen capture shows the *Cellular* tab if the Novatel E725 is installed.


The following table lists the fields and options offered on the *Cellular* tab. See the previous table for information related to activation with specific cellular carriers.

FIELD/OPTION	EXPLANATION
NAM 0, NAM 1	(MC5725 only) Select the profile by clicking the toggle button next to either <i>NAM 0</i> or <i>NAM 1</i> . The <i>NAM 0</i> and <i>NAM 1</i> profile information allow two different accounts to exist on the same modem module. Some modems may only contain one set of profile information. If both profiles are activated, either may be provisioned for use in the cellular operation. Only one profile may be provisioned at any given time. The four fields for either profile may be cleared by clicking the Clear button to the right of the row. The MC5727 only has one NAM profile.
MDN, MTN	Enter the <i>Mobile Directory Number</i> (or <i>Mobile Telephone Number</i>) of the cellular module.
MIN, MSID	Enter the <i>Mobile Station Identification Number</i> of the cellular module.
System ID	(MC5725 only) Enter the <i>System ID</i> (SID). Some carriers do not require specific information for this field.
Network ID	(MC5725 only) Enter the <i>Network ID</i> (NID). Some carriers do not require specific information for this field.
MSL, OTSL, SPC	The <i>Master Subsidy Lock</i> (or <i>One Time Subsidy Lock</i> , or <i>Service Programming Code</i>) is a password for the activation of NAM profiles and is supplied by the network provider. This needs to be entered before a NAM profile may be activated.

The following table lists the available buttons.

BUTTON	EXPLANATION
Get NAM Profiles	<p>Clicking this button reads from the module any existing account profiles in the modem. This reads the <i>MDN</i>, <i>MSID</i>, <i>System ID</i>, and <i>Network ID</i> and fills the <i>NAM 0</i> and/or <i>NAM 1</i> entries on the Web page with this data. Otherwise, these values (supplied by the network provider) may also be entered by hand into those fields.</p> <p>The normal response from this action should begin with <i>HTTP Reply Status - 200</i> and contain additional lines with the MDN and other profile information as follows:</p>
(MC5727 response)	<pre> HTTP Reply Status - 200 MC5727: ---> at OK <NAM-0> ---> at~namval?0 MDN: 8016519710 MIN: 8019183951 SID: 4139 NID: 65535 OK </NAM-0> </pre>
(MC5725 response)	<pre> HTTP Reply Status - 200 <NAM-0> MDN: 9135299437 MDN: 9852534784 SID: 0 NID: 65535 OK </NAM-0> <NAM-1> MDN: 8585551515 MDN: 0000006951 SID: 0 NID: 65535 OK </NAM-1> </pre> <p>If the word <i>ERROR</i> is displayed here, another attempt may be made to request the NAM profiles.</p>

(E725 response)	<pre> HTTP Reply Status - 200 E725: ---> at NO CARRIER ---> at OK ---> at\$nwactivation? \$NWACTIVATION: 8018337159, 8019539892 OK ----- IOTA STATUS ----- ---> at+iota? Iota Enabled In Progress: 0 Repeat Test OK: 0 Repeat Test Failed: 0 Retry Command: 0 Current State: 1 Network Down Server Disconnected Retry: 0 Global State: 0 Number Get: 0 Number Post: 0 HTTP Status: 0 Proxy Not Trusted OK If the word <i>ERROR</i> is displayed here, another attempt may be made to request the NAM profiles. Note the "In Progress" value set to 0. If an IOTA Provisioning has been requested, this value may go to 1 for a period of time until it finishes and returns to 0. </pre>
Set NAM Profile	<p>This button sets the information for a modem account profile (MC5725, and possibly MC5727, only). After the <i>Master Subsidy Lock</i> and all the data for the modem profile are entered, click the Set NAM Profile button to activate the profile. After a few seconds, status information is displayed in the large text area.</p> <p>The normal response from this action should begin with <i>HTTP Reply Status - 200</i> as follows:</p>
(MC5725 response)	<pre> HTTP Reply Status - 200 at~namlck=468691 OK at~namval=0,9135299437,9852534784,0,65535 OK at!reset OK NAM Profile is set. Please allow a few seconds for the modem to reset. Wait at least 5-10 seconds before moving on to the next step. If the word <i>ERROR</i> is displayed here, another attempt may be made to set the NAM profile. </pre>

(E725 response)	<p>HTTP Reply Status - 200</p> <pre> ---> at NO CARRIER ---> at OK ---> at\$nwactivation=940038,8018337159,8019539892 OK </pre> <p>Wait at least 5-10 seconds before moving on to the next step. If the word ERROR is displayed here, another attempt may be made to set the NAM profile.</p>
IOTA/OMA-DM Provision	<p>After one or both NAM profiles has been activated, select the button for <i>NAM 0</i> or <i>NAM 1</i>, and then click the IOTA/OMA-DM Provision button. This provisions the profile by connecting to the cellular network using this account.</p> <hr/> <div data-bbox="523 862 603 943">  </div> <p>Note: The provisioning process requires an active cellular connection to the service provider and may not be able to be done in a roaming area. Make sure that a cellular antenna is connected to the ZyWAN and that the ZyWAN is located in an area where EvDO/CDMA service for the service provider is available.</p> <hr/>
	<p>Status information is displayed in the large text area. This may take several minutes for a response, possibly up to six minutes. The following message is displayed:</p> <p>Waiting for reply (this may take a few minutes to complete)</p> <p>The normal response from this action should look something like the following and end with the sentence <i>IOTA session completed successfully!</i> Scroll to the bottom of the received text response to validate that this message is given. The message should look something like one of the following:</p>

(MC5727 response)	<pre> 2963] HTTP: finished reading data: 237 bytes 2963] HTTP: Session(3) request tid=6 completed 2963] SSL session 0x12c5180 closed with status 0 2963] SSL session 0x12c5180 deleted 2964] Socket 684 closed 2964] HTTP: Disconnect request succeeded, SID=3 2968] HTTP: Shutdown 2970] Network closed 2970] Committing MIP Profile1 data... 2970] Committing NAM... 2970] Committing MDN... 2970] New NAM/MDN/PRL data activated 2970] MIP Profile 1 was provisioned - Setting active MIP profile to 1 2970] DM session completed successfully (type=1 initiator=0) OK Please wait for ZyWAN unit to restart ... If this success message is not displayed here, another attempt may be made to provision the account. If necessary, the entire response text from the text area can be copied and pasted, in order to request troubleshooting assistance from the service provider. </pre>
(MC5725 response)	<pre> <mmc mmcID="126" status-uri=""> <method id="1" name="disconnect" reportstatus="false" </method> </mmc> 140> MMC session disconnected, session id="126" 140> Resetting IOTA session, end status=0 140> HTTP: Shutdown 140> SSL session fff7f4 closed with status 0 140> SSL session fff7f4 deleted 141> Socket 275 closed 142> PPP closed 142> Netlib closed (app_id=101) 142> MIP Profile 1 was provisioned - Set active MIP profile to 1 142> IOTA session completed successfully! Client initiated=1 OK If this success message is not displayed here, another attempt may be made to provision the account. If necessary, the entire response text from the text area can be copied and pasted, in order to request troubleshooting assistance from the service provider. </pre>

(E725 response)	<p>Status information is displayed in the large text area. The following message is displayed:</p> <pre> Waiting for reply (this may take a few minutes to complete)... The normal response from this action should look something like the following: HTTP Reply Status - 200 ---> at NO CARRIER ---> at OK ---> at+iota=2 OK !! !!! Please wait for IOTA session to complete the work. !!! !!! Use 'Get NAM Profiles' option to verify IOTA status. !!! !! ----- IOTA STATUS ----- ---> at+iota? Iota Enabled In Progress: 1 Repeat Test OK: 0 Repeat Test Failed: 0 Retry Command: 1 Current State: 1 Network Up Server Connected Retry: 1 Global State: 400 Number Get: 1 Number Post: 0 HTTP Status: 0 Proxy Not Trusted OK This response will be returned from the E725 before the provisioning process is complete. This will be indicated by the “In Progress: 1” message (above). Wait a short period of time, then click Get NAM Profiles again – the provisioning attempt is completed when the response contains “In Progress: 0”. If this success message is not displayed here, another attempt may be made to provision the account. If necessary, the entire response text from the text area can be copied and pasted, in order to request troubleshooting assistance from the service provider. </pre>
Clear Status Area	Clicking the Clear Status Area button clears any previous status information in the text area.

ZyWAN-3G Options

The following screen capture shows the *Cellular* tab on the ZyWAN-3G.

The following options may be configured to set up the 3G cellular network.

OPTION	EXPLANATION
Obtain DNS from Service Provider?	Normally, the cellular provider supplies one or more addresses of a DNS server to use while connected to the carrier. So this option should be set to Yes. If there is a case where the DNS server needs to be explicitly specified instead, set this to No and enter numeric IP addresses in the <i>Preferred</i> and (optional) <i>Alternate DNS Server</i> fields.
Choose Your Network Provider	Choosing an option determines the network settings which are used to connect to the cellular data network. Options are: <i>-Disabled-</i> , <i>AT&T</i> , <i>O2</i> , <i>Orange</i> , <i>T-Mobile</i> , and <i>Custom</i> .
Select Frequency Band	Allows a specific 3G frequency band to be selected. This option is only available for network providers AT&T and T-Mobile.
Frequency Band	If Select Frequency Band is set to Yes, choose a cellular frequency band to operate on. Options are: <i>All bands</i> , <i>WCDMA 2100</i> , <i>GSM 900/1800</i> , <i>GSM ALL</i> , <i>WCDMA ALL</i> . If <i>All Bands</i> is selected, the modem will try all available bands when it attempts to register on the network. It may be more efficient to narrow the band or group of bands (such as <i>GSM All</i> , or <i>WCDMA All</i>) in the configuration, if this is known for the network being used.

Certain default settings are used for connecting to accounts when selecting specific providers. This information is listed in the following table for the various carriers. If any other settings are required, use the *Custom* option instead.

PROVIDER	DEFAULT SETTINGS
AT&T	APN: isp.cingular Dial String: atd*99***1# Authentication: PAP Username: ISP@CINGULARGPRS.COM Password: CINGULAR1
O2	APN: mobile.o2.co.uk Dial String: atd*99***1# Authentication: PAP Username: mobileweb Password: password (default, can be changed in <code>/etc/ppp/pap-secrets</code> file)
Orange	APN: orangeinternet Dial String: atd*99***1# Authentication: PAP Username: user Password: pass (default, can be changed in <code>/etc/ppp/pap-secrets</code> file)
T-Mobile	APN: wap.voicestream.com Dial String: atd*99***1# Authentication: (none)

If *Custom* is chosen as the network provider for ZyWAN-3G, the following screen capture lists the fields and options that are available.

FIELD/OPTION	EXPLANATION
APN	Enter the <i>APN</i> (Access Point Name) of the cellular provider's data connection. This is supplied by the cellular provider.
Dial String	Enter the AT command dial string which is dialed for connection to the cellular provider's APN.
Auth Type	Enter the Authentication type used by the cellular provider. Available types are: <i>None</i> , <i>Pap</i> , and <i>Chap</i> .
Frequency Band	If <i>Select Frequency Band</i> is set to <i>Yes</i> , choose a cellular frequency band to operate on. Options are: <i>All bands</i> , <i>WCDMA 2100</i> , <i>GSM 900/1800</i> , <i>GSM ALL</i> , <i>WCDMA ALL</i> . If <i>All Bands</i> is selected, the modem will try all available bands when it attempts to register on the network. It may be more efficient to narrow the band or group of bands (such as <i>GSM All</i> , or <i>WCDMA All</i>) in the configuration, if this is known for the network being used.

If the *Auth Type* is set to *Pap* or *Chap*, the following fields are available.

FIELD	EXPLANATION
Username	Enter the username required to log on to the APN of the cellular provider.
Password	Enter the password required to log on to the APN of the cellular provider.

ZyWAN-IDEN Options

The following screen capture shows the *Cellular* tab on the ZyWAN-IDEN.

The following table lists the items that are available.

FIELD/OPTION	EXPLANATION
Obtain DNS from Service Provider?	Normally, the cellular provider supplies one or more addresses of a DNS server to use while connected to the carrier, so this option should be set to <i>Yes</i> . If there is a case where the DNS server needs to be explicitly specified instead, set this to <i>No</i> and enter numeric IP addresses in the <i>Preferred</i> and (optional) <i>Alternate DNS Server</i> fields.
Choose Your Network Provider	Choosing an option determines the network settings which are used to connect to the cellular data network. Options are: <i>-Disabled-</i> , <i>Nextel</i> , and <i>Southern Linc</i> . For other private IDEN carriers, use the <i>Nextel</i> option.

ZyWAN-GPRS Options

The following screen capture shows the *Cellular* tab on the ZyWAN-GPRS.

The following options may be configured to set up the GPRS cellular network.

OPTION	EXPLANATION
Obtain DNS from Service Provider?	Normally, the cellular provider supplies one or more addresses of a DNS server to use while connected to the carrier, so this option should be set to <i>Yes</i> . If there is a case where the DNS server needs to be explicitly specified instead, set this to <i>No</i> and enter numeric IP addresses in the <i>Preferred</i> and (optional) <i>Alternate DNS Server</i> fields.
Choose Your Network Provider	Choosing an option determines the network settings which are used to connect to the cellular data network. Options are: <i>-Disabled-</i> , <i>AT&T</i> , <i>O2</i> , <i>Orange</i> , <i>T-Mobile</i> , and <i>Custom</i> .

Certain default settings are used for connecting to accounts when selecting specific providers. The following table lists this information for the various carriers. If any other settings are required, use the *Custom* option instead.

PROVIDER	DEFAULT SETTINGS
AT&T	APN: isp.cingular Dial String: atd*99***1# Authentication: PAP Username: ISP@CINGULARGPRS.COM Password: CINGULAR1
O2	APN: mobile.o2.co.uk Dial String: atd*99***1# Authentication: PAP Username: mobileweb Password: password (default, can be changed in <code>/etc/ppp/pap-secrets</code> file)
Orange	APN: orangeinternet Dial String: atd*99***1# Authentication: PAP Username: user Password: pass (default, can be changed in <code>/etc/ppp/pap-secrets</code> file)
T-Mobile	APN: wap.voicestream.com Dial String: atd*99***1# Authentication: (none)

If *Custom* is chosen as the network provider for ZyWAN-GPRS, the following screen capture lists the fields and options that are available.

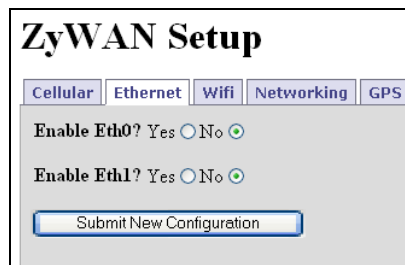
FIELD/OPTION	EXPLANATION
APN	Enter the <i>APN</i> (Access Point Name) of the cellular provider's data connection. This is supplied by the cellular provider.
Dial String	Enter the AT command dial string which is dialed for connection to the cellular provider's APN.
Auth Type	Enter the Authentication type used by the cellular provider. Available types are: <i>None</i> , <i>Pap</i> , and <i>Chap</i> .

If the *Auth Type* is set to *Pap* or *Chap*, the following fields are available.

FIELD	EXPLANATION
Username	Enter the username required to log on to the APN of the cellular provider.
Password	Enter the password required to log on to the APN of the cellular provider.

Chapter 4 Ethernet configuration

The following screen capture shows the Ethernet tab.



ZyWAN Setup

Cellular Ethernet Wifi Networking GPS

Enable Eth0? Yes ☐ No ☒

Enable Eth1? Yes ☐ No ☒

Submit New Configuration

The following items must be configured in order to enable one or both of the Ethernet network connections.

Enable Eth0/Eth1

Select *Yes* to enable the first and/or second Ethernet ports available on the ZyWAN. When the Ethernet port is enabled, the options may be configured as described in the following sections.

