WiMetry™ CDMA 1xEV-DO Cellular Concentrator

User Manual
PN: 001-0007-500 Rev 0

This manual covers the operation of the CalAmp Corp WiMetryTM Cellular Concentrator. Specifications described are typical only and are subject to normal manufacturing and service tolerances.

CalAmp reserves the right to modify the equipment, its specification or this manual without prior notice, in the interest of improving performance, reliability or servicing. At the time of publication all data is correct for the operation of the equipment at the voltage and/or temperature referred to. Performance data indicates typical values related to the particular product. No part of this documentation or information supplied may be divulged to any third party without the express written consent of CalAmp Corp.

Products offered may contain software which is proprietary to CalAmp Corp. The offer or supply of these products and services does not include or infer any transfer of ownership.

Device Use Limitations

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for Class B Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates 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 nearby electrical devices, the user is encouraged to try to correct the interference by one or more of the following measures.

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult CalAmp technical support for help

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To comply with FCC regulations for the device, the following rules must be obeyed during and after installation

Keep the cellular antenna of the Concentrator at a safe distance from your head and body while the modem is in use (see below). Maintain a distance of at least 20 cm (8 inches) between the transmitter's antenna and any person while in use. This modem is designed for use in applications that observe the 20 cm separation distance.

When using an external 802.15 and cellular antenna, maintain a distance of 20cm (8 inches) between the antennas. Placing the antennas closer than 20cm violates FCC certifications of the concentrator.

To comply with FCC approval for the EVDO device, do not use a cellular antenna with a gain greater than 5.1dBi in the cellular (800MHz) band, or 4.15 dBi in the 1900MHz band.

For customers using an external antenna for 802.15 communication, do not use an antenna with a gain greater than 2dBi. For customers using the internal antenna supplied with the device, CalAmp has verified the antenna does not violate FCC rules.

The required antenna impedance for both the cellular and 802.15 antennas is 50ohms.

Safety Issues

Avoid unsafe operation of the concentrator by following these guidelines.

Important: A version of the concentrator that has been certified to work in hazardous environments such as gas and oil fields is available. If your application requires operation in these environments, contact Calamp to ensure your concentrator has the necessary certifications.

The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action or both.

- Do not operate in the vicinity of gasoline or diesel-fuel pumps unless use has been approved and authorized
- Do not operate in locations where medical equipment that the device could interfere with may be in use
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized
- Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers.

Contents

SECTION 1 – PRODUCT OVERVIEW

Module Identification

The label contains the CalAmp part number, serial number, MAC ID, FCC ID and the ESN numbers. The ESN number is required by your cellular carrier when activating your data contract.

General Description

The CalAmp WiMetry™ Concentrator is an Internet Protocol-based, bidirectional wireless data concentrator platform used for advanced metering and demand response monitoring and control applications. The platform also has other smart grid applications and facilitates real-time acquisition of critical usage and rate data from electric, gas or water meters via public wireless networks and the Internet.

The WiMetry™ platform supports the latest in cellular 3G high-speed data communications and is backward compatible to existing EV-DO Rev. 0 and 1x networks. WiMetry™ takes advantage of ongoing investments made by cellular network operators to build-out, improve and maintain ubiquitous, reliable wireless networks using the latest standards, thereby enabling utility companies to focus on their core business rather than having to establish their own proprietary wireless networks.

WiMetry uses the industry standard TCP/IP communication protocol and is compatible with most leading software applications. It offers wired EIA-232, EIA-485, USB and Ethernet connectivity as well as wireless IEEE 802.15.4 wireless connectivity to remote meters and thermostats.

Features

- CDMA 1xEV-DO Rev. A with data transfer rates up to 3.1 Mbps downlink/1.8 Mbps uplink.
- Optional 802.15.4 wireless communication with 20dBm transmit power
- Embedded Linux (with support for custom applications) on ARM 9 processor
- Browser-based User Interface
- Local and remote configuration and monitoring
- One button OTASP
- RSSI indicator

Hardware Features

- Up to 8 Standard RS-232 Serial Ports with optional hardware flow control
- 1 Configurable RS-485 port

- Optional Isolated AC/DC power supply
- Two Relay Outputs (Up to 1A)
- NEMA 4 non-metal Enclosure
- External Battery Connection

Figure 1 shows the key components and connectors on the WiMetry Concentrator.

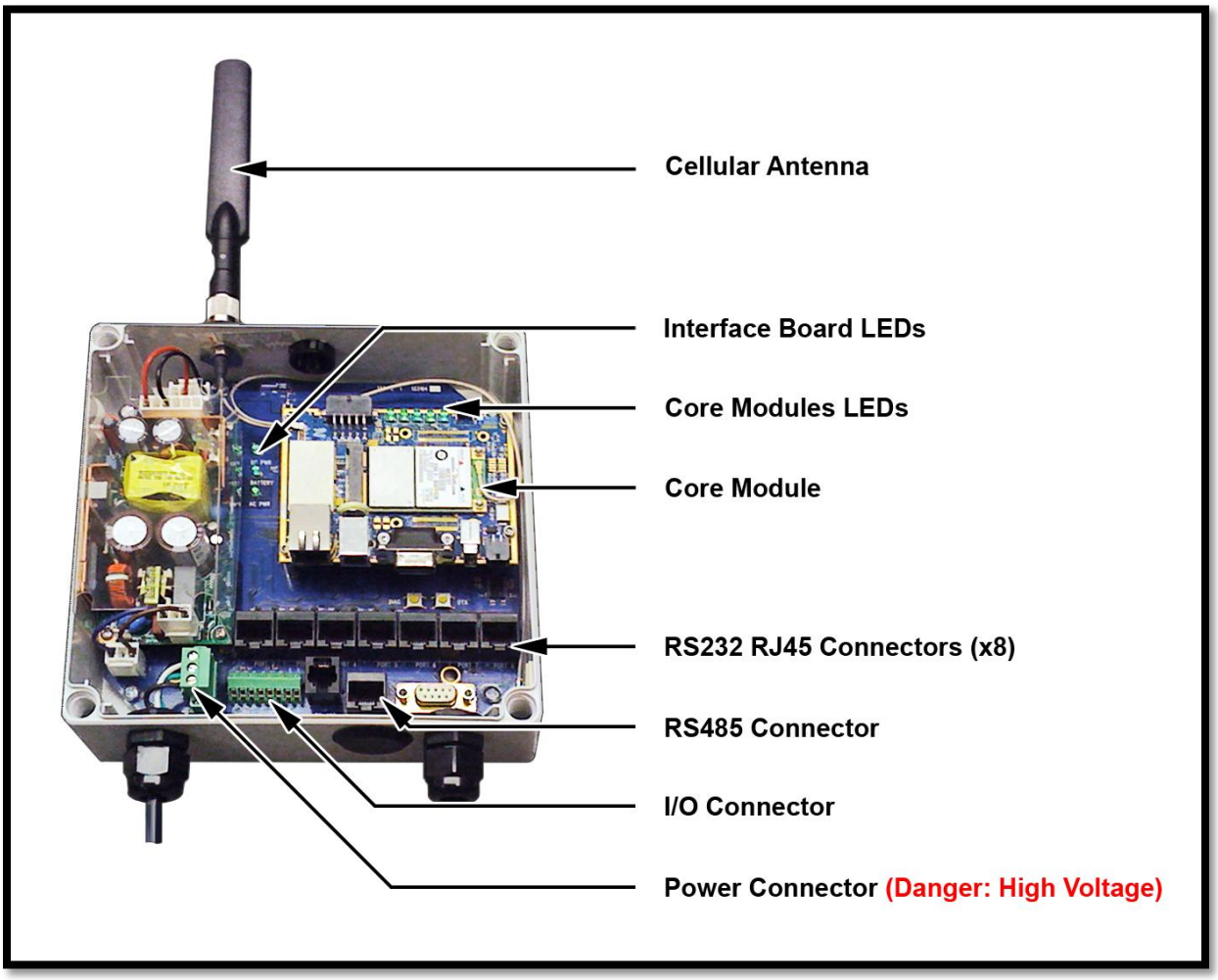


Figure 1: WiMetry Concentrator Key Components

SECTION 2 – HARDWARE SETUP

RJ-45 Serial Ports (EIA-232)

The concentrator contains 8 RJ-45 serial ports that contain all the required signals for RS232 serial communication per the RS232 specification.

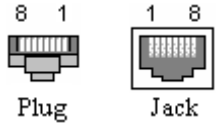
The table below provides the information to purchase or build cables to connect to one of the 8 RJ45s on the Concentrator. You can also purchase a RJ45 to DB9 adapter cable from CalAmp that allows direct connection to a device with a standard serial connector (refer to RS-232 specification for more information).

Note: All signal names and directions are from the perspective of the concentrator.

Table 1: RJ-45 EIA-232 Pin-out (Port 1 – Port 8)

Function	Pinout RJ45 (board)	Pinout DB9 female (Port 1 only)	Direction
DCE Ready DSR	1	6	Output
Line Signal Detect	2	1	Input
Clear to Send (CTS)	3	7	Input
Receive*	4	3	Input
Request to Send (RTS)	5	8	Output
Transmit*	6	2	Output
Ground*	7	5	NA
DTE Ready (DTR)	8	4	Input

** Required Signals*



RJ-11 Serial Port

The Concentrator provides a single RS485/RS422 connector for differential serial communication.

Table 2: RS485/RS422 Connection (J7)

Pin	Signal
1	TX +
2	TX -
3	RX+
4	RX-

External I/O

The Concentrator contains remotely controlled relays that can be used to drive larger latch relays external to the device. The internal relays and be open and closed remotely from the Concentrator HTML interface. The battery connections can be used if an external backup battery is desired.