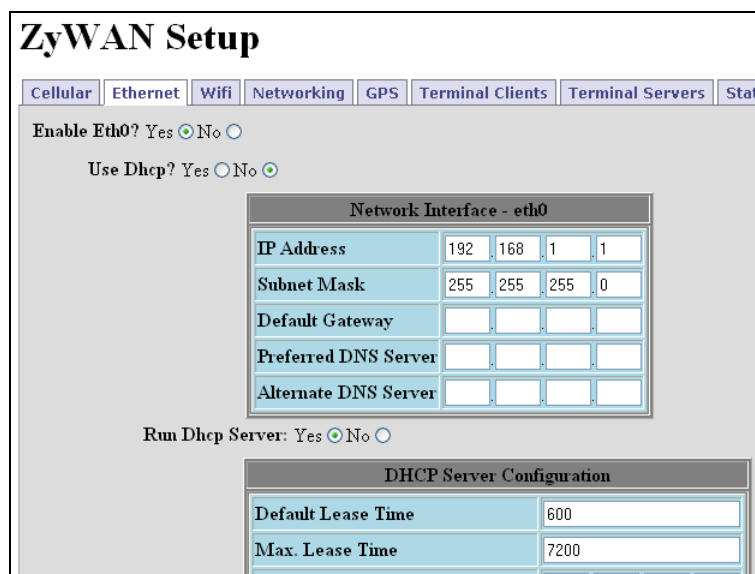
After setting all the Ethernet properties, click the **Submit New Configuration** button before switching to a new tab or closing the window.

DHCP Client

If *Use Dhcp?* is set to *Yes*, the ZyWAN acts as a DHCP client to automatically obtain its Ethernet network address settings from a server on the LAN. Otherwise, set this parameter to *No* in order to configure specific TCP/IP addresses.

Fixed Address

The following screen capture shows the *Ethernet* tab if *Use Dhcp?* is set to *No*.



ZyWAN Setup

Cellular Ethernet Wifi Networking GPS Terminal Clients Terminal Servers Stat

Enable Eth0? Yes ☒ No ☐

Use Dhcp? Yes ☐ No ☒

Network Interface - eth0

IP Address	192	168	1	1
Subnet Mask	255	255	255	0
Default Gateway				
Preferred DNS Server				
Alternate DNS Server				

Run Dhcp Server: Yes ☐ No ☒

DHCP Server Configuration

Default Lease Time	600
Max. Lease Time	7200

The following table lists the fields available in the *Ethernet* tab if *Use Dhcp?* is set to *No*.

FIELD/OPTION	EXPLANATION
IP Address	Enter the specific numeric address for ZyWAN. Each of the four fields must be a number between 1 and 255.
Subnet Mask	Enter the subnet mask for this Ethernet network. Each of the four fields must be a number between 0 and 255.
Default Gateway	Enter the numeric address of the default gateway for this network, if this interface should be used as the default route. Each of the four fields must be a number between 1 and 255. If this interface is not the default route, leave the <i>Default Gateway</i> blank.
Preferred DNS Server	Enter the primary DNS server address. Each of the four fields must be a number between 1 and 255. If DNS is not needed or the server is unavailable, the DNS address may be left blank.
Alternate DNS Server	Enter the secondary DNS server address. Each of the four fields must be a number between 1 and 255. If DNS is not needed or a secondary DNS server is unavailable, the DNS address may be left blank.
Run DHCP Server	This option is used when the ZyWAN is to act as a DHCP server on the Ethernet network, assigning network addresses to other devices. Set this to <i>No</i> if this option is not used.

DHCP Server

The following screen capture shows the *Ethernet* tab if *Run Dhcp Server* is set to *Yes*.

Use Dhcp? Yes ☐ No ☒

Network Interface - eth0

IP Address	192	168	1	1
Subnet Mask	255	255	255	0
Default Gateway				
Preferred DNS Server				
Alternate DNS Server				

Run Dhcp Server: Yes ☒ No ☐

DHCP Server Configuration

Default Lease Time	600
Max. Lease Time	7200
Subnet Mask	255 255 255 0
Range From	192 168 1 10
Range To	192 168 1 254
Pass DNS servers to DHCP clients	Yes <input type="radio"/> No <input checked="" type="radio"/>

The following table lists the fields and options available in the *Ethernet* tab if *Run Dhcp Server* is set to *Yes*.

FIELD/OPTION	EXPLANATION
Default Lease Time	Enter the default lease time (in seconds) for the assigned DHCP lease to expire. The default time is the time assigned if the client does not request a specific lease time.
Max. Lease Time	Enter the maximum lease time (in seconds). This is the maximum lease time which is assigned, regardless of whether the client has requested a longer lease time.
Subnet Mask	Enter the subnet mask defining the range of network addresses to be assigned by this DHCP server. Each of the four fields must be a number between 0 and 255.
Range From	Enter the numeric address of the lowest DHCP address to be assigned by this DHCP server. Each of the four fields must be a number between 1 and 254.
Range To	Enter the numeric address of the highest DHCP address to be assigned by this DHCP server. Each of the four fields must be a number between 1 and 254, greater than the Range From.
Pass DNS Servers to DHCP Clients	Set this option to <i>Yes</i> if the ZyWAN should act as a DNS proxy server on the network. The ZyWAN will pass requests to whatever DNS server is assigned on its default route, and will pass the responses back to the requesting client.

Note:



If the *Run Dhcp Server* option is set to *Yes*, then UDP port 67 must be included in the "Open Ports" section of the *Networking* page.

If *Pass DNS servers to DHCP clients* is set to *Yes*, UDP port 53 must be included in "Open Ports".

Chapter 5 WiFi configuration

The following screen capture shows the *Wifi* tab.

The following items must be configured in order to enable the 802.11 network connection.

FIELD/OPTION	EXPLANATION												
Mode	<p>Select the mode of operation of the 802.11 module. Options are: <i>ad-hoc</i>, <i>managed</i>, <i>master</i>, and <i>Disabled</i>. A brief description of these modes is given next.</p> <p><i>Ad-hoc</i>: Network composed of only one group of wireless devices and without an Access Point.</p> <p><i>Managed</i>: ZyWAN connects to an 802.11 Access Point on a network.</p> <p><i>Master</i>: ZyWAN is the synchronization master, acting as an Access Point.</p> <p>Depending on the option selected, several of the main configuration options change, as shown in the following table.</p> <table><tr><th>MODE</th><th>DHCP/FIXED IP</th><th>RUN DHCP SERVER</th></tr><tr><td><i>Ad-hoc</i></td><td>Selectable</td><td>Selectable, fixed IP only</td></tr><tr><td><i>Managed</i></td><td>Selectable</td><td>Not an option</td></tr><tr><td><i>Master</i></td><td>Fixed IP only</td><td>Selectable</td></tr></table>	MODE	DHCP/FIXED IP	RUN DHCP SERVER	<i>Ad-hoc</i>	Selectable	Selectable, fixed IP only	<i>Managed</i>	Selectable	Not an option	<i>Master</i>	Fixed IP only	Selectable
MODE	DHCP/FIXED IP	RUN DHCP SERVER											
<i>Ad-hoc</i>	Selectable	Selectable, fixed IP only											
<i>Managed</i>	Selectable	Not an option											
<i>Master</i>	Fixed IP only	Selectable											
SSID	Enter the network name (domain ID) which is to be used for this wireless network. Enter an SSID of <i>any</i> (case-sensitive) to allow roaming in managed or ad-hoc modes.												
Channel	Select the frequency (channel) to use for the wireless network.												
Use Encryption?	Select whether to use wireless encryption of data sent through this wireless network. It is strongly recommended to use encryption, unless the application does not support it.												
Encryption Type	If <i>Use Encryption?</i> is selected above, select the <i>Encryption Type</i> . Options are: <i>WEP</i> (Wired Equivalent Privacy), <i>WPA</i> (WiFi Protected Access), and <i>WPA2</i> . WPA2 uses the more secure AES encryption standard.												

FIELD/OPTION	EXPLANATION
Key or Passphrase	<p>If WEP is chosen for the Encryption Type, the Key must be entered. This is entered as either a 5-character alphanumeric or 10-character hexadecimal string (40-bit encryption), or a 13-character alphanumeric or 26-character hexadecimal value (104-bit encryption). The hexadecimal characters must be entered as numbers, or letters between A and F (upper or lowercase).</p> <p>If WPA or WPA2 is chosen for the Encryption Type, the Passphrase must be entered. This is an 8 to 63 character alphanumeric string or 64-character hexadecimal value (256-bit encryption).</p>

After setting all the *WiFi* properties, click the **Submit New Configuration** button before switching to a new tab or closing the window.

Depending on the choice of *Mode* for *WiFi* operation, the *DHCP Client*, *Fixed Address*, and *DHCP Server* options are used for the IP address settings, as discussed in the following sections.

DHCP Client

If *Use Dhcp?* is set to *Yes*, the ZyWAN acts as a DHCP client to automatically obtain its WiFi network address settings from a server on the WiFi network.

Fixed Address

If this parameter is set to *No* in *ad-hoc* or *managed* modes or if the mode is set to *master*, the specific TCP/IP addresses must be configured.

The following screen capture shows the *Wifi* tab if *Use Dhcp?* is set to *No*.

ZyWAN Setup

Cellular Ethernet **Wifi** Networking GPS Terminal Clients

Mode: **ad-hoc**

Use Dhcp? Yes ☐ No ☒

Network Interface - wifi

IP Address				
Subnet Mask				
Default Gateway				
Preferred DNS Server				
Alternate DNS Server				

Run DHCP Server: Yes ☐ No ☒

SSID:

The following table lists the fields and options available in the *Wifi* tab if *Use Dhcp?* is set to *No*.

FIELD/OPTION	EXPLANATION
IP Address	Enter the specific numeric address for ZyWAN. Each of the four fields must be a number between 1 and 255.
Subnet Mask	Enter the subnet mask for this Ethernet network. Each of the four fields must be a number between 0 and 255.
Default Gateway	Enter the numeric address of the default gateway for this network, if this interface should be used as the default route. Each of the four fields must be a number between 1 and 255. If this interface is not the default route, leave the <i>Default Gateway</i> blank.
Preferred DNS Server	Enter the primary DNS server address. Each of the four fields must be a number between 1 and 255. If DNS is not needed or the server is unavailable, the DNS address may be left blank.
Alternate DNS Server	Enter the secondary DNS server address. Each of the four fields must be a number between 1 and 255. If DNS is not needed or a secondary DNS server is unavailable, the DNS address may be left blank.
Run DHCP Server	This option is available when the <i>Mode</i> is <i>ad-hoc</i> or <i>master</i> . This allows the ZyWAN is to act as a DHCP server on the WiFi network, assigning network addresses to other devices. Set this to <i>No</i> if this option is not used.

DHCP Server

If *Run DHCP Server* is set to Yes, the *DHCP Server Configuration* table is displayed.

Alternate DNS Server

Run DHCP Server: Yes ☒ No ☐

DHCP Server Configuration	
Default Lease Time	<input type="text" value="600"/>
Max. Lease Time	<input type="text" value="7200"/>
Subnet Mask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Range From	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Range To	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Pass DNS servers to DHCP clients	Yes <input type="radio"/> No <input checked="" type="radio"/>

SSID:

The following table lists the fields and options available in the *DHCP Server Configuration* table.

FIELD/OPTION	EXPLANATION
Default Lease Time	Enter the <i>Default Lease Time</i> (in seconds) for the assigned DHCP lease to expire. The default time is the time assigned if the client does not request a specific lease time.
Max. Lease Time	Enter the maximum lease time (in seconds). This is the maximum lease time which is assigned, regardless of whether the client has requested a longer lease time.
Subnet Mask	Enter the <i>Subnet Mask</i> defining the range of network addresses to be assigned by this DHCP server. Each of the four fields must be a number between 0 and 255.
Range From	Enter the numeric address of the lowest DHCP address to be assigned by this DHCP server. Each of the four fields must be a number between 1 and 254.
Range To	Enter the numeric address of the highest DHCP address to be assigned by this DHCP server. Each of the four fields must be a number between 1 and 254, greater than the <i>Range From</i> .
Pass DNS Servers to DHCP Clients	Set this option to <i>Yes</i> if the ZyWAN should act as a DNS proxy server on the network. The ZyWAN will pass requests to whatever DNS server is assigned on its default route, and will pass the responses back to the requesting client.

Note:

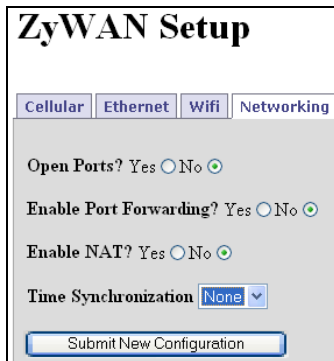


If the *Run Dhcp Server* option is set to *Yes*, then UDP port 67 must be included in the "Open Ports" section of the *Networking* page.

If *Pass DNS servers to DHCP clients* is set to *Yes*, UDP port 53 must be included in "Open Ports" section of the *Networking* page.

Chapter 6 Networking configuration

The following screen capture shows the *Networking* tab.



ZyWAN Setup

Cellular Ethernet **Wifi** Networking

Open Ports? Yes ☐ No ☒

Enable Port Forwarding? Yes ☐ No ☒

Enable NAT? Yes ☐ No ☒

Time Synchronization **None**

Submit New Configuration

The following items must be configured in order to enable open ports, port forwarding, network address translation, or NTP services.

Open Ports

Select Yes if you wish to open the ZyWAN firewall to inbound TCP or UDP connections. This applies to any traffic from other devices that terminates at the ZyWAN, not port forward or NAT traffic.

Note:

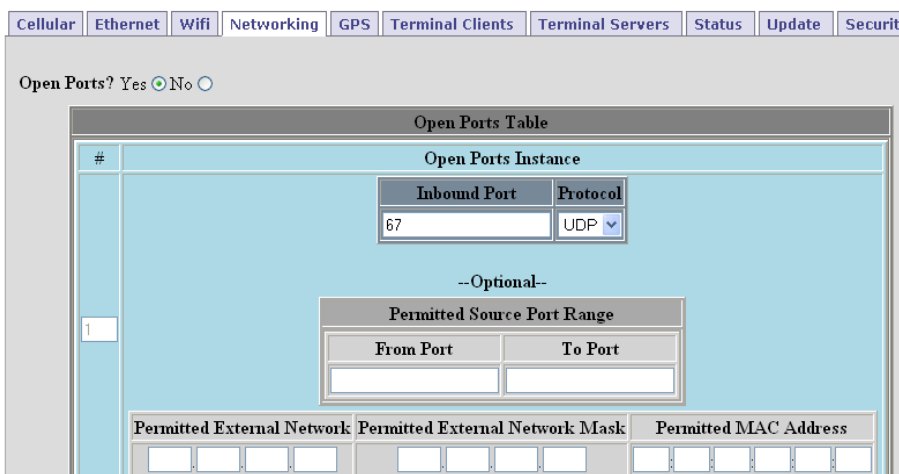
The *Open Ports* section must include UDP port 67 if *DHCP Server* is used for Ethernet or WiFi. UDP port 53 must be included if *Pass DNS Servers to DHCP Clients* is set to Yes for Ethernet or WiFi.



Any configured ports on the *Terminal Server* page, GPS UDP, or GPS Terminal Server ports will also need to have those ports configured in the *Open Ports* page. If not, the firewall will block those connections.

On the ZyWAN-IDEN models, the IO270 modem firewall is limited to 35 open ports which can be added based on the ZyWAN configuration, plus the ports 22, 80 and 443 which are added by default.

The following screen capture shows the *Networking* tab if *Open Ports* is set to Yes.



Cellular Ethernet Wifi **Networking** GPS Terminal Clients Terminal Servers Status Update Security

Open Ports? Yes ☒ No ☐

Open Ports Table		
#	Open Ports Instance	
	Inbound Port	Protocol
1	67	UDP
--Optional--		
Permitted Source Port Range		
	From Port	To Port
Permitted External Network Permitted External Network Mask Permitted MAC Address		

**Note:**

Changes made to the *Open Ports*, *Port Forwarding* and *NAT* portions of the *Networking* page take effect immediately after submitting changes, without requiring a reboot.

The following table lists the buttons available.