Table 3: Relay Connections (J4)

Pin	Signal
1	Relay 1 Normally closed
2	Relay 1 Common
3	Relay 1 Normally Open
4	Relay 2 Normally Closed
5	Relay 2 Common
6	Relay 2 Normally Open
7	External Battery Positive
8	External Battery Negative

Power Connection

The concentrator is delivered with a AC Wall Plug power cable. Due to the presence of high voltage, the power cable should only be removed or modified by a trained and qualified installer or electrician.

Table 4: Screw Terminals (J4)

Pin	Signal
1	AC Power
2	Ground
3	AC Neutral

Caution: When plugged into a 120V supply, high voltage will exist on the terminals.

Status LEDs

Status LEDs are installed inside the Concentrator case. Remove the top of the case to check status during installation. Below is a summary of the LEDs.

LEDs on the Core Module

Power: The Concentrator is powered
Service: The unit has connected to a cellular network
Activity: Shows activity on the cellular link
Signal: Indicates a sufficient RSSI on the cell signal
Zigbee: Zigbee circuitry is present and functional

LEDs on the Interface Board

DC Power: The 12V DC power is present
Battery: The backup battery is present
AC Power: AC Power is present

Antenna Options

An external Cellular antenna is required for operation. A 802.15.4 antenna is required if 802.15.4 wireless communication is required. Antennas are available for Concentrator installations from CalAmp Corp.

Cellular Antenna

The Concentrator requires a dual-band cellular antenna for operation in the 800 MHz band and the 1900 MHz band. The primary antenna connection on the Concentrator is a TNC female connector; therefore you must purchase an antenna with a TNC male connector. Do not select a TNC antenna with "reverse polarity" or RP-Male. When using a direct mount or "rubber duck" antenna, choose the antenna specific to your band requirements. Mounting options and cable lengths are the user's choice and application specific.

To comply with FCC approval for the EVDO device, do not use a cellular antenna with a gain greater than 5.1dBi in the cellular (800MHz) band, or 4.15 dBi in the 1900MHz band.

802.15 Antenna

The concentrator is available with an integrated 2.4GHZ 802.15 antenna. For customers requiring an external antenna, an external SMA antenna connector is provided. Select an 2.4GHZ antenna with a gain of up to 2dBi depending on your range requirements.

To comply with FCC approval for the EVDO device, do not use a 2.4GHZ antenna with a gain greater than 2dBi.

To comply with FCC approval for the concentrator device, do not place the 802.15 antenna within 20cm of the cellular antenna.

SECTION 3 – GETTING STARTED

Package Contents

- WiMetry™ Concentrator
- Quick Start Guide
- Power cable
- Serial Cables (optional)
- Cell Antenna (optional)
- IEEE 802.15 Antenna (optional)

Set-up Requirements

- Concentrator Module
- Computer running Windows 2000, XP or Vista
- AC power connection
- Ethernet cable
- Active cellular data account
- Cellular antenna
- External or Internal 802.15 antenna

To remain in compliance with FCC certification for this CDMA product, do not use an antenna with >5.1 dBi gain in the cellular (800 MHz) Band or >4.15 dBi in the PCS (1900 MHz) band.

For customers using an external antenna for 802.15 communications, do not use an antenna with a gain greater than 2dBi. For customers using the internal antenna supplied with the device, CalAmp has verified the antenna does not violate FCC rules

Quick Start

Initial start up and service provisioning of the Concentrator must be done with a local Ethernet connection. Remote administration is only possible once the module is provisioned.

Connecting Your Device

1. If the Concentrator did not come with an attached antenna, attach a dual band cellular antenna to the TNC bulkhead on the top of the concentrator.

2. Open the Concentrator case by removing the four screws on the corner of the case.

3. Connect an Ethernet cable from the LAN connector (J7) on the core module to the PC. You may need to temporarily disconnect some of the RJ45 serial connectors to access the Ethernet jack.

4. Connect the power supply. Use caution not to touch high voltage on J16 when the case is open and concentrator is powered on.

5. Verify that the “AC PWR” LED comes on when powered.

Configuring Local PC

1. Verify network settings on local PC are set to automatically detect IP and DNS server. The path to network settings varies with the version of Windows you are using.

   Windows XP Users
   Start → Control Panel → Network Connections

   Windows 2000 Users
   Start → Settings → Network and dial up connections

   Windows Vista Users
   Start → Control Panel → Network and Sharing Center

2. Select the appropriate network connection, typically the ***Local Area Connection***, and right click to select ***Properties***.