BUTTON	EXPLANATION
Insert Row#	Each of the table rows is numbered. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row needs to be filled in with all data required.
Delete Row#	In order to delete a row in the table, enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.

The following table lists the fields available in the *Networking* tab if *Open Ports* is set to *Yes*.

FIELD	EXPLANATION
Inbound Port	Enter the port number of the incoming connection. Port numbers must be a number between 1 and 65535.
Protocol	Enter the protocol of the incoming port (TCP or UDP).
<u>Optional fields:</u>	The following optional fields configure the firewall to filter allowed incoming connections to the ZyWAN.
Permitted Source Port Range	Enter the range of source port numbers allowed for the incoming connection. Normally source ports are randomly assigned, so this field should only be used when the source port is specified.
Permitted External Network	Enter the numeric IP address, or range of addresses, which is the source of the connection to the ZyWAN. Each of the four fields must be a number between 0 and 255. For instance, entering an IP address network of 172.16.11.0 limits incoming connections from addresses 172.16.11.1 through 172.16.11.255.
Permitted External Network Mask	Enter the subnet mask for the <i>Permitted External Network</i> . Each of the four fields must be a number between 0 and 255.
Permitted MAC Address	Enter the MAC address, in hexadecimal format, of a specific computer which is allowed to make a connection to the configured <i>Inbound Port</i> .

Enable Port Forwarding

Select **Yes** if you wish to forward individual IP ports. If a host connection comes in on one network interface at a given port, its communication is redirected to the IP address and port number on another of the ZyWAN interfaces.



Note:

When forwarding a port number from one interface to another, there must usually also be a NAT rule created on the *Networking* page, from the source IP network to the destination interface.

The following screen capture shows the *Networking* tab if *Enable Port Forwarding* is set to **Yes**.



Note:

Changes made to the *Open Ports*, *Port Forwarding* and *NAT* portions of the *Networking* page take effect immediately after submitting changes, without requiring a reboot.

The following table lists the buttons available.

BUTTON	EXPLANATION
Insert Row#	Each of the table rows is numbered. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row needs to be filled in with all data required.
Delete Row#	In order to delete a row in the table, enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.

The following table lists the fields available in the *Networking* tab if *Enable Port Forwarding* is set to *Yes*.

FIELD	EXPLANATION
Inbound Interface	Enter the name of the network interface on which to monitor the incoming connection to an IP port, such as <i>eth0</i> or <i>ppp0</i> . See Understanding Network Interfaces on page 21 for a description of the available interfaces on the ZyWAN.
Inbound Port	Enter the port number of the incoming connection. Port numbers must be a number between 1 and 65535.
Destination Address	Enter the numeric IP address to which the network traffic is redirected. Each of the four fields must be a number between 1 and 255.
Destination Port	Enter the destination port number to which the network traffic is redirected. Port numbers must be a number between 1 and 65535.
<u>Optional fields:</u>	The following optional fields configure the firewall to filter allowed incoming connections to the ZyWAN.
Permitted Source Port Range	Enter the range of source port numbers allowed for the incoming connection. Normally source ports are randomly assigned, so this field should only be used when the source port is specified.
Permitted External Network	Enter the numeric IP address, or range of addresses, which is the source of the connection to the ZyWAN. Each of the four fields must be a number between 0 and 255. For instance, entering an IP address network of 172.16.11.0 limits incoming connections from addresses 172.16.11.1 through 172.16.11.255.
Permitted External Network Mask	Enter the subnet mask for the <i>Permitted External Network</i> . Each of the four fields must be a number between 0 and 255.
Permitted MAC Address	Enter the MAC address, in hexadecimal format, of a specific computer which is allowed to make a connection to the configured <i>Inbound Port</i> .

Enable NAT

Select *Yes* if you wish to enable Network Address Translation, also referred to as IP Masquerading. This allows devices on one interface of the ZyWAN ('internal' side) to access the network on a second interface ('external' side), typically to allow devices to connect to the Internet via a single external IP address. The ZyWAN re-writes the source and/or destination Internet addresses in a packet as they pass through, so that they appears on the external side as from a single IP address, but on the internal side there may be multiple addresses which are hidden from the external network. NAT keeps track of outbound TCP connections and distributes incoming packets to the correct machine.

The following screen capture shows the *Nat Table* if *Enable NAT* is set to *Yes*.

Enable NAT? Yes ☒ No ☐

NAT Table											
#	Source Network/Address				Source Netmask				Source Interface	Destination Interface	Masquerade
1	192	168	1	0	255	255	255	0	eth0	ppp0	Yes <input checked="" type="radio"/> No <input type="radio"/>

The following table lists the buttons available.

BUTTON	EXPLANATION
Insert Row#	Each of the table rows is numbered. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row needs to be filled in with all data required.
Delete Row#	In order to delete a row in the table, enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.


The following table lists the fields available in the *Nat Table* if *Enable NAT* is set to *Yes*.

FIELD	EXPLANATION
Source Network / Address	Enter the numeric IP address, or range of addresses, which the ZyWAN translates from the source (internal) network. Each of the four fields must be a number between 0 and 255. For instance, entering an IP address network of 172.16.11.0 translates all addresses from 172.16.11.1 through 172.16.11.255.
Source Netmask	Enter the subnet mask for the <i>Source Network/Address</i> . Each of the four fields must be a number between 0 and 255.
Source Interface	Enter the name of the network interface which contains the source network (above).
Destination Interface	Enter the name of the network interface which is the destination (external) side of the network address translation. The public IP address on that interface has already been defined in the <i>Ethernet</i> or <i>WiFi</i> sections of the configuration, or it might be assigned by the cellular provider as part of the data services activation on that network. The interface names must be entered such as <i>eth0</i> or <i>ppp0</i> . See Understanding Network Interfaces on page 21 for a description of the available interfaces on the ZyWAN.
Masquerade	The normal setting for <i>Masquerade</i> is <i>Yes</i> , providing forwarding and Network Address Translation between the two interfaces. There may be rare cases where this should be set to <i>No</i> , which retains the internal forwarding of packets between the two interfaces, but disables the network address translation.

Time Synchronization

Select the method of synchronizing the internal clock of the ZyWAN. Available options are: *None*, *GPS*, and *NTP*. The GPS option allows the time to be acquired from the GPS receiver (if installed). The NTP (Network Time Protocol) updates the clock using NTP protocol from a network server. The following screen capture shows the *Table of NTP Servers* table available if *Time Synchronization* is set to *NTP*.

The following table lists the buttons available.

BUTTON	EXPLANATION
Insert Row#	Each of the table rows is numbered. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row needs to be filled in with all data required.
Delete Row#	<p>In order to delete a row in the table, enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.</p> <hr/> <p>Note:</p> <p> If the clock is not retained after loss of power, it may either be that the battery link on the main circuit board is not fitted or that the coin cell battery has failed and needs to be replaced.</p> <hr/>

The following table lists the fields available in *Table of NTP Servers* if *Time Synchronization* is set to *NTP*.

FIELD	EXPLANATION
NTP Servers to Use (IP address or FQDN)	<p>Enter either the numeric address or named address (Fully Qualified Domain Name, FQDN) of an NTP server to use for synchronizing the system date and time. Insert additional rows if more NTP servers are desired.</p> <p>The best time server to use is one available on a local network, if available. This avoids using public Internet resources and gives more accurate time. The second best option is to use a time server which is located on the Internet somewhere close (small roundtrip time). Otherwise, some possible addresses are: 0.pool.ntp.org, 1.pool.ntp.org, and 2.pool.ntp.org (these addresses point to three randomly assigned servers, which change every hour), or simply pool.ntp.org.</p>

After setting all the properties, click the **Submit New Configuration** button before switching to a new tab or closing the window.

Chapter 7 GPS configuration

The following screen capture shows the *GPS* tab.

GPS (Global Positioning System) data is gathered from the GPS receiver using the standard NMEA protocol and may be redirected to either a serial or TCP port. See the NMEA Web site (www.nmea.org) for more information on the NMEA protocol standard. The GPS data may also be cached and delivered to a server in another format using the UDP protocol.

The following table lists the options that may be configured to enable the collection and distribution of GPS data.

OPTION	EXPLANATION
Forward GPS to physical COM Port?	Select Yes for this item to send GPS data to a physical serial port on the ZyWAN in NMEA format. See page 88.
Enable GPS Terminal Server?	Select Yes to enable a terminal server on the ZyWAN, which allows a host to connect and obtain streaming GPS data over a network connection in NMEA format. See page 89.
GPS UDP Message Format?	<p>Select a data format to enable the ZyWAN to send GPS data over a network connection using UDP protocol. Available options are <i>None</i>, <i>Arcom Format</i>, and <i>ActSoft Format</i>. See page 90.</p> <p>When selecting the <i>ActSoft Format</i>, the server address is sent to a Comet Tracker server by Actsoft™ Inc. (www.actsoft.com).</p> <p>When selecting the <i>Arcom Format</i>, a server is required which is able to handle the Arcom GPS data format. See Arcom Format for GPS Messages (UDP) on page 92 for further details.</p>

After setting all the properties, click the **Submit New Configuration** button before switching to a new tab or closing the window.

Forward GPS to Physical COM Port

The following screen capture shows the *GPS* tab if *Forward GPS to Physical COM Port* is set to *Yes*.

Cellular Ethernet Wifi Networking GPS Ter

Forward GPS to physical COM Port? Yes ☒ No ☐

Outbound COM Port: COM2

Baud Rate: 115200

Data Bits: 8

Parity: None

Stop Bits: 1

Flow Control: None

Enable GPGLL? Yes ☒ No ☐

Enable GPGGA? Yes ☒ No ☐

Enable GPVTG? Yes ☒ No ☐


Enable GPRMC? Yes ☒ No ☐

Enable GPGSA? Yes ☒ No ☐

Enable GPGSV? Yes ☒ No ☐

Enable PFST,FOM? Yes ☒ No ☐

The following table lists the options offered.

OPTION	EXPLANATION
Outbound COM Port	Select the serial COM port to which the GPS data is sent. <div>  Important: Make sure this COM port is not configured for another service in the ZyWAN. Otherwise, both services may conflict for the port and not operate correctly. </div>
Baud Rate	Select the baud rate to use for the serial GPS output. Baud rate options range from 1200 to 115,200 bps.
Data Bits	Select the number of data bits to use for the serial GPS output. Options are 5, 6, 7, and 8.
Parity	Select the parity to use for the serial GPS output. Options are <i>None</i> , <i>Odd</i> , <i>Even</i> , <i>Mark</i> , <i>Space</i> .
Stop Bits	Select the number of stop bits to use for the serial GPS output. Options are 1, 1.5, and 2.
Flow Ctrl	Select whether to use hardware flow control for the serial GPS output. Options are <i>None</i> , and <i>RTS/CTS</i> (hardware flow control).

The *Enable* options determine which NMEA messages are sent through the COM port. The following table describes these options.

OPTION	EXPLANATION
Enable GPGLL?	Select Yes to enable the <i>GPGLL</i> message in the NMEA data stream.
Enable GPGGA?	Select Yes to enable the <i>GPGGA</i> message in the NMEA data stream.
Enable GPVTG?	Select Yes to enable the <i>GPVTG</i> message in the NMEA data stream.
Enable GPRMC?	Select Yes to enable the <i>GPRMC</i> message in the NMEA data stream.
Enable GPGSA?	Select Yes to enable the <i>GPGSA</i> message in the NMEA data stream.
Enable GPGSV?	Select Yes to enable the <i>GPGSV</i> message in the NMEA data stream.
Enable PFST,FOM?	Select Yes to enable the <i>PFST</i> and <i>FOM</i> messages in the NMEA data stream.

Enable GPS Terminal Server

The following screen capture shows the window if *Enable GPS Terminal Server?* is set to **Yes**.

Enable GPS Terminal Server? Yes ☒ No ☐

TCP Port To Listen On:

Maximum Number of Connections Allowed:

Enable GPGLL? Yes ☒ No ☐

Enable GPGGA? Yes ☒ No ☐

Enable GPVTG? Yes ☒ No ☐

Enable GPRMC? Yes ☒ No ☐

Enable GPGSA? Yes ☒ No ☐

Enable GPGSV? Yes ☒ No ☐

Enable PFST,FOM? Yes ☒ No ☐



Note:

If the GPS Terminal Server is configured here, it must also be included as a TCP port in the “Open Ports” section of the *Networking* page, so the firewall will allow connections to be made to the ZyWAN.

The following table lists the fields offered if *Enable GPS Terminal Server?* is set to **Yes**.

FIELD	EXPLANATION
TCP Port To Listen On:	Enter the port number to use for the terminal server which delivers GPS data to a host. Port numbers must be an unused port number between 1 and 65535.
Maximum Number of Connections Allowed:	Enter the maximum number (between 1 and 8) of simultaneous host connections which are allowed to connect to the ZyWAN to receive streaming GPS data.

The *Enable* options determine which NMEA messages are sent through the network port. The following table describes these options.

OPTION	EXPLANATION
Enable GPGLL?	Select Yes to enable the <i>GPGLL</i> message in the NMEA data stream.
Enable GPGGA?	Select Yes to enable the <i>GPGGA</i> message in the NMEA data stream.
Enable GPVTG?	Select Yes to enable the <i>GPVTG</i> message in the NMEA data stream.
Enable GPRMC?	Select Yes to enable the <i>GPRMC</i> message in the NMEA data stream.
Enable GPGSA?	Select Yes to enable the <i>GPGSA</i> message in the NMEA data stream.
Enable GPGSV?	Select Yes to enable the <i>GPGSV</i> message in the NMEA data stream.
Enable PFST,FOM?	Select Yes to enable the <i>PFST</i> and <i>FOM</i> messages in the NMEA data stream.

GPS UDP Message Format


The following screen capture shows the window if *GPS UDP Message Format?* is set to *Arcom Format* or *ActSoft Format*.


Note:



If the GPS UDP option is configured here, its UDP server port must also be included in the "Open Ports" section of the *Networking* page as UDP, so the firewall will allow acknowledgements to be sent back to the ZyWAN. This is required for the *Actsoft Format* mode, and for *Arcom Format* where the "Enable Cache" option is set to **Yes**.

The following table lists the fields and options offered.

FIELD/OPTION	EXPLANATION
Server IP Address:	Enter the numeric IP address or fully qualified domain name (FQDN) to which the UDP packets are sent containing GPS data. This is the address of the host computer, which must be available on the network (such as the Internet) to receive this data. Each of the four fields must be a number between 1 and 255. If the ActSoft Format is used, this IP address should generally be gps.cometracker.com.
Server Port Number:	Enter the destination port number on the host computer which receives the GPS data over UDP. Port numbers must be a number between 1 and 65535. If the ActSoft Format is used, the port number should generally be 8502.
Request Interval:	Enter the interval (in seconds) for how often the GPS data is obtained from the GPS receiver. Range is 1 to 65535 seconds for the Arcom mode, 30 to 65535 for ActSoft mode. Multiple GPS positions can be collected and buffered, to be sent all together as determined by the <i>Send Threshold</i> , in order to reduce the network traffic.
Send Threshold:	Enter the <i>Send Threshold</i> as a number between 1 and 19. The <i>Send Threshold</i> is a numeric value which indicates how many GPS positions should be sent in one position message. The position message will not be sent until the specified number of GPS positions have been obtained from the GPS receiver.
Unit ID:	<p>Enter the unit ID which identifies the GPS data from this ZyWAN when reported to a host computer. This allows the host computer to have unique identifiers for data coming from multiple remote units.</p> <p>When using the <i>Actsoft Format</i>, this <i>Unit ID</i> must be a unique 10-character serial number to identify this device in the Actsoft system.</p> <p>For ZyWAN-IDEN: The <i>Unit ID</i> reported to ActSoft must be the 10-character modem serial number.</p> <p>For all other models: The <i>Unit ID</i> is a unique 10-character serial number, with format to be specified by ActSoft.</p> <hr/> <div>  <p>Warning: It is essential to observe that this <i>Unit ID</i> field is entered correctly. If not and if duplicate ID's are reporting from any other device, both remote devices may suffer loss of data and an interruption of GPS reporting service.</p> </div> <hr/>

FIELD/OPTION	EXPLANATION
Enable Cache?	<p>Select Yes to enable caching of GPS data. When caching is enabled, the ZyWAN stores 100 positions in non-volatile memory. After this cache is filled, the oldest positions are discarded. Once the network connection is re-established, positions in the cache will transmitt in a first-in, first-out order. This is the only option for ActSoft mode, and the option is not available to set to No.</p> <p>When Enable Cache is set to Yes, a UDP acknowledgement is required from the host computer, which allows the ZyWAN to verify the data has been received. If the UDP acknowledgement is not received, the data points begin to be cached.</p> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>The Enable Cache option requires that the ZyWAN network address must be accessible to the host computer, since the host must initiate a one-way UDP acknowledgement message to the ZyWAN. If the acknowledgement is not received (due to network problems, etc.), the ZyWAN caches the GPS points based on the Request Interval and Send Threshold parameters (above) and continues trying to send the next point every 10 seconds.</p> </div> </div> <hr/> <p>When Enable Cache is set to No (Arcom format only), a UDP acknowledgement is not required. The ZyWAN simply sends out the GPS points when it can and does not store them locally. If the host computer does not receive the position message, those positions are lost.</p>

Arcom Format for GPS Messages (UDP)

When using the *Arcom Format* for GPS data, the position message is transmitted using the User Datagram Protocol (UDP). If caching is enabled, the ZyWAN waits a minimum of 10 seconds to receive an acknowledgement message after transmission of a position message. If a response message is received that does not contain the characters *ACK* or no message is received within the timeout period, the position message is retransmitted. This process continues indefinitely. The *ACK* must be 3 ASCII characters (0x41 0x43 0x4B).

The position message is defined next. The first 12 bytes are a header, followed by 19-byte portions containing the timestamp and position information. The number of these 19-byte portions is determined by the *Send Threshold* parameter. All data is in binary big-endian format, unless otherwise specified.

Message header:

som(1)	snum(10)	npos(1)
--------	----------	---------

Position data (repeated):

sval(1)	time(4)	stat(1)	sats(1)	lat(4)	lon(4)	psrc(1)	speed(1)	head(2)
---------	---------	---------	---------	--------	--------	---------	----------	---------

The following table describes the fields of the position message.

FIELD	BYTES	DESCRIPTION
som	1	This field indicates the start of message and is always set to 0x7E.
snum	10	This field contains the unit serial number in ASCII left justified and null(0) filled to the right.
npos	1	This field gives the number of positions in this message.
sval	1	The field contains the sequence value for each position transmitted. The sequence value for the first position transmitted is 0. The sequence value is incremented by 1 for each subsequent position transmitted. Since this value is only one byte, the maximum sequence value is 255.
time	4	This field contains the UTC timestamp of the GPS position and its value is in seconds since 1/1/1970.
stat	1	This field contains a code representing status of the position from the GPS receiver. In addition, bits 5-7 are used as flags for other conditions. <i>Status Codes:</i> Bit: 1 Condition: No response from GPS receiver Bit: 2 Condition: Error in response from GPS receiver Bit: 3 Condition: Almanac error response from GPS receiver Bit: 4 Condition: Good position response from GSP receiver <i>Flag Bits:</i> Bit 5: UTC TIME FLAG – This bit must be set to indicate that the TIMETAG represents UTC time. Bit 6: OVERFLOW FLAG – This bit is set to indicate that this position, after being added to the store and forward cache, caused an existing position in the store and forward cache to be deleted. Bit 7: FIRST POSITION FLAG – This bit is set to indicate that this is the first position to be transmitted after the device was powered on. For all subsequent positions, this bit must be cleared.
sats	1	This field contains the number of satellites currently being tracked.
lat	4	This field contains the latitude of the position in 1/100,000 minutes. For example, the 'North 26 Degrees 8.767840 Minutes' is represented as $(26 * 60 * 100000 + 8.767840 * 100000) = 156876784$.
lon	4	This field contains the longitude of the position in 1/100,000 minutes. For example, the 'WEST 80 Degrees 15.222400 Minutes' is represented as $-(80 * 60 * 100000 + 15.222400 * 100000) = -481522240$.
psrc	1	This field contains ASCII 'G'(0x47) if this is a valid GPS position. Otherwise, it contains ASCII 'N'(0x4E).
speed	1	This field contains the speed in miles per hour.
head	2	This field contains the heading in degrees.

Chapter 8 Terminal Clients

The following screen capture shows the *Terminal Clients* tab.

The Terminal Client makes an outbound TCP/IP connection to a remote server, allowing pass-through communication with a local serial port. Its serial port also provides AT command emulation to act similar to a dial modem.

After setting all the Terminal Client properties, click the **Submit New Configuration** button before switching to a new tab or closing the window.



Note:

Changes made to the *Terminal Clients* page take effect immediately after submitting changes without requiring a reboot.

To allow one or more Terminal Client services to be configured, set *Enable Terminal Clients* to *Yes*. The *Table of Terminal Clients* is displayed, as shown in the following screen capture.

The following table lists the buttons available.

BUTTON	EXPLANATION
Insert Row#	<p>Each of the Terminal Clients exists as a large set of properties in a numbered table row. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row must be filled in with all data required.</p> <p>Note that this table can get very large, with inner tables on each Terminal Client table row. When adding or deleting a Terminal Client configuration, make sure to click the Insert Row# or Delete Row# buttons at the very bottom of the main table.</p>
Delete Row#	<p>In order to delete a Terminal Client configuration (a row in the main table), enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.</p>

The following screen capture shows a *Table of Terminal Clients* containing the Terminal Client configuration.

Enable Terminal Clients: Yes ☒ No ☐

#	COM Port	Baud Rate	Data Bits	Parity	Stop Bits	Flow Control	Respond with OK?	DTR Indicates Connect State?
1	- Select -	115200	8	None	1	None	Yes <input type="radio"/> No <input checked="" type="radio"/>	Yes <input type="radio"/> No <input checked="" type="radio"/>


Buffer Size: Demark Timer: Reconnect Delay: Connect Mode: - Select - Serial Driver: Native Linux

Host Connection Table

#	Host Connection Instance
1	

Insert Row # Delete Row #

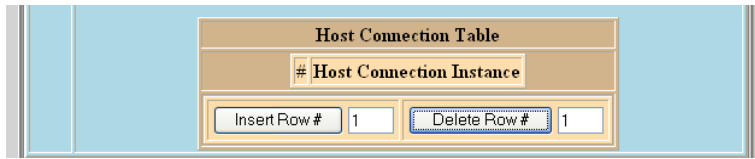
The following table lists the fields and options that are available and that must be set for each configured Terminal Client configuration.

FIELD/OPTION	EXPLANATION
COM Port	<p>Select the serial COM port to which the Terminal Client data is sent.</p> <hr/> <p>Important:</p> <p> Make sure this COM port is not configured for another service in the ZyWAN. Otherwise, both services may conflict for the port and not operate correctly.</p> <hr/>
Baud Rate	Select the baud rate to use for the Terminal Client port. Baud rate options range from 1200 to 115,200 bps.
Data Bits	Select the number of data bits to use for the Terminal Client port. Options are 5, 6, 7, and 8.
Parity	Select the parity to use for the Terminal Client port. Options are <i>None</i> , <i>Odd</i> , <i>Even</i> , <i>Mark</i> , <i>Space</i> .
Stop Bits	Select the number of stop bits to use for the Terminal Client port. Options are 1, 1.5, and 2.
Flow Ctrl	Select whether to use hardware flow control for the Terminal Client port. Options are <i>None</i> , and <i>RTS/CTS</i> (hardware flow control).
Respond with OK?	Choose whether an OK message is sent in response to AT commands entered at the Terminal Client serial port. The OK response is similar to the way in which a modem responds to a computer over its serial port.
DTR Indicates Connect State	Specify whether DTR indicates the IP connection state. If set to Yes, the serial port's DTR output is asserted to a positive voltage when the IP connection is established, and is de-asserted when the IP connection is lost. This is meant to operate similar to a Carrier Detect (CD) output from a dial modem, which is asserted after a data connection is established.

FIELD/OPTION	EXPLANATION
Buffer Size	Enter the maximum number of data bytes (between 1 and 4095) which are allowed in an IP packet. The actual amount may be less if the <i>Demark Timer</i> times out before the serial buffer is full. This <i>Buffer Size</i> works both ways –network originated packets are sent to the serial port in blocks of bytes, and data coming in the serial port are broken into network packets of the configured number of bytes.
Demark Timer	Enter the maximum time (in milliseconds, between 10 and 30000) the ZyWAN waits for non-activity on the serial port before sending whatever serial data has been received.
Reconnect Delay	Enter the length of time (in seconds, between 1 and 65535) the Terminal Client waits before attempting to re-establish a lost connection with the server, if the connection has been dropped for any reason. This option only applies when the <i>Connect Mode</i> is set to <i>Continuously</i> .
Connect Mode	<p>Choose the connection mode. The options available are:</p> <p><i>Continuously</i>: Connect automatically upon system restart or upon either device dropping the IP connection. There must be only one Host Connection row, and its <i>Matching Dial String</i> field must be left empty.</p> <p><i>Any Data</i>: Connect only when data is received from a serial device connected to the COM Port. There must be only one Host Connection row, and its <i>Matching Dial String</i> field must be left empty.</p> <p><i>ATDT String</i>: Connect only if an <i>ATDT####</i> message is received on the serial port, where <i>####</i> is some alphanumeric string. There may be many Host Connection rows configured under this Terminal Client, with their <i>Dial String</i> set to unique <i>ATDT####</i> values. The ATDT mode acts as a modem emulator, whereby each ATDT dial sequence initiates a connection to an IP address. Until a matching dial string is received, the ZyWAN does not make an outbound Terminal Client connection. See <i>Matching Dial String</i> for more details.</p> <p><i>Use DCD Pin</i>: Connect if the Data Carrier Detect (DCD) input signal on the serial port is raised to a positive RS-232 voltage. This must be used with an RS-232 port and does not apply when COM3 uses the RS-485 hardware option. There must be only one Host Connection row, and its <i>Matching Dial String</i> field must be left empty.</p> <p><i>ATDT or DCD</i>: Connect if either <i>ATDT####</i> message is received or if the Data Carrier Detect (DCD) signal on the serial port is asserted. If the ATDT message is received, it is compared against the <i>Matching Dial String</i> in the Host Connection rows to find which IP address to use for connection. If the DCD is received, the ZyWAN is connected to the IP address of the first Host Connection row with an empty field for the <i>Matching Dial String</i>.</p>
Serial Driver	Select whether to use the Native Linux (ttyS) serial driver or the ACSCOMM Eurotech driver. The ACSCOMM option allows for half-duplex RS-485 communication, and it can provide better handling of hardware flow control if needed.

Host Connection Table

The *Host Connection Table* is part of the Terminal Client configuration, as shown in the following screen capture.



At least one row must be configured in the *Host Connection Table* for it to work properly.



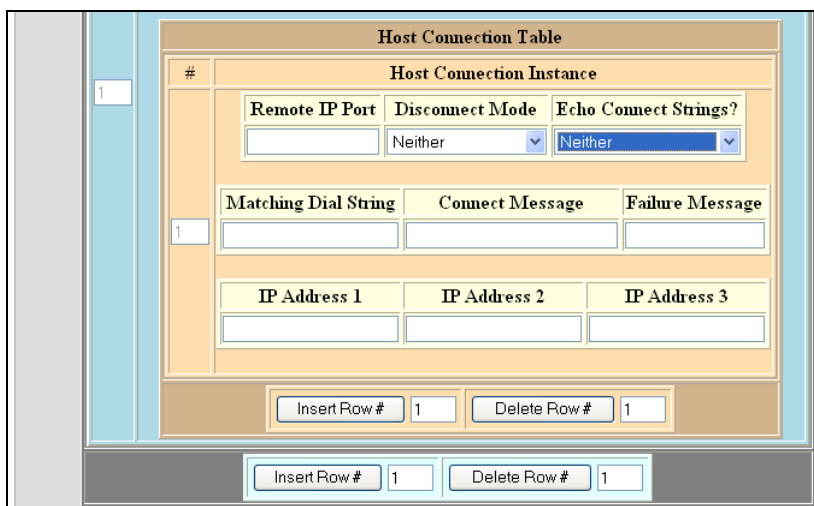
Note:

When adding or deleting rows of a *Host Connection Table*, make sure to click the **Insert Row#** or **Delete Row#** buttons within the brown section of the Terminal Client, not the buttons at the very bottom of the main table.

The following table lists the buttons available in the *Host Connection Table*.

BUTTON	EXPLANATION
Insert Row#	Each row of the <i>Host Connection Table</i> exists as a set of properties in a numbered table row within the Terminal Client configuration. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row must be filled in with all data required.
Delete Row#	In order to delete a row of the <i>Host Connection Table</i> , enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.

The following screen capture shows the *Host Connection Table*.



The following table lists the fields and options available for each row of the *Host Connection Table*. Multiple rows may be added if necessary:

FIELD/OPTION	EXPLANATION
Remote IP Port	Enter the port number (between 1 and 65535) to which the Terminal Client connects. The same port number is used to attempt connections to each of the three IP Addresses, if configured. There is no option to connect to different port numbers for each address in the Host Connection row.
Disconnect Mode	<p>Select when to disconnect from the remote address. In any case of a session disconnect, the <i>Connect Mode</i> (above) determines how a reconnection occurs.</p> <p>Options available are:</p> <p><i>On +++</i>: Disconnect if three characters +++ (and no more than three) are received on the serial port within the <i>Demark Time</i>. This emulates the modem attention string often used prior to hanging up a dial connection.</p> <p><i>On Dropped DCD</i>: Disconnect when the Data Carrier Detect (DCD) input on the serial port goes to a low (inactive) state.</p> <p><i>Either</i>: Disconnect either on receiving +++ at the serial port or on an inactive serial DCD line.</p> <p><i>Neither</i>: Never disconnect from the remote server. Connections may still be lost due to the remote side dropping its connection or due to network interruptions.</p>
Echo Connect Strings?	<p>Choose whether to echo all commands. The options are:</p> <p><i>To Async</i>: Echo the Connect Message and Failure Message to the serial port after a connection attempt or after the Terminal Client disconnects.</p> <p><i>To Async and Socket</i>: Echo the <i>Connect Message</i> and <i>Failure Message</i> to the serial port and to the remote server after a connection attempt or after the Terminal Client disconnects.</p> <p><i>Neither</i>: Do not echo the strings to the serial or TCP port.</p>
Matching Dial String	<p>Enter the ATDT string that is used to make a connection if the <i>Connect Mode</i> option is set to <i>ATDT</i> or <i>ATDT or DCD</i>. Otherwise, this field must be left empty.</p> <p>If used, the string must always start with the letters <i>ATDT</i> and be followed by some unique text (uppercase/lowercase text is treated identically, and spaces are ignored).</p> <p>For instance, the Host Connection rows may contain <i>Matching Dial Strings</i> of <i>ATDT1</i>, <i>ATDT555-1212</i>, <i>ATDIAL</i>. When any of these strings is received on the serial port, the ZyWAN attempts to connect to the first configured IP address of its Host Connection row.</p>
Connect Message	Enter a text message (such as "CONNECT") sent to the network and/or serial port when a network connection is established to the remote address. This text is only sent when the <i>Echo Connect Strings?</i> is set to something other than <i>Neither</i> . This option emulates a modem's option to echo a connect message to a dialing computer. This field may be left blank if no message is desired.

FIELD/OPTION	EXPLANATION
Failure Message	Enter a text message (such as “NO CARRIER”) sent to the network and/or serial port when the Terminal Client disconnects from a network connection and to the serial port when a connection attempt fails. This text is only sent when the <i>Echo Connect Strings?</i> is set to something other than <i>Neither</i> . This option emulates a modem’s option to echo a fail message to a dialing computer. This field may be left blank if no message is desired.
IP Address 1, IP Address 2, IP Address 3	Enter the IP address or fully qualified domain name (FQDN) to which the Terminal Client connects.

Chapter 9 Terminal Servers

The following screen capture shows the *Terminal Servers* tab.