3. Select ***Internet Protocol (TCP/IP)*** and click ***Properties***.

Figure 2: Local Area Connection Properties (Windows XP)

4. Verify that ***Obtain an IP address automatically*** and ***Obtain DNS Server address automatically*** are selected.

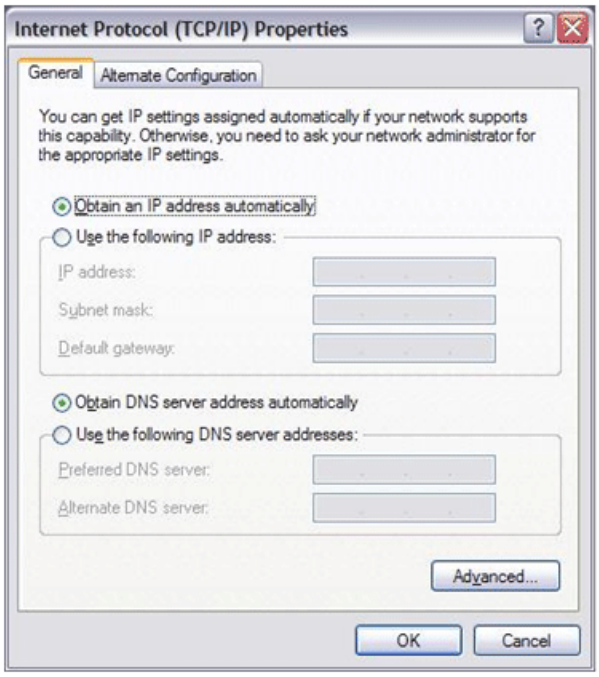


Figure 3: Internet Protocol (TCP/IP Properties

Device Log In

1. Power on the Concentrator
2. In an Internet browser, enter http://192.168.1.55 to access the Concentrator login page.
3. Login to the device. When logging in for the first time, use the default values:

   User Logon: admin
   Password: password

4. This will bring up the Concentrator homepage. You can view configuration parameters from this screen. The configuration options are further explained later in this document.

Provisioning the Concentrator

WiMetry requires an active cellular data service contract for provisioning. Verify that your cellular service contract is a data service contract with packet data NOT circuit switched technology. If you do not have an active data contract, contact your service provider.

1. Before provisioning the unit, verify that you have a strong cellular signal and that you are not roaming. This status information is available on the home page. If you are activating a 3G

CDMA contract, you will most likely need to be in an area that has 3G coverage. Verify that the service type is “CDMA EVDO service”.

2. The ESN (electronic serial number) must be registered with your cellular provider prior to completing the following steps to provision the Concentrator. To activate your account, call your service provider

3. On the left side of the homepage, select the WAN (Cellular) page. At the bottom of the page is the OTASP/IOTA Activation box. See figure below. The default command of *22899 is the OTA command for Verizon. If activating a unit on the Verizon network, you do not need to change this command. If activating a unit on the Sprint network, the OTASP command is not used and the default can remain. If using another carrier, see the carrier specific information section in this document.

4. **For Verizon:** At the bottom of the page, select “OTASP” for activation type and select “Submit”.

   For Sprint: Select “IOTA” and click “Submit”.

   Do not turn off the unit while it is provisioning.

5. After a few moments you will receive a message saying the OTA was successful. Once the OTA is complete the unit will reset. You must refresh your browser to reconnect with the device following the reset.

6. Once your module is activated, browse to an Internet webpage to confirm connectivity.

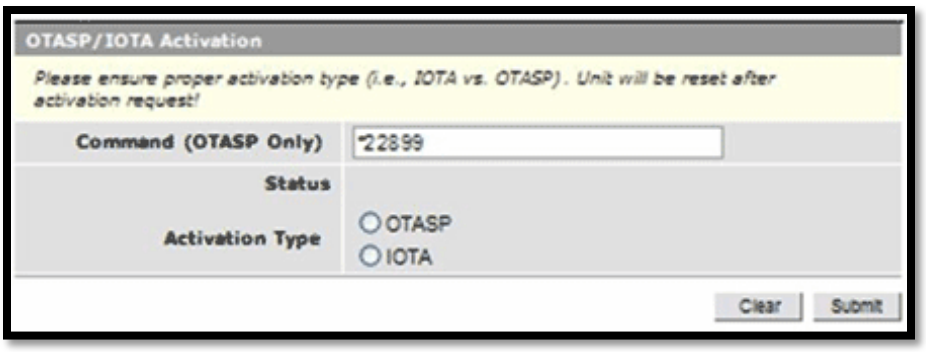


Figure 4: Concentrator WAN (Cellular) Page

SECTION 4 – CONFIGURATION

General Instructions

The following instructions are common to all html pages. The Help, Home and Reset links are located at the top right of all HTML pages.

Help	Select this link on any of the devices configuration pages to bring up the help text for that screen.
Home	Select this link to return to the home page of the modem.
Reset	Select this link to command the unit to reboot. This process will take about 40 seconds. The software will ask you to confirm this command prior to re-booting.
Save	Most changes to a configuration parameter require the user to click save before the change will take effect.
Clear/Cancel	Most configuration menus also have a "Clear/Cancel" option. Selecting this button will restore all fields in a section to their last saved value. Note: This does not return them to their factory defaults.

Home Page Parameters

The WiMetry™ Concentrator's home page lists the unit's primary operating parameters and status. Configuration changes cannot be made from this page. Refer to Figure 5 for the WiMetry Home Page.

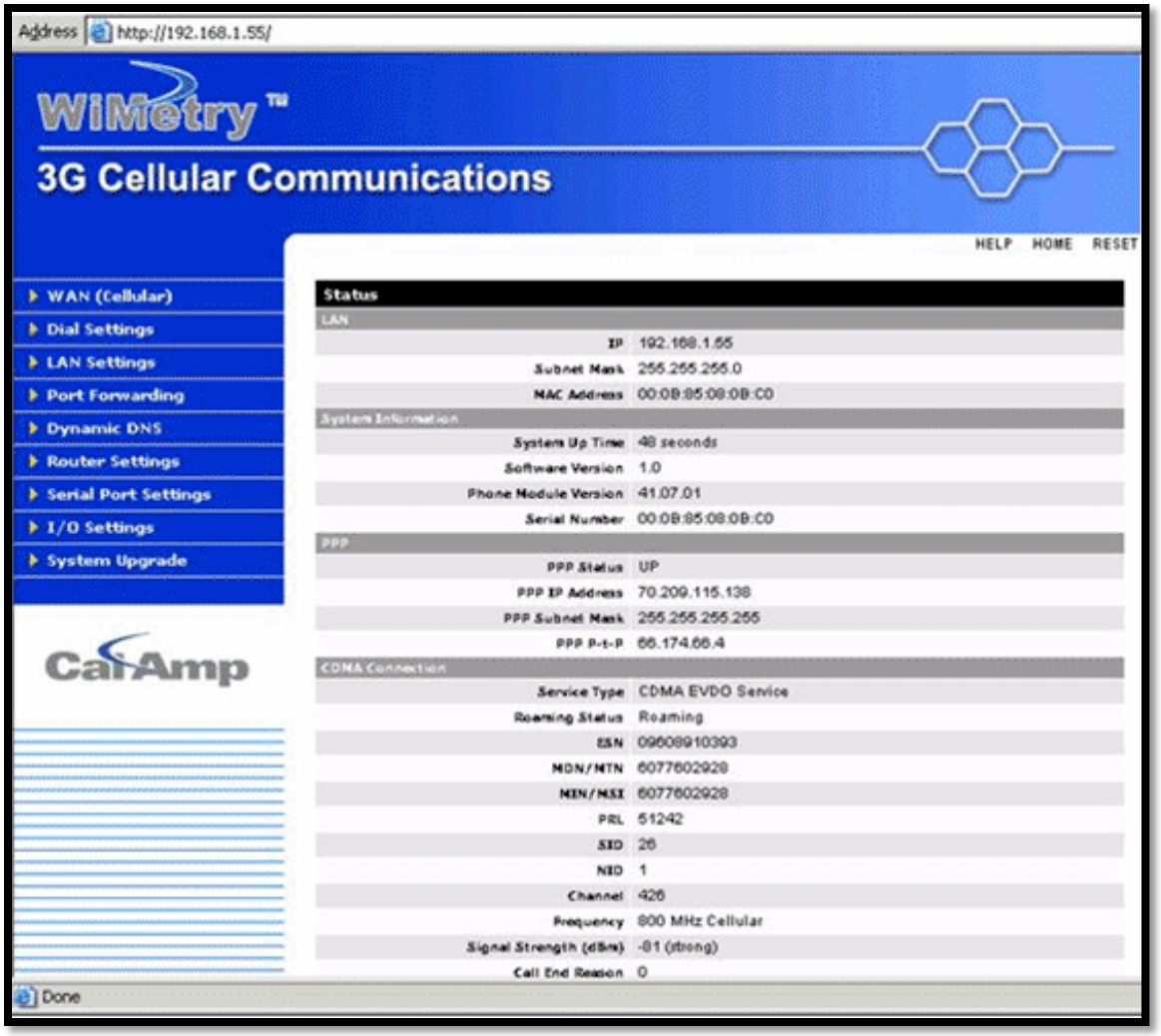


Figure 5: WiMetry Home Page

IP	IP Lists the LAN IP address of the Concentrator. This IP becomes the gateway and DNS server for all PCs and devices connected on the LAN. This value is configured on the LAN Settings Page.
Subnet Mask	The Subnet mask is used in conjunction with the network address to partition the IP address into the network(subnet) portion and the host portion. In most cases, this value will be automatically set by the software based on the class of IP address used for the Ethernet IP. This value can be modified on the LAN Settings page.
MAC Address	Media Access Control Address, this is configured at the factory and cannot be changed by the user
System Up Time	Displays a counter that starts when the unit is powered on and resets when the unit is powered down or hardware reset. Note: This counter does NOT indicate how long the WAN connection has been up.
Software Version	This reflects the version of application software loaded on the unit.
Phone Module	This is the version of the cellular module installed in the device. This may be