The Terminal Server sets up a listening port for inbound TCP/IP connection, allowing communication directly to a local serial port.

After setting all the Terminal Server properties, click the **Submit New Configuration** button before switching to a new tab or closing the window.



Note:

Changes made to the *Terminal Server* page take effect immediately after submitting changes without requiring a reboot.

To allow one or more Terminal Server services to be configured, set *Enable Terminal Servers* to *Yes*. This makes the items shown in the following screen capture available in the *Table of Terminal Servers*.

The following table lists the buttons available in the *Table of Terminal Servers*.

BUTTON	EXPLANATION
Insert Row#	Each of the Terminal Servers exists as a large set of properties in a numbered table row. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row must be filled in with all data required.
Delete Row#	In order to delete a Terminal Server configuration (a row in the table), enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.

The following screen capture shows the *Table of Terminal Servers*.



Note:

Any Terminal Server (TCP) ports configured here must also be included in the “Open Ports” section of the *Networking* page, so the firewall will allow connections to be made to the ZyWAN.

The following table lists the fields and options that are available and that must be set for each configured Terminal Server configuration.

FIELD/OPTION	EXPLANATION
IP Port	Enter the IP port number (between 1 and 65535) to be used on the ZyWAN for incoming TCP/IP connections from a network client application. The IP address to which the client connects may be any valid address configured for the ZyWAN on any interface.
Time to Live	Enter the <i>Time To Live</i> for the connection (in seconds). This is the maximum time of no activity from the network-connected client, before the ZyWAN closes the Terminal Server connection. The range for <i>Time To Live</i> is 1 to 65535 seconds. (Setting the value to zero (0) will cause the Terminal Server to never shut down upon no activity, which is not recommended.)

FIELD/OPTION	EXPLANATION
Duplex	<p>Select the duplex mode for the Terminal Server. This selects a mode of operation for handling bi-directional communication with a serial device.</p> <p><i>Full Duplex:</i> This mode is designed for unsolicited data from serial devices, full bi-directional communication, or any serial protocol which may send large or multiple responses to a request. In this mode, the Terminal Server is always able to receive data on both the serial and network ports, as long as a client is connected to the <i>IP Port</i>.</p> <p><i>Half Duplex:</i> This mode is designed for simple request-response networks, especially where serial port sharing with another Terminal Server may be required. After a request is received from the network and sent to the serial port, one response is expected (with a number of bytes less than the <i>Buffer Size</i>). After data is transmitted to the serial port and the <i>Response Timer</i> times out with no data or after one response is received and returned to the network client, the Terminal Server does not read any more serial data until the next request.</p>
Modbus Mode	<p>Select the mode of operation, if Modbus protocol translation is required. Modbus protocol translation is only needed if the network client is sending "Open Modbus/IP" protocol requests. Translation is <u>not</u> needed for other types of data or if the standard serial Modbus (ASCII or RTU) is encapsulated within the TCP/IP requests. Options available are:</p> <p><i>None:</i> This is the normal option for most applications.</p> <p><i>Open Modbus to ASCII:</i> Converts Open Modbus/IP protocol requests to serial Modbus ASCII protocol, and converts the ASCII response to an Open Modbus/IP response.</p> <p><i>Open Modbus to RTU:</i> Converts Open Modbus/IP protocol requests to serial Modbus RTU (Binary) protocol, and converts the RTU response to an Open Modbus/IP response.</p>
Serial Driver	<p>Select whether to use the Native Linux (ttyS) serial driver or the ACSCOMM driver. The ACSCOMM allows for half-duplex RS-485 communication and can provide somewhat better handling of hardware flow control if required.</p>
Broadcast Only	<p>Select Yes to only send to the serial port. This option allows the network computer to send data to the serial port without waiting for a response. The <i>Response Timeout</i> and <i>Duplex</i> mode are ignored.</p>
Demark IP Packets	<p>If a large network packet is sent to the ZyWAN and gets broken up over the network, the fragments can sometimes arrive at slightly different times. Each packet is sent to the serial port, but if the time difference is too great, the serial device may not react properly. Set this value to Yes to allow delayed IP packets to be put together before sending to the serial port. The value for <i>Demark Timer</i> is used to specify the time to wait for additional IP data. Set this value to No if this feature is not needed.</p>
Echo Cancel RS-485	<p>This option is used when the internal (COM3) or an external RS-485 converter is used in half-duplex mode. Set this option to Yes to block the reception of echo bytes on the serial port which get echoed back from the RS-485 device.</p>

FIELD/OPTION	EXPLANATION
Print Server	This option is used when the Terminal Server is used as a print server to a serial printer. Setting this option to Yes causes the Terminal Server to operate in <i>Print Server</i> mode. The Terminal Server absorbs as much IP data as it can within the available memory and sends data to the serial port until it is all delivered, regardless of whether the host disconnects. When this option is set to No (default mode), if a host disconnects and data is still in the Terminal Server buffer, the remaining data is discarded and will <u>not</u> be sent to the serial port.
Number of Servers	Enter the number of simultaneous clients which can connect to this Terminal Server simultaneously. Values must be between 1 and 8. If this is set to 1, the Terminal Server is <u>pre-emptive</u> . This means that if a second client connects to the port, an already-connected client is disconnected. With <i>Number of Servers</i> set to 2 or greater, any further connections are blocked when the number of simultaneous connections have been made.
Password	Enter a non-blank field as a password for the Terminal Server, if desired. The password must be no longer than 15 characters. When this is set, making a connection to the Terminal Server port returns a prompt for 'Password'. If the correct password (case-sensitive) is not entered within a minute, the connection is dropped.
Buffer Size	Enter the maximum number of bytes (between 1 and 4095) which are allowed in a response to a network client. (The actual number of bytes sent may be less if the <i>Demark</i> timer times out before the serial buffer is full.)
Demark Timer	Enter the maximum time (in milliseconds, between 10 and 30000) the ZyWAN waits for inactivity on the serial port before sending a response to the network client, if at least one byte has been received.
Response Timeout	This option only applies if the <i>Duplex</i> option is set to <i>Half Duplex</i> . Otherwise, this field is ignored. Enter the <i>Response Timeout</i> (in milliseconds, between 10 and 30000). For simple request-response networks (half-duplex), the request from a network client is sent to the serial port. If no serial response is received within the <i>Response Timeout</i> , the Terminal Server does not read any more serial data until the next request and the serial port is released.

Serial Ports Table

The *Serial Ports Table* is part of the Terminal Server configuration as shown in the following screen capture.

#	COM Port	Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
1	- Select -	115200	8	None	1	None

Insert Row # 1 Delete Row # 1

Insert Row # 1 Delete Row # 1

At least one row must be configured in the *Serial Ports Table* for it to work properly.


**Note:**

When adding or deleting rows of a *Serial Ports Table*, make sure to click the **Insert Row#** or **Delete Row#** buttons within the brown section of the *Serial Ports Table*, not the buttons at the very bottom of the main table.

The following table lists the buttons available in the *Serial Ports Table*.

BUTTON	EXPLANATION
Insert Row#	Each row of the <i>Serial Ports Table</i> contains the definition of a serial port to use for this Terminal Server configuration. One Terminal Server may send data received from the network client to multiple serial ports simultaneously. In order to insert a row in the table, enter a number in the box between 1 and one greater than the highest number of rows. Then click the Insert Row# button to insert a blank row. This row must be filled in with all data required.
Delete Row#	In order to delete a row of the <i>Serial Ports Table</i> , enter a number in the box between 1 and the highest number of rows. Then click the Delete Row# button to delete the row. Once a row is deleted, it cannot be restored without inserting a row and entering the data again.

The following table lists the options available for the *Serial Ports Table*. At least one row of the *Serial Ports Table* is required for the Terminal Server to operate.

FIELD/OPTION	EXPLANATION
COM Port	<p>Select the serial COM port to which the Terminal Server data is sent.</p> <hr/> <p>Important: Make sure this COM port is not configured for another service in the ZyWAN. Otherwise, both services may conflict for the port and not operate correctly.</p> <p> It is possible in some applications to configure two Terminal Servers to use the same COM port. In order for this to work, the <i>Demark</i> option must be set to <i>Half Duplex</i> or <i>Broadcast</i>. In <i>Half Duplex</i> mode, the clients connecting to each port may need to wait much longer for a response, since the <i>Demark</i> and <i>Response Timeout</i> times for all connections are observed, in the order that the requests are received from each client.</p> <hr/>
Baud Rate	Select the baud rate to use for the Terminal Server port. Baud rate options range from 1200 to 115,200 bps.
Data Bits	Select the number of data bits to use for the Terminal Server port. Options are 5, 6, 7, and 8.
Parity	Select the parity to use for the Terminal Server port. Options are <i>None</i> , <i>Odd</i> , <i>Even</i> , <i>Mark</i> , <i>Space</i> .
Stop Bits	Select the number of stop bits to use for the Terminal Server port. Options are 1, 1.5, and 2.
Flow Control	Select whether to use hardware flow control for the Terminal Server port. Options are <i>None</i> , and <i>RTS/CTS</i> (hardware flow control).

Chapter 10 Update

The following screen capture shows the *Update* tab.

The *Update* tab on the Web interface provides one method to update the ZyWAN firmware to a later version. See the following section, [Updating Using WinSCP](#) on page 106, for a more recommended method of updating, especially for systems where the default network is a cellular or private network.

Warning:

The update process may take a significant amount of time, possibly several minutes, depending on the size and number of updates that have to occur. Do not remove power or perform a Linux command line 'reboot' until the updates have completed.



In some cases, the ZyWAN will be required to reboot automatically in the middle of its update process. If this occurs, it will continue installing additional files after the reboot. When this occurs, the following line will be seen on a serial console after the intermediate reboot:

```
**** more updates available ****
```

Updating Via the Web Interface

In the *Update URL* field, enter the network address URL (Uniform Resource Locator) from which an update file may be downloaded. The address must be accessible through the default network interface of the ZyWAN and must point to a file server location containing update files for the ZyWAN. Some examples of addresses which could be used are:

<code>http://files.arcom.com/Zywan/updates</code>	(HTTP download over the Internet)
<code>http://<i>ip_address</i>/<i>pathname</i></code>	(HTTP download from <i>ip_address</i> which must be an HTTP server, with the files existing in <i>pathname</i>)
<code>--ftp-user=<i>username</i> --ftp-password=<i>password</i> ftp://ip_address/somepath</code>	(for FTP download from <i>ip_address/somepath</i> , using <i>username</i> and <i>password</i>)

The server location must contain the latest versions of the files, such as:

<code>version_multi.txt</code>	
<code>version_multi2.txt</code>	
<code>Zywan-update-1_<i>x</i>.star</code>	(where files for versions 1.5 and higher would be required to update a version 1.4 ZyWAN)
or <code>Zywan-update_v1.<i>xx</i>.star</code>	

If no *Update URL* is entered, the ZyWAN will use the default address of <http://files.arcom.com/Zywan/updates>. When the **Update Zywan** button is pressed, the files are downloaded and installed. After the update is complete, the ZyWAN must be rebooted.

Updating Using WinSCP

Several of the version updates for ZyWAN are fairly large. For this reason, it may not be recommended to use the Web interface described above because of the cost or length of time it requires to load files over the cellular network. The following method describes how to load the ZyWAN update files locally over Ethernet or WiFi and to install them manually.

See the section [SFTP/SCP Client \(WinSCP\)](#) on page 27 for information on installing the WinSCP file transfer program. This program provides a free and secure means of loading the required files, although other programs may be used which support the SFTP or SCP protocols.

Determine the current software revision by viewing the *Status* tab of the ZyWAN Web configuration page. The following screen capture shows an example indicating a ZyWAN at software revision level 1.4.

Cellular		Ethernet		Wifi		Networking		GPS		Terminal Clients		Terminal Servers		Status		Update		Security	
Full Hardware Model: ZyWAN-1000																			
Current software version: 1.4																			
Hardware Model: none																			
GPS Yes <input type="radio"/> No <input type="radio"/>																			
802.11B Yes <input type="radio"/> No <input type="radio"/>																			
Last COM Port: COM3																			
COM3 Type: RS232																			

The required files can be obtained upon request from Eurotech, or they may be downloaded from <http://files.arcom.com/Zywan/updates/>. From this Web site, choose the update file “Zywan-1.xto1.yupdate.tar” as mentioned next, depending on what version from which the ZyWAN is starting.

File Name	File Size
version_multi.txt	404
version_multi2.txt	150
Zywan-1.0to1.2update.tar	177664
Zywan-1.2to1.5update.tar	4587008
Zywan-1.4to1.5update.tar	4001792
Zywan-1.5to1.7update.tar	6411776
Zywan-update-1_1.star	161909
Zywan-update-1_2.star	11897
Zywan-update-1_3.star	13249
Zywan-update-1_4.star	570754
Zywan-update-1_5.star	3999057
Zywan-update_v1.06.star	9730
Zywan-update_v1.07.star	6398044

Starting with versions 1.2 through 1.4

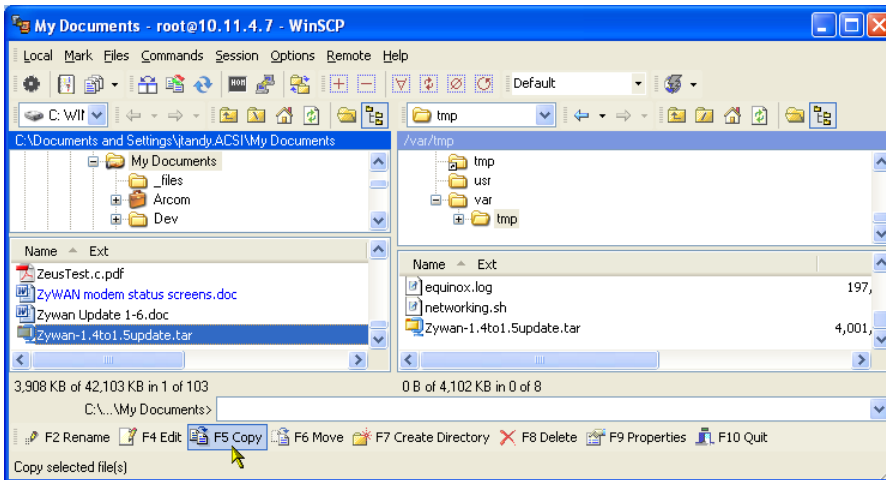
If the ZyWAN is currently at version 1.2, the following file is needed:

Zywan-1.2to1.5update.tar

If the ZyWAN is currently at version 1.4, the following file is needed:

Zywan-1.4to1.5update.tar

Use WinSCP to connect to the ZyWAN, and browse to its `/tmp/` (or `/var/tmp/`) folder. Download the “Zywan-1.xto1.yupdate.tar” file to the ZyWAN as shown in the following screen capture.

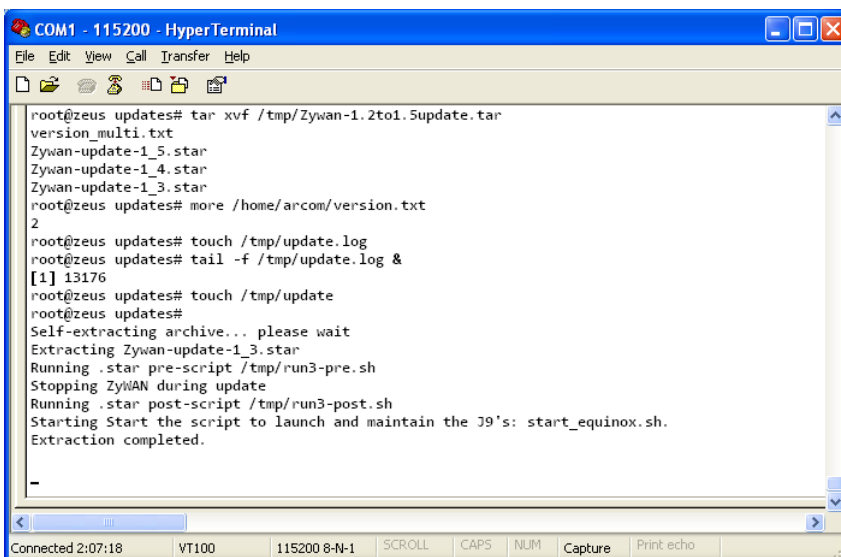


After the files are loaded, connect to the ZyWAN using either HyperTerminal on the COM1 diagnostics port or over the network using PuTTY (or another SSH application). See the section [Setting Up Software](#) on page 25, for help setting up HyperTerminal or PuTTY.