Version	required by tech support but is not required for any user applications.
Serial Number	This is assigned at the factory. This may be required by tech support but is not required for any user applications.
PPP Status	PPP Status indicates if the device has an established connection to the WAN. Status is UP or DOWN
PPP IP Address	PPP IP Address is the WAN IP address of the Concentrator. Remote access for the device requires entering this address into a browser. The PPP IP Address is assigned by the cellular carrier and will be dynamic unless a static address is specifically requested
PPP Subnet Mask	This subnet mask is assigned by the carrier and is not configurable by the user.
PPP P-t-P	WAN IP address of the network access point of the cellular carrier
Service Type	Service Type indicates the type of service connection. The Concentrator will automatically connect to the most advanced service available and will fallback to other networks (such as 1xRTT) when EV-DO Rev A is not available.
Roaming Status	Roaming Status indicates the unit roaming status. Status is ROAMING or NOT ROAMING
ESN	The Electronic Serial Number is assigned to the cellular modem at the factory. This number must be provided to the carrier to activate the module.
MDN/MTN	The Mobile Directory Number; assigned by the carrier when the module is activated
MIN/MSI	Mobile Identification Number, in most cases, this is the same as the MDN.
PRL	Preferred Roaming List; a database that declares the priority of other carriers while roaming. This file should be updated periodically to ensure proper connectivity while roaming. In most cases, the PRL file will be updated automatically when connected to the network but can be updated manually by performing an OTASP operation, (see provisioning section).
SID	System ID, this is status only and is assigned by the carrier when connecting to the network.
NID	Network ID, this is status only and is assigned by the carrier when connecting to the network.
Channel	Status only, indicates the channel assigned by the carrier when connecting to the network.
Frequency	Status only, indicates the frequency band on which the unit is communicating. If the unit is being used in North America, it will indicate either 800MHz or 1900MHz.
RSSI	Receive Signal Strength Indication indicates the strength of the network signal with both a numerical value and a good/medium/poor message.

WAN Cellular Parameters

This page contains the provisioning information and the carrier activation settings. For more information on the procedure for carrier activation, see the “Provisioning the Concentrator on page xx” section.

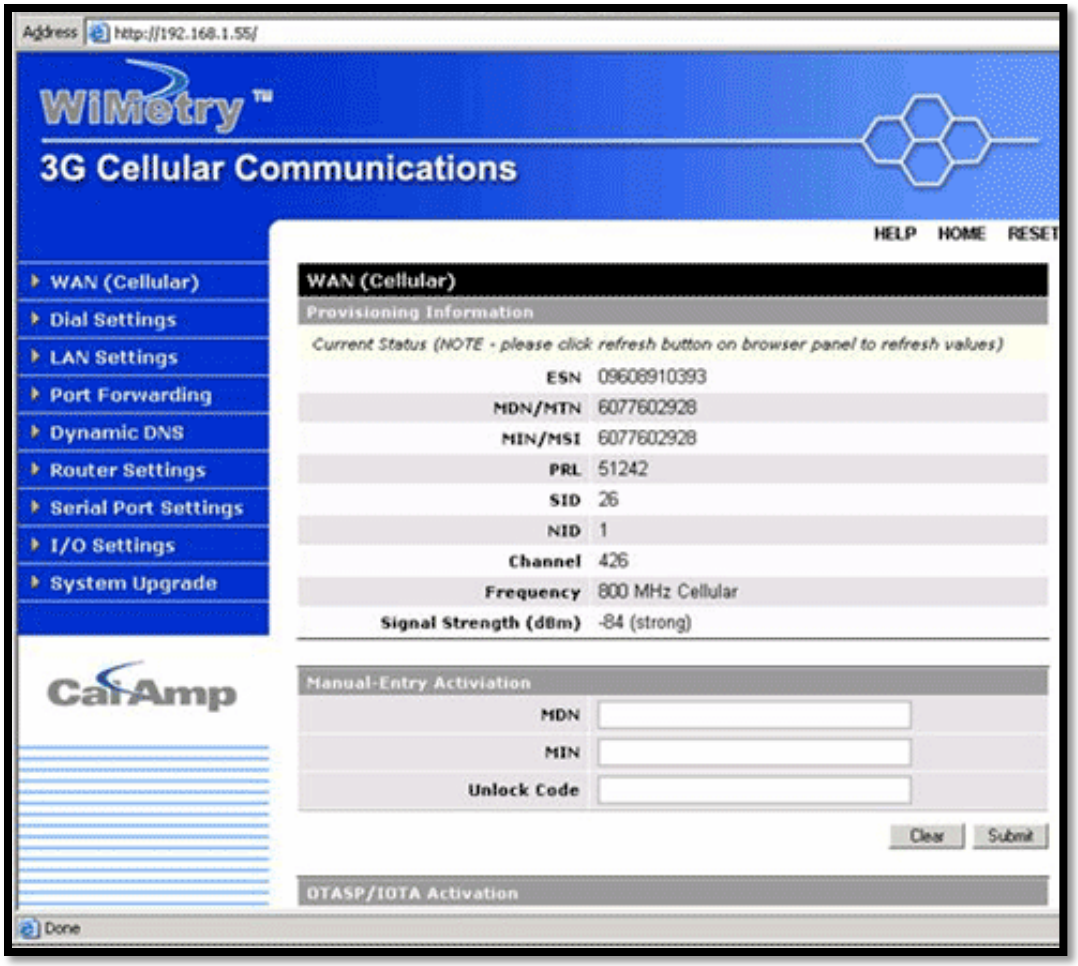


Figure 6: WAN Cellular Page

Provisioning Information

The provisioning information is also available on the home page. These parameters are defined in the home page section above.