From the ZyWAN command line, issue the following commands:

```
cd /var/www/updates
tar xvf /tmp/Zywan-1.2to1.5update.tar
or
tar xvf /tmp/Zywan-1.4to1.5update.tar
touch /tmp/update.log
tail -f /tmp/update.log &          (Notice the ampersand '&' at the end.)
touch /tmp/update
```

A series of diagnostic messages will be displayed, ending with a system reboot. If updating from version 1.2, there will also be a reboot after completing the 1.4 update. The following screen captures show these messages.



```

COM1 - 115200 - HyperTerminal
File Edit View Call Transfer Help

Setting up libracoon0 (0.7-2) ...
Setting up linux-image-2.6.16.28-arcom2-1-zeus (2.6.16.28-2) ...
Setting up net-tools (1.60-1) ...
Setting up openssl (0.9.7g-1) ...
Setting up pptpd (1.3.4-1) ...
Setting up pump (0.8.19-5) ...
Setting up racoon (0.7-2) ...
Setting up stunnel (4.07-1) ...
Setting up usbutils (0.72-1) ...
Running .star post-script /tmp/postinst_script.sh
Starting SSL tunnels: [started: /etc/stunnel/stunnel.conf] stunnel.
mv: unable to rename '/etc/udhcpd*': No such file or directory
Please wait while system reboots.
Extraction completed.

Reboot required after s/w update

Broadcast message from root (Tue Mar 31 18:00:39 2009):

The system is going down for reboot NOW!
INIT: Sending processes the TERM signal
INIT: SendingStopping portmap daemon: portmap.

Connected 2:21:53  VT100  115200 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo

```

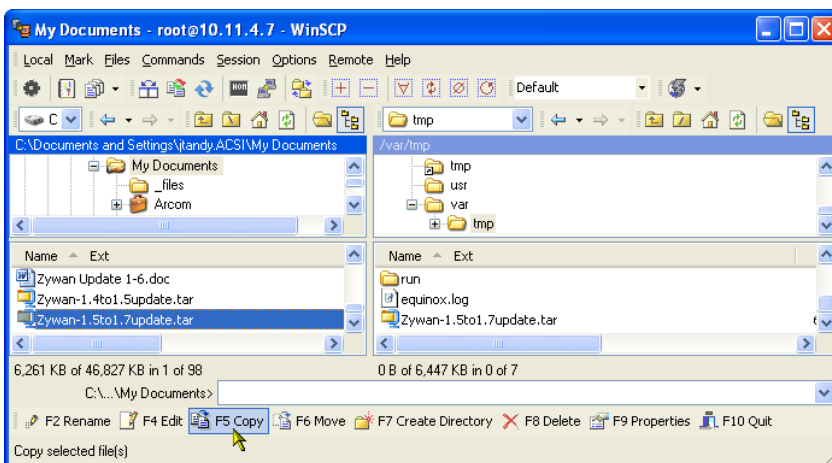
Once the reboot (or reboots) are finished, the system has been updated to version 1.5. This can be verified on the Web configuration page or by typing the command `cat /home/arcom/version.txt` (the response should be '5'). Proceed to the next section in order to install further updates.

Starting with version 1.5

If the ZyWAN is currently at version 1.5, the following file is needed:

`Zywan-1.5to1.7update.tar`

Use WinSCP to connect to the ZyWAN, and browse to its `/tmp/` (or `/var/tmp/`) folder. Download the “Zywan-1.5to1.7update.tar” file to the ZyWAN as shown in the following screen capture.



After the files are loaded, connect to the ZyWAN using either HyperTerminal on the COM1 diagnostics port or over the network using PuTTY (or another SSH application). See the section [Setting Up Software](#) on page 25, for help setting up HyperTerminal or PuTTY.

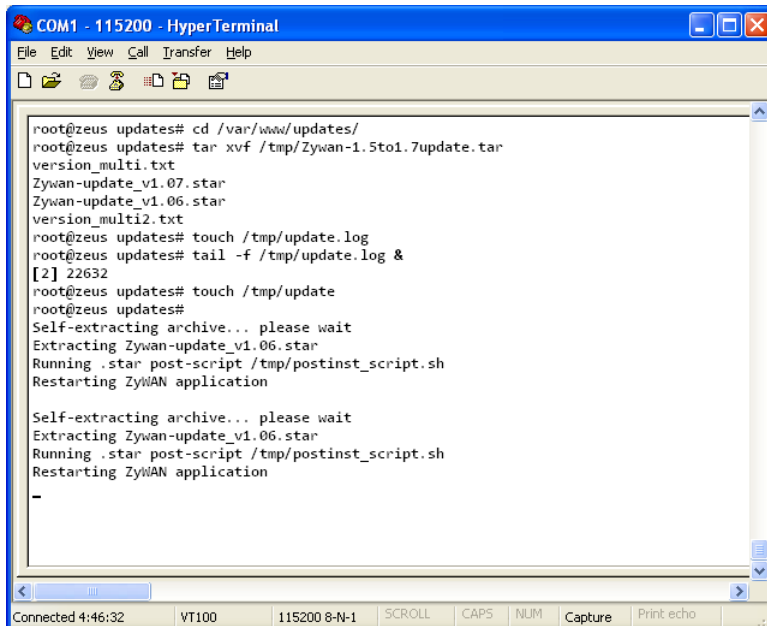
From the ZyWAN command line, issue the following commands:

```

cd /var/www/updates
tar xvf /tmp/Zywan-1.5to1.7update.tar
touch /tmp/update.log
tail -f /tmp/update.log &          (Notice the ampersand '&' at the end.)
touch /tmp/update

```

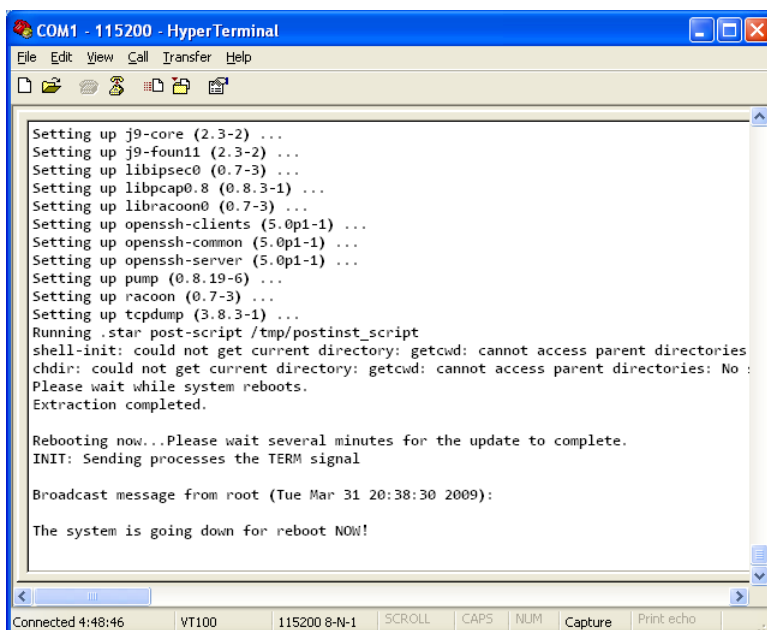
A series of diagnostic messages will be displayed, ending with a system reboot. The following screen captures show these messages.



```
COM1 - 115200 - HyperTerminal
File Edit View Call Transfer Help

root@zeus updates# cd /var/www/updates/
root@zeus updates# tar xvf /tmp/Zywan-1.5to1.7update.tar
version_multi.txt
Zywan-update_v1.07.star
Zywan-update_v1.06.star
version_multi2.txt
root@zeus updates# touch /tmp/update.log
root@zeus updates# tail -f /tmp/update.log &
[2] 22632
root@zeus updates# touch /tmp/update
root@zeus updates#
Self-extracting archive... please wait
Extracting Zywan-update_v1.06.star
Running .star post-script /tmp/postinst_script.sh
Restarting ZyWAN application

Self-extracting archive... please wait
Extracting Zywan-update_v1.06.star
Running .star post-script /tmp/postinst_script.sh
Restarting ZyWAN application
-
```



```
COM1 - 115200 - HyperTerminal
File Edit View Call Transfer Help

Setting up j9-core (2.3-2) ...
Setting up j9-foun11 (2.3-2) ...
Setting up libipsec0 (0.7-3) ...
Setting up libpcap0.8 (0.8.3-1) ...
Setting up libraccoon0 (0.7-3) ...
Setting up openssh-clients (5.0p1-1) ...
Setting up openssh-common (5.0p1-1) ...
Setting up openssh-server (5.0p1-1) ...
Setting up pump (0.8.19-6) ...
Setting up racoon (0.7-3) ...
Setting up tcpdump (3.8.3-1) ...
Running .star post-script /tmp/postinst_script
shell-init: could not get current directory: getcwd: cannot access parent directories
chdir: could not get current directory: getcwd: cannot access parent directories: No :
Please wait while system reboots.
Extraction completed.

Rebooting now...Please wait several minutes for the update to complete.
INIT: Sending processes the TERM signal

Broadcast message from root (Tue Mar 31 20:38:30 2009):

The system is going down for reboot NOW!
```

Once the reboot has finished, the system has been updated to version 1.7. This can be verified on the Web configuration page or by typing the command `cat /home/arcom/version.txt`. (The response should be '7'.)

Chapter 11 Security

The following screen capture shows the *Security* tab.

ZyWAN Setup

Cellular | Ethernet | Wifi | Networking | GPS | Terminal Clients | Terminal Servers | Status | Update | **Security**

Current Username:

Current Password:

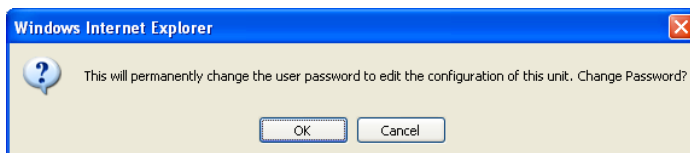
New Username:

New Password:

The *Security* tab provides an option to change the ZyWAN Web configuration password. The following table lists the fields available in this tab.

FIELD/OPTION	EXPLANATION
Current Username	Enter the current username for logging into the Web configuration page.
Current Password	Enter the current password.
New Username	Enter a new username for logging into the Web configuration page.
New Password	Enter a new password.

After entering these values, click the **Change Web Password** button. A prompt will confirm whether to change the password, as shown in the following screen capture.



If the current username and password have been entered correctly, a confirmation will be displayed, as shown in the following screen capture.

Password Change Confirmation

Result:

```
old user name: arcom
old password: arcom
new user name: new
new password: new
Password changed
```

Otherwise, a negative confirmation will indicate that the change password operation was not successful. The following screen capture illustrates this case.

Password Change Confirmation

Reboot with New Settings

Make More Changes

Result:

Username/password entered do not match
those stored
Please try again
Password NOT changed

Chapter 12 Backing Up Configurations

The Web configuration page is the main way to implement configuration changes on the ZyWAN. However, it may be useful to be able to copy configuration files from the ZyWAN, either to install on a multiple devices or to save for archive purposes. This section describes the process of retrieving configuration files from the ZyWAN and loading them onto a different ZyWAN.

Saving Configuration Files

Once the configurations have been set and tested on a ZyWAN, log on to the administrative account (typically 'root') using either Windows HyperTerminal or PuTTY. See the section [Setting Up Software](#) on page 25, for help setting up HyperTerminal or PuTTY.

Issue the following commands, observing the two uppercase 'C' on 'ConfigChanged':

```
cp /var/www/props/*.properties /tmp
cd /tmp
chown nobody *.properties
chgrp nobody *.properties
sed -i s/ConfigChanged=false/ConfigChanged=true/ *.properties
sed -i s/reboot=false/reboot=true/ reboot.properties
```

After the files have been copied and modified as described previously, they can be packaged up with the following command:

```
tar cvf /tmp/config.tar *.properties
```

This will create a file /tmp/config.tar that contains all the unit property files, which are all the properties set through the Web configuration page. Use WinSCP to upload this file from the ZyWAN to a computer. This file can be stored for archiving purposes or for transfer to a different device.

Restoring Configuration Files

In order to load these .properties files to another ZyWAN, copy the file config.tar to the /tmp/ directory. Then issue the following command:

```
tar xvf /tmp/config.tar -C /var/www/props
```

This will extract the files and install the new configuration. The modified reboot.properties file will cause the ZyWAN to reboot automatically. After the reboot, it should have the same configuration as the original device from which the configuration was taken. If there are unit-specific configuration changes (such as IP addresses, WiFi information, ActSoft/Arcom GPS unit names, etc.), these must be configured at this time.

PART 3: CONFIGURATION EXAMPLES

Introduction

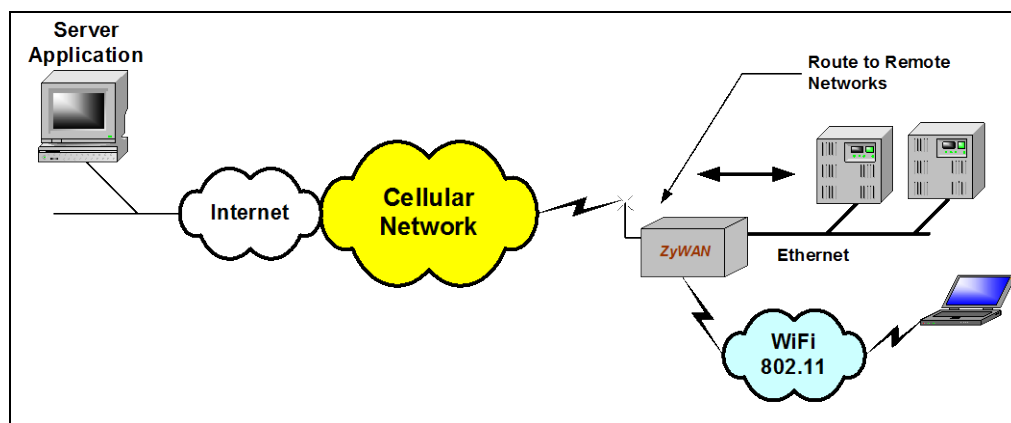
This section provides examples of a few common ways the ZyWAN can be configured to achieve various custom applications. Detailed information is given for each configuration example. These examples illustrate some of the basic ZyWAN features. The actual implementation may vary with customer requirements.

The configurations described in this section are only a subset of the functionality of the ZyWAN. Many other configurations are possible that are not represented by the examples included in this section.

Configuration Example 1: Network Router

The Network Router configuration example illustrates the following features of the ZyWAN:

- Cellular Internet connection
- Local Ethernet LAN connection
- Wireless (WiFi) 802.11b network connection (access point)
- Allowing Ethernet or WiFi devices on the network to connect to the Internet via cellular, using the ZyWAN as a gateway (NAT)



The following table lists the network settings used in this example.

SETTING	DETAILS
Cellular	The DNS servers passed to other computer will be obtained from the cellular network.
Ethernet (eth0)	192.168.1.1, subnet 255.255.255.0 ZyWAN will be the default gateway and DNS server to devices on its Ethernet network, assigning them addresses 192.168.1.10 through 192.168.1.200.
WiFi (wlan0)	192.168.3.1, subnet 255.255.255.0 WiFi will act as an access point ("master" mode) with SSID 'zywan'. ZyWAN will be the default gateway and DNS server to devices on the WiFi network, assigning them addresses 192.168.3.10 through 192.168.3.200.
Networking	UDP ports 67 and 53 (DHCP and DNS) are allowed in the ZyWAN firewall, and NAT is configured for eth0 and wlan0.

The next sections provide detailed descriptions including Web configuration pages for each setting.

Cellular Setup


The cellular page will depend on the model of ZyWAN and the network provider.

Ethernet Setup

Do not configure the Default Gateway and DNS Server addresses because these addresses will override the cellular network. If configured, the Default Gateway address will be the ZyWAN's default route, and the ZyWAN will obtain its public DNS servers from that network.

The following screen capture shows the *Ethernet* configuration page.

ZyWAN Setup


A MEMBER OF EUROTECH GROUP

Cellular

Ethernet

Wifi

Networking

GPS

Terminal Clients

Terminal Servers

Status

Update

Security

Enable Eth0? Yes ☒ No ☐

Use Dhcp? Yes ☐ No ☒

Network Interface - eth0				
IP Address	192	168	1	1
Subnet Mask	255	255	255	0
Default Gateway				
Preferred DNS Server				
Alternate DNS Server				

Run Dhcp Server: Yes ☒ No ☐

DHCP Server Configuration				
Default Lease Time	7200			
Subnet Mask	255	255	255	0
Range From	192	168	1	10
Range To	192	168	1	200
Pass DNS servers to DHCP clients	Yes <input checked="" type="radio"/> No <input type="radio"/>			

Enable Eth1? Yes ☐ No ☒


Submit New Configuration

WiFi Setup

Do not configure the Default Gateway or DNS Server addresses because these addresses will override the cellular network. If configured, the Default Gateway address will be the ZyWAN's default route, and the ZyWAN will obtain its public DNS servers from that network. The WEP/WPA encryption password is optional.

The following screen capture shows the *WiFi* configuration page.

ZyWAN Setup


A MEMBER OF EUROTECH GROUP

CellularEthernet**Wifi**NetworkingGPSTerminal ClientsTerminal ServersStatusUpdateSecurity

Mode: master

Network Interface - wifi

IP Address	192	168	3	1
Subnet Mask	255	255	255	0
Default Gateway				
Preferred DNS Server				
Alternate DNS Server				

Run DHCP Server? Yes ☒ No ☐

DHCP Server Configuration

Default Lease Time	7200			
Subnet Mask	255	255	255	0
Range From	192	168	3	10
Range To	192	168	3	200
Pass DNS servers to DHCP clients	Yes <input checked="" type="radio"/> No <input type="radio"/>			

SSID: zywan

Channel: 7 - 2.442 GHz

Use Encryption? Yes ☒ No ☐

Encryption Type: WEP ☒ WPA ☐

Key: passw

Submit New Configuration

Networking Setup

Port 67 (UDP) is required for the ZyWAN to act as a Default Gateway to other devices, and port 53 (UDP) is required for it to act as a DNS server. The NAT entries allow devices on each network to route through the ZyWAN to reach the cellular network (ppp0 interface).

The following screen capture shows portions of the *Networking* configuration page.

Open Ports? Yes ☒ No ☐

Open Ports Table						
#	Open Ports Instance					
1	Inbound Port		Protocol			
	67		UDP			
--Optional--						
Permitted Source Port Range						
From Port			To Port			
Permitted External Network		Permitted External Network Mask		Permitted MAC Address		
2	Inbound Port		Protocol			
	53		UDP			
--Optional--						
Permitted Source Port Range						
From Port			To Port			
Permitted External Network		Permitted External Network Mask		Permitted MAC Address		
Insert Row # <input type="text" value="1"/> Delete Row # <input type="text" value="3"/>						

Enable Port Forwarding? Yes ☐ No ☒

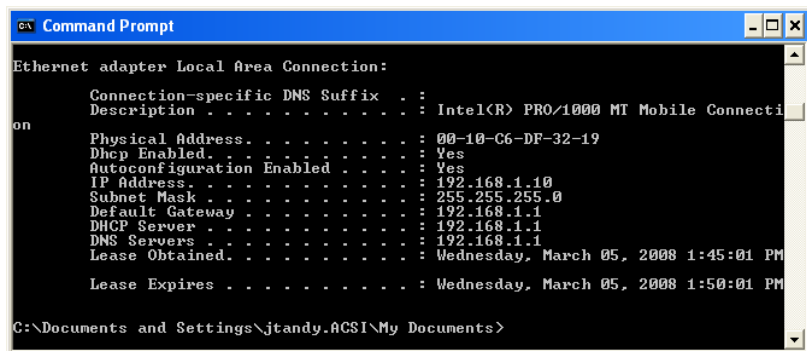
Enable NAT? Yes ☒ No ☐

NAT Table											
#	Source Network/Address				Source Netmask				Source Interface	Destination Interface	Masquerade
1	192	168	1	0	255	255	255	0	eth0	ppp0	Yes <input checked="" type="radio"/> No <input type="radio"/>
2	192	168	3	0	255	255	255	0	wlan0	ppp0	Yes <input checked="" type="radio"/> No <input type="radio"/>
Insert Row # <input type="text" value="1"/> Delete Row # <input type="text" value="1"/>											

Checking Out Example 1

The following screen captures show diagnostic information on checking the operation of this Network Router configuration. A computer is connected to the Ethernet 0 port on the ZyWAN and is set to automatically obtain an IP address and DNS. The screen captures show the output of “ipconfig /all” on a computer running the Windows operating system.

The computer has obtained its address (192.168.1.10) from the ZyWAN, and the ZyWAN is its Default Gateway, DHCP Server, and DNS Server.



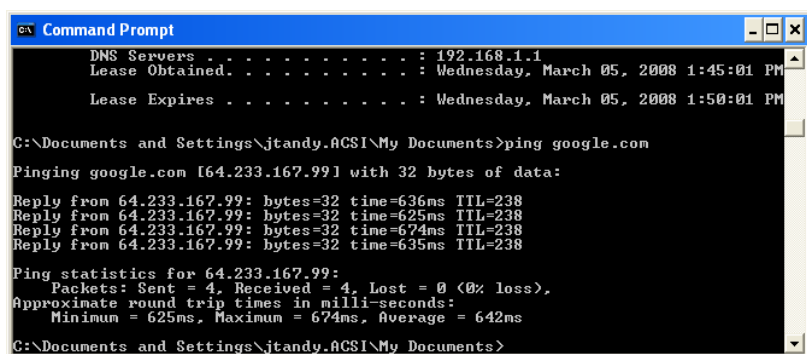
```
Command Prompt

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) PRO/1000 MT Mobile Connecti
on
    Physical Address. . . . . : 00-10-C6-DF-32-19
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
    Lease Obtained. . . . . : Wednesday, March 05, 2008 1:45:01 PM
    Lease Expires . . . . . : Wednesday, March 05, 2008 1:50:01 PM

C:\Documents and Settings\jtandy.ACSI\My Documents>
```

The computer can ping google.com, using the public cellular network both to resolve the URL with DNS and to route the network traffic between eth0 and ppp0. The same can be done by connecting the computer to the ZyWAN using the WiFi interface.



```
Command Prompt

    DNS Servers . . . . . : 192.168.1.1
    Lease Obtained. . . . . : Wednesday, March 05, 2008 1:45:01 PM
    Lease Expires . . . . . : Wednesday, March 05, 2008 1:50:01 PM

C:\Documents and Settings\jtandy.ACSI\My Documents>ping google.com

Pinging google.com [64.233.167.99] with 32 bytes of data:

Reply from 64.233.167.99: bytes=32 time=636ms TTL=238
Reply from 64.233.167.99: bytes=32 time=625ms TTL=238
Reply from 64.233.167.99: bytes=32 time=674ms TTL=238
Reply from 64.233.167.99: bytes=32 time=635ms TTL=238

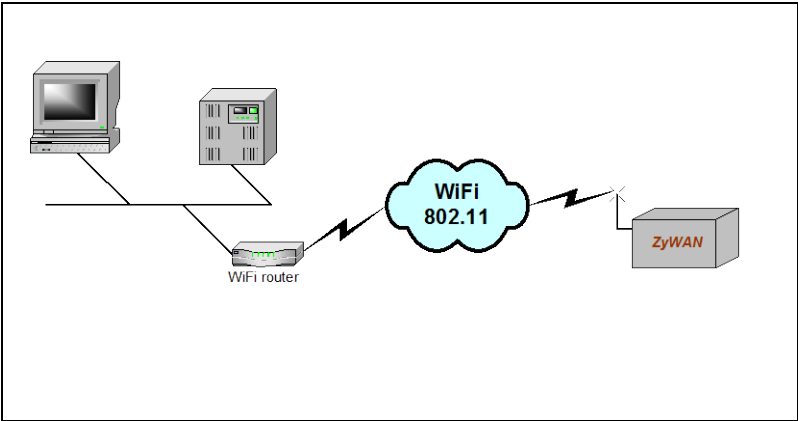
Ping statistics for 64.233.167.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 625ms, Maximum = 674ms, Average = 642ms

C:\Documents and Settings\jtandy.ACSI\My Documents>
```

Configuration Example 2: WiFi Client

The WiFi Client configuration example illustrates the following features of the ZyWAN:

- Ability of the ZyWAN to connect to a WiFi network using an access point or wireless router



The following table lists the network settings used in this example, which is only a partial configuration to illustrate the WiFi network.

SETTING	DETAILS
WiFi (wlan0)	ZyWAN is a client on a host network using a wireless access point, using static IP addressing. WiFi in managed mode may use DHCP instead to automatically acquire an address from the host network. A WEP password may also be configured (currently WPA is not supported).

The next section provides a detailed description including the Web configuration page for this setting.

WiFi Setup

In this example, the ZyWAN network address is configured to 10.41.32.20, with network settings to match the host network (subnet 255.255.0.0, default gateway 10.41.30.1, DNS server 10.41.30.2). The access point has the SSID name 'wirelesshub', and the frequency is set to channel 7.

Cellular

Ethernet

Wifi

Networking

GPS

Terminal Clients

Mode:

managed

Use Dhcp?

Yes

No

Network Interface - wifi

IP Address	10	41	32	20
Subnet Mask	255	255	0	0
Default Gateway	10	41	30	1
Preferred DNS Server	10	41	30	2
Alternate DNS Server				

SSID:

wirelesshub

Channel:

7 - 2.442 GHz

Use Encryption?

Yes

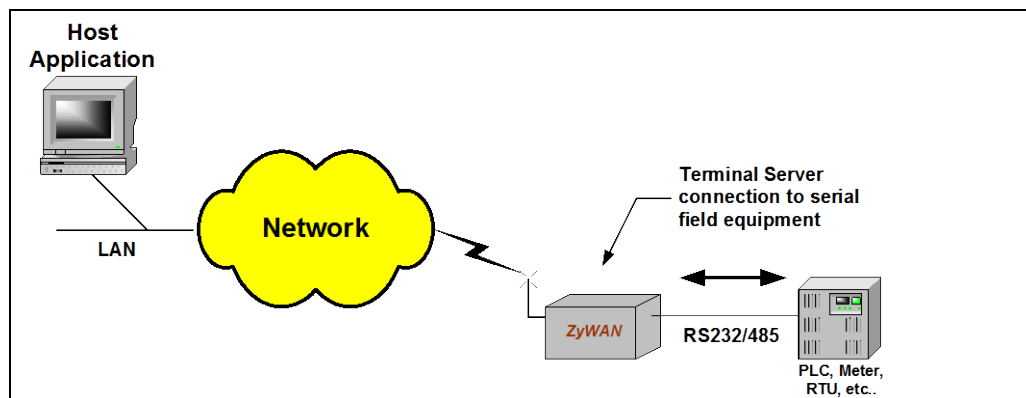
No

Submit New Configuration

Configuration Example 3: Terminal Server

The Terminal Server configuration example illustrates the following features of the ZyWAN:

- Terminal Server for IP to serial conversion, allowing host applications to communicate with a local serial device



The following table lists the network settings used in this example, which is only a partial configuration to illustrate the Terminal Server network.

SETTING	DETAILS
Terminal Server	IP port 4000 will be set up as a Terminal Server, which will redirect data to the COM2 port.
Networking	Open port 4000 in ZyWAN firewall. This must be included explicitly in <i>Networking</i> for any Terminal Server port configured.

The next sections provide detailed descriptions including the Web configuration pages for each setting.

Terminal Server Setup

This Terminal Server configuration uses “Full Duplex” mode, which allows full bi-directional communication. This example also shows the use of COM2 (RS-232) at a baud rate of 19,200, which must be set correctly for the application. If RS-485 is needed (on an appropriate model of ZyWAN), use COM3 with “Flow Control” set to *RTS/CTS* and “Echo cancel RS485” set to Yes. See [Terminal Servers](#) on page 100 for more details on other Terminal Server options.

The following screen capture shows the *Terminal Servers* configuration page.

Cellular Ethernet Wifi Networking GPS Terminal Clients Terminal Servers Status Update Security

Enable Terminal Servers: Yes ☒ No ☐

Table of Terminal Servers					
#	Terminal Server Instance				
	IP Port	Time to Live	Duplex	Modbus Mode	Serial Driver
1	4000	30	Full Duplex	None	Native Linux

Demark IP Packets: Yes ☒ No ☐
 Echo cancel RS485: Yes ☒ No ☐
 Print Server: Yes ☒ No ☐

Number of Servers: 4
 Password:
 Buffer Size: 100
 Demark Timer: 100
 Response Timeout: 1000

Serial Ports Table						
#	COM Port	Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
1	COM2	19200	8	None	1	None

Insert Row # 1 Delete Row # 1

Insert Row # 1 Delete Row # 1

Networking Setup

Port 4000 (TCP) must be opened in the firewall to allow external connections to be made to the Terminal Server.

The following screen capture shows the *Networking* configuration page.

Cellular Ethernet Wifi Networking GPS Terminal Clients Terminal Servers Status Update Security

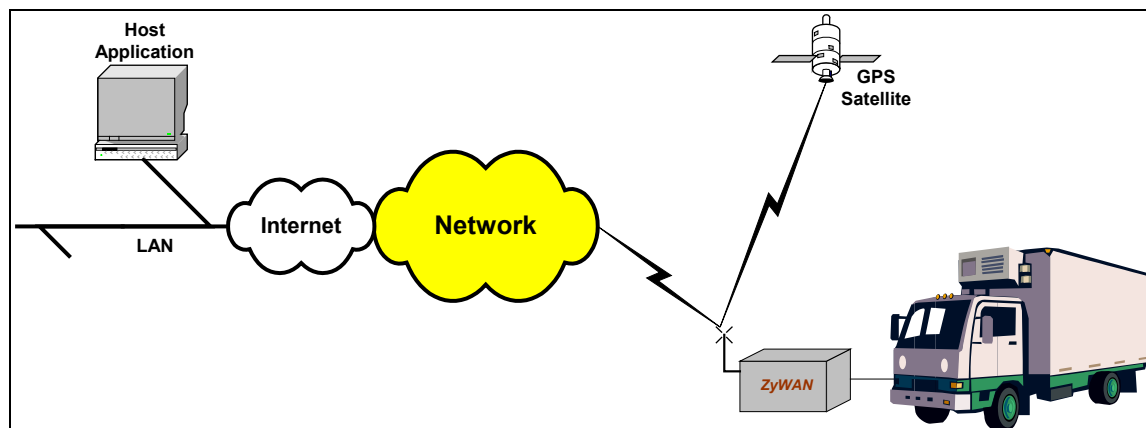
Open Ports? Yes ☒ No ☐

Open Ports Table																	
#	Open Ports Instance																
1	<table border="1"> <tr> <th>Inbound Port</th> <th>Protocol</th> </tr> <tr> <td>4000</td> <td>TCP</td> </tr> </table> <p>--Optional--</p> <table border="1"> <tr> <th colspan="2">Permitted Source Port Range</th> </tr> <tr> <th>From Port</th> <th>To Port</th> </tr> <tr> <td></td> <td></td> </tr> </table> <table border="1"> <tr> <th>Permitted External Network</th> <th>Permitted External Network Mask</th> <th>Permitted MAC Address</th> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Inbound Port	Protocol	4000	TCP	Permitted Source Port Range		From Port	To Port			Permitted External Network	Permitted External Network Mask	Permitted MAC Address			
Inbound Port	Protocol																
4000	TCP																
Permitted Source Port Range																	
From Port	To Port																
Permitted External Network	Permitted External Network Mask	Permitted MAC Address															

Configuration Example 4: GPS interface

The GPS Interface configuration example illustrates the following features of the ZyWAN:

- Remotely obtaining the GPS location of a mobile ZyWAN
- Communicating the position of the ZyWAN to serial field equipment



The following table lists the network settings used in this example.