Manual-Entry Activation

Manual entry of the parameters in this section is required by some carriers while some carriers will enter the parameters automatically during an OTASP call. Refer to carrier specific provisioning section to get specific instructions for your carrier.

MDN	Mobile Directory Number, identifier for your device provided by the cellular carrier when activating a service contract
MIN	Mobile Identifier Number, identifier similar to the MDN. In many cases, this number will be the same as the MDN
Unlock Code	Code provided by some carriers when activating a contract that must be entered to perform an OTASP. Refer to carrier specific instructions to

	determine if you carrier requires an unlock code
OTASP/IOTA Activation	*Command:* Carrier specific command used for OTASP (over the air service provisioning). The default is *22899 (Verizon OTA command)
Activation Type	Activation type is carrier dependent
OTASP	Over the air service provisioning
IOTA	Internet over the air

Dial Settings

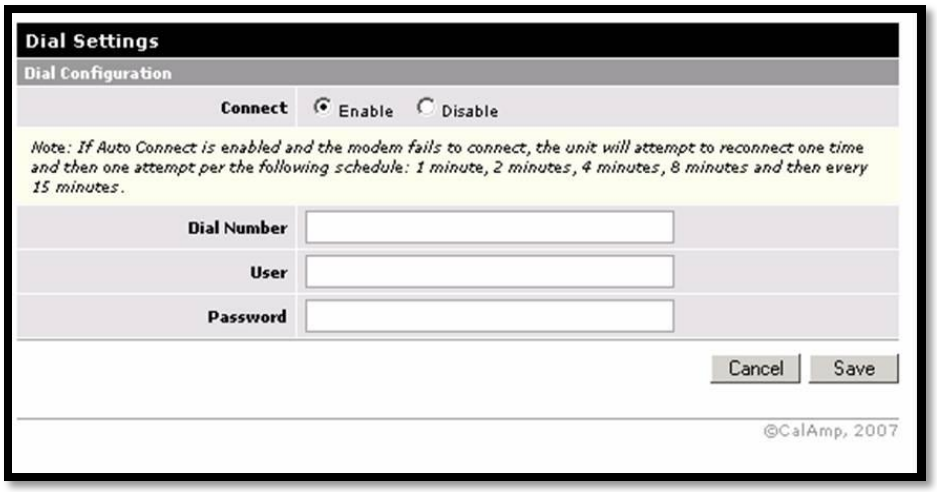


Figure 7: Dial Settings Screen

The Dial Setting page allows the user to Disable auto-connect. This page also contains information on the reconnect timers in the note under the "Connect" selection. These reconnect timers are defined per carriers certification requirements; they cannot be changed.

By default, the auto-connect feature (labeled "Connect") is enabled. When this feature is enabled, the Concentrator will automatically connect to the network on power up. If the auto-connect is disabled, you must re-enable the auto-connect, the cycle power or perform a hardware reset to connect to the network. If you want to keep the auto-connection function disabled, you will have to disable it before powering down again.

This page also contains dial number, user and password information. This information should only be entered if required by your carrier.
Note: Most users will not enter a dial number, user or password. This is required for older dial-up cellular standards. It is not used for 3G standards. Unless it is specifically required for your application, do not enter any information in these fields.

SECTION 5 – SERIAL PORT SETUP

The serial port settings page allows the user to configure up to 8 serial ports on the concentrator. It also allows the user to assign unique port numbers to each serial port. These port numbers allow a remote PC to communicate to the end device by sending data to the WAN IP of the concentrator followed by the port of the device as assigned in the serial port setup.

The serial port settings page shown below can be accessed by selecting ***Serial Port Settings*** on the left side of the user interface. The naming convention used to describe the serial port lines assumes that the concentrator is a terminal device and the device connected to the serial port is the client.