SETTING	DETAILS
Cellular	This example uses the cellular network to transmit GPS locations to a remote server.
GPS	GPS data is obtained from the GPS module (on appropriate model of ZyWAN). This data is sent automatically to a remote network server and is available via Terminal Server connection to the ZyWAN.
Networking	Networking configuration allows access to GPS Terminal Server port.

The next sections provide detailed descriptions including the Web configuration pages for each setting.

Cellular Setup

The cellular page will depend on the model of ZyWAN and the network provider. The inbound TCP connection to obtain GPS data requires the cellular account to have a static, public IP address.

GPS Setup

The GPS Terminal Server allows incoming TCP connections to be made to the ZyWAN to obtain raw NMEA data from the GPS module. The desired NMEA messages may be enabled. This NMEA data may also be sent to a local COM port.

The ActSoft or Arcom format UDP option allows the ZyWAN to send formatted GPS reports on a regular basis to an external server.

The following screen capture shows the *GPS* configuration page.

The screenshot shows the 'GPS' configuration tab. It includes options for forwarding GPS to a physical COM port, enabling a GPS terminal server, and configuring various NMEA sentences (GPGLL, GPGGA, GPVTG, GPRMC, GPGSA, GPGSV, PFST,FOM). It also features a dropdown for 'GPS UDP MessageFormats?' set to 'ActSoft Format'. At the bottom, there are fields for 'Server IP Address' (gps.cometracker.com), 'Server Port Number' (8502), 'Request Interval' (60), 'Send Threshold' (1), and 'Unit ID' (TEST123456). A 'Submit New Configuration' button is at the bottom left.

Networking Setup

The portions of the *Networking* configuration page shown are used to enable inbound connections to the Terminal Server port 5000 (TCP). The NTP setting allows the ZyWAN to obtain the correct system time, so GPS reports sent with UDP will contain the correct timestamp.

The screenshot shows the 'Networking' configuration tab. It includes an 'Open Ports?' section with a 'Yes' radio button selected. Below this is an 'Open Ports Table' with one instance. The instance has an 'Inbound Port' of 5000 and a 'Protocol' of TCP. There are optional fields for 'Permitted Source Port Range' (From Port and To Port) and 'Permitted External Network' (Network, Network Mask, and MAC Address). Below the table is a 'Time Synchronization' section with a dropdown set to 'NTP'. It includes a list of NTP servers with one entry: 'pool.ntp.org'. There are buttons for 'Insert Row #' and 'Delete Row #' both set to 1. A 'Submit New Configuration' button is at the bottom left.

#	Open Ports Instance																
1	<table border="1"> <thead> <tr> <th>Inbound Port</th> <th>Protocol</th> </tr> </thead> <tbody> <tr> <td>5000</td> <td>TCP</td> </tr> </tbody> </table> <p>--Optional--</p> <table border="1"> <thead> <tr> <th colspan="2">Permitted Source Port Range</th> </tr> <tr> <th>From Port</th> <th>To Port</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Permitted External Network</th> <th>Permitted External Network Mask</th> <th>Permitted MAC Address</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Inbound Port	Protocol	5000	TCP	Permitted Source Port Range		From Port	To Port			Permitted External Network	Permitted External Network Mask	Permitted MAC Address			
Inbound Port	Protocol																
5000	TCP																
Permitted Source Port Range																	
From Port	To Port																
Permitted External Network	Permitted External Network Mask	Permitted MAC Address															

#	NTP Servers to Use (IP address or FQDN)
1	pool.ntp.org

Appendix

A.1. Mechanical Specifications

Mechanical Characteristics

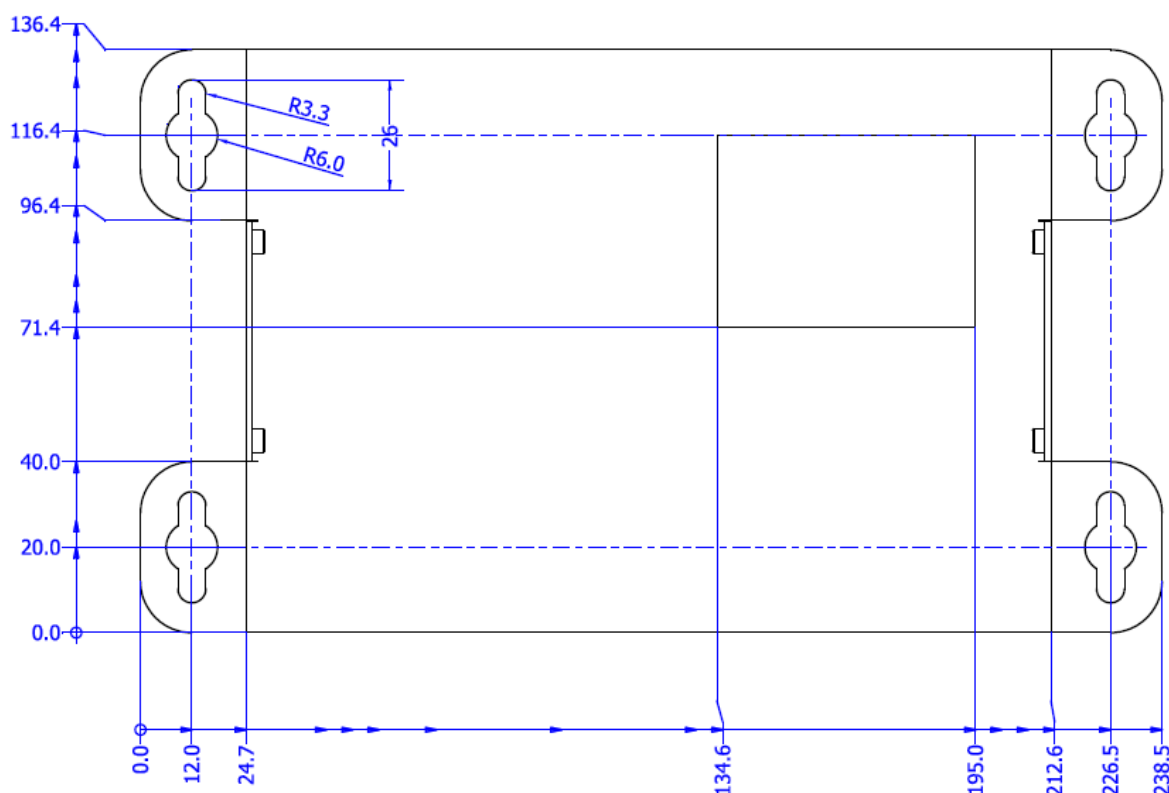
The electrical circuitry of the ZyWAN is contained in a sturdy aluminium enclosure consisting of a base and lid. The following table lists the ZyWAN mechanical characteristics.

Length	141 mm (9.4 in.)
Width	238.5 mm (5.6 in.)
Height	65 mm (2.5 in.)
Weight	1.25 kg (2.75 lbs) approx. (may vary based on optional hardware)

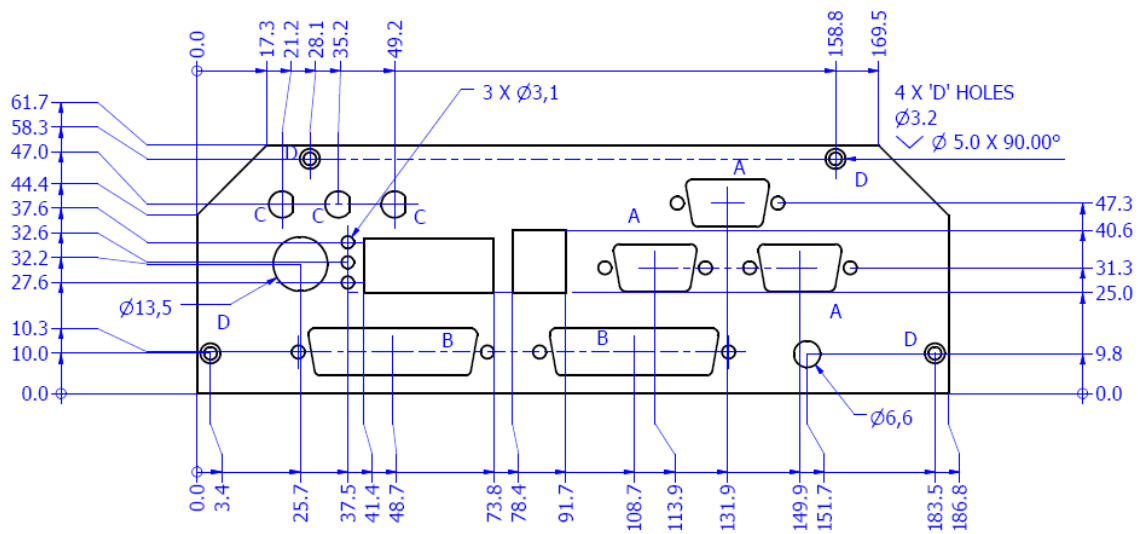
Mounting Details

The mechanical dimensions of the ZyWAN are shown next (all dimensions are shown in millimeters). When the unit is mounted, there must be sufficient space to connect the cables. Antennas must be located in an area where there will be adequate exposure to RF signals. For GPS, this generally means the GPS antenna must have line of sight to a wide area the sky in order to receive signals from multiple positioning satellites.

Mounting Dimensions of Base



Dimensions of ZyWAN Faceplate



A.2. Electromagnetic Compatibility (EMC)

The ZyWAN is classified as a component with regard to the European Community EMC regulations, and it is the user's responsibility to ensure that systems using the product are compliant with the appropriate EMC standards.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules and European Community EMC regulations. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

1. Reorient or relocate the receiving antenna.
2. Use shielded RJ-45 cables for the Ethernet connections.
3. Increase the separation between the equipment and receiver.
4. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
5. Consult the dealer or an experienced radio/TV technician for help.

Radio Frequency Requirements

This device complies with Part 15 of FCC Rules. Operation is subject to the following conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.
3. To comply with RF safety requirements, you must maintain a distance of 20 cm from the antenna when operating the device.
4. Each antenna of this device must not be co-located with (within 20 cm of) any other antenna or transmitter. Antenna requirements are listed in the FCC grant information for each module given in the next sections.

Changes or modifications to the product not expressly approved by Eurotech could void the user's authority to operate the equipment.

Radio Frequency Standards for ZyWAN-EVDO (MC5725, MC5727)

FCC ID: UFNZEUSMC5725

FCC grant information: Modular Approval for use as a module in mobile-only exposure conditions, antenna gain including cable loss must not exceed 5.1dBi in cellular band and 4.15dBi in PCS band, for purposes of 2.1043 and 2.1091. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter within a host device.

Radio Frequency Standards for ZyWAN-3G (MC8775)

FCC ID: UFNZEUSMC8775

FCC grant information: This device is approved for mobile RF exposure conditions. Approved for use with antenna(s) as listed in this filing. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio Frequency Standards for ZyWAN-IDEN (IO270)

FCC ID: UFNZEUSIO270

FCC grant information: Products operating with this OEM module must not exceed 2.54 W EIRP total system output with antenna gain not exceeding 7.3dBi. The antenna must operate at 20 cm or more from persons. This module is not approved for use in any products operating as a portable transmitter with respect to 2.1093 or other mobile operating conditions that do not meet categorical exclusion requirements of 2.1091, which requires separate approval.

Radio Frequency Standards for ZyWAN-GPRS (GR64)

FCC ID: UFNZEUSGR64

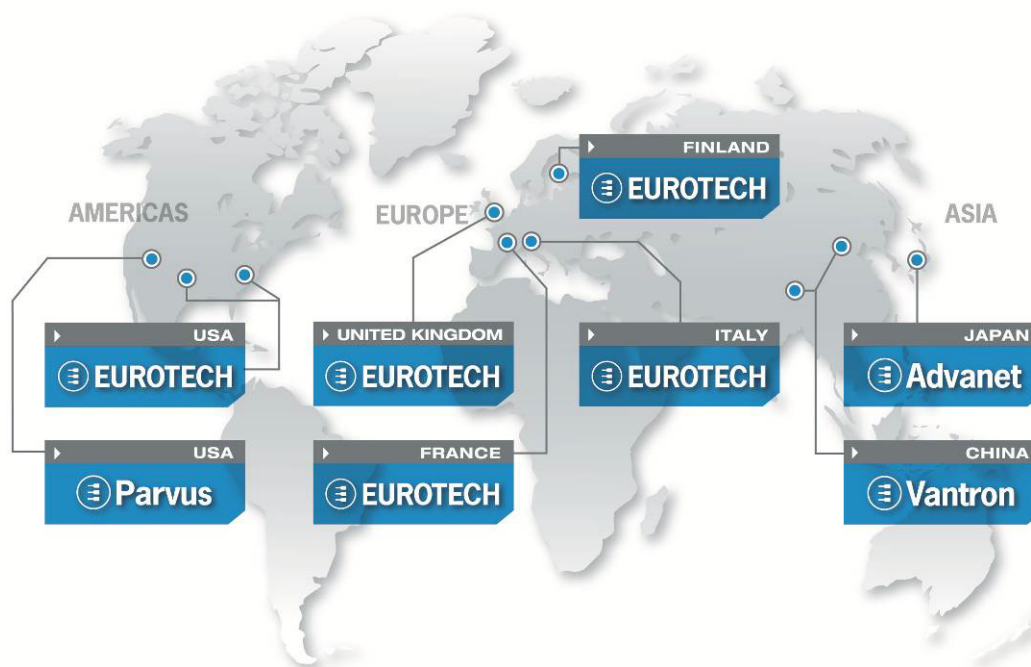
FCC grant information: This device is approved for mobile RF exposure conditions. Approved for use with antenna(s) as listed in this filing. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio Frequency Standards for ZyWAN with 802.11

FCC ID: UFNZEUSPN18

FCC grant information: Modular Approval for mobile RF exposure conditions, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. The only antennas approved for use with this module are those documented in the filings under this FCC ID.

Eurotech Worldwide Presence



AMERICAS

EUROPE

ASIA



USA

EUROTECH

Toll free +1 888.941.2224
Tel. +1 301.490.4007
Fax +1 301.490.4582
E-mail: sales.us@eurotech.com
E-mail: support.us@eurotech.com
Web: www.eurotech-inc.com

PARVUS

Tel. +1 800.483.3152
Fax +1 801.483.1523
E-mail: sales@parvus.com
E-mail: tsupport@parvus.com
Web: www.parvus.com

Italy

EUROTECH

Tel. +39 0433.485.411
Fax +39 0433.485.499
E-mail: sales.it@eurotech.com
E-mail: support.it@eurotech.com
Web: www.eurotech.com

United Kingdom

EUROTECH

Tel. +44 (0) 1223.403410
Fax +44 (0) 1223.410457
E-mail: sales.uk@eurotech.com
E-mail: support.uk@eurotech.com
Web: www.eurotech.com

France

EUROTECH

Tel. +33 04.72.89.00.90
Fax +33 04.78.70.08.24
E-mail: sales.fr@eurotech.com
E-mail: support.fr@eurotech.com
Web: www.eurotech.com

Finland

EUROTECH

Tel. +358 9.477.888.0
Fax +358 9.477.888.99
E-mail: sales.fi@eurotech.com
E-mail: support.fi@eurotech.com
Web: www.eurotech.com

Japan

ADVANET

Tel. +81 86.245.2861
Fax +81 86.245.2860
E-mail: sales@advanet.co.jp
E-mail: tsupport@advanet.co.jp
Web: www.advanet.co.jp

China

VANTRON

Tel. +86 28.85.12.39.30
Fax +86 28.85.12.39.35
E-mail: sales@vantrontechnology.com.cn
E-mail: support.cn@eurotech.com
Web: www.vantrontechnology.com.cn

To find your nearest contact refer to: www.eurotech.com/contacts



www.eurotech.com

EUROTECH HEADQUARTERS

Via Fratelli Solari 3/a
33020 Amaro (Udine) – ITALY
Phone: +39 0433.485.411
Fax: +39 0433.485.499

For full contact details go to: www.eurotech.com/contacts