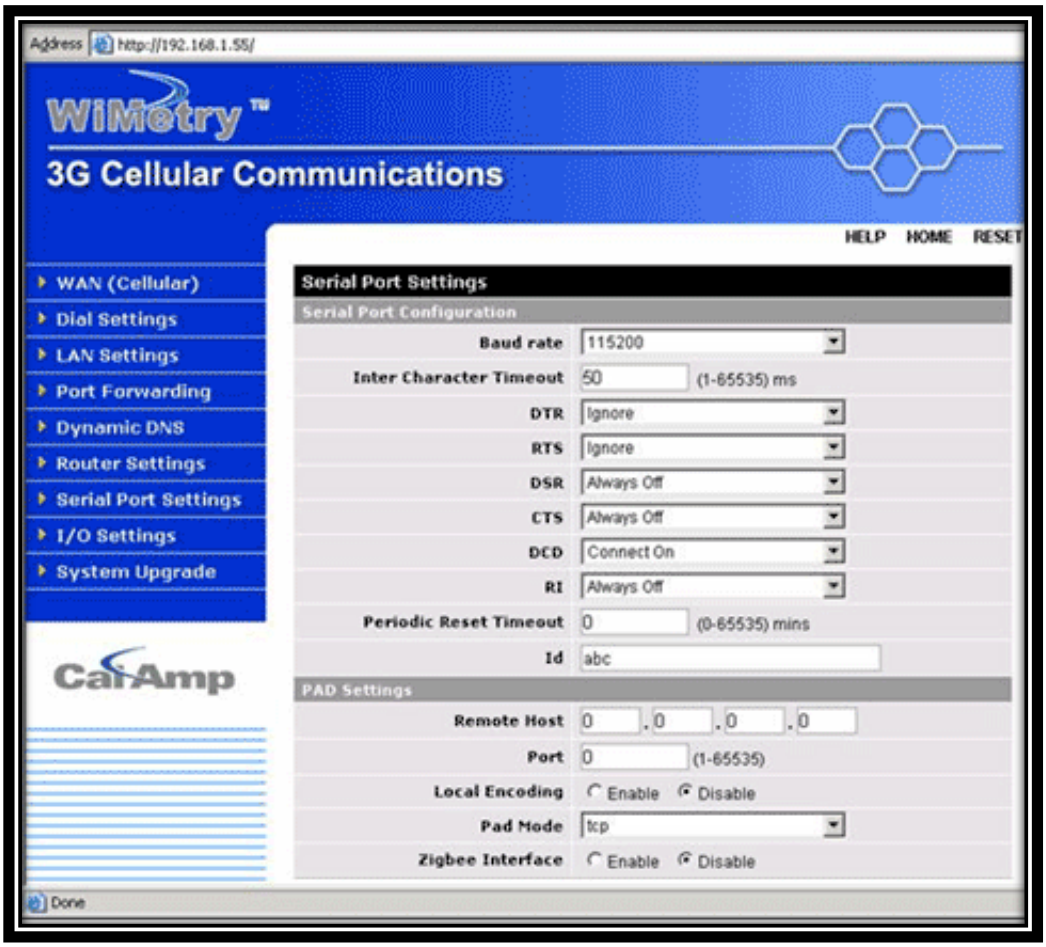


Figure 8: Serial Configuration Page

Serial Port Configurations

Serial Port Selection	A pull down menu that allows the user to select the serial port to configure.
Baud Rate	Set the baud rate of the serial port from the standard baud rates. Baud rates from 300baud to 230Kbaud available

DTR (output)	Device Terminal Ready, used when communicating with a modem to tell the modem that the terminal is ready. Can be set to Always On, Always Off, or On When Available
RTS (output)	Request to Send: Used when hardware flow control is active. To activate hardware flow control set this signal and the CTS signal to "Flow Control". This signal can also be set to "Always On" or "Always Off"
DSR (input)	An indication from a modem device that it is "active". This line can be set to "ignore" or Modem operation. In most applications, this line will be ignored
CTS (input)	Set this line to "Flow Control" to use hardware flow control on the Serial line. Set to "Ignore" if flow control is not required

Packet Assembler/Disassembler Settings

Remote Host	Set the WAN IP address of the remote device that is allowed to access the third party device on this serial channel. This may also be set to 0.0.0.0 which allows all external devices to access this serial port. A setting of 0.0.0.0 should be used if multiple PCs may access the device or the PC has a dynamically assigned IP
Incoming Port	The incoming port that will be mapped to this serial port. This port must be entered following the WAN IP of the Concentrator device when accessing the serial port remotely. Note: Do not assign two serial ports the same Incoming Port.
PAD Mode	Set to TCP or UDP depending on the third party device requirements

Example of Serial PAD Mapping

Once each active serial channel has been mapped to a unique port number in the PAD settings, the serial channels can be accessed remotely by entering the WAN IP of the Concentrator followed by the port of the serial as shown below:

http://70.209.115.93:8080

Where 70.209.115.93 represents the PPP IP Address on the home page and :8080 represents the incoming port that is mapped to serial port in PAD Settings.

When the mapping is set up, all packet data coming across the cellular link will be disassembled and sent to the serial channel corresponding to the port in the incoming address. Conversely, all data received on the serial port will be packetized and sent across the cellular network to the remote PC.

SECTION 6 – 802.15.4 NETWORK SETUP

The WiMetry Concentrator IEE 802.15.4 Application acts as the coordinator on the local wireless network. It supports both mesh and tree networking. The concentrator will automatically form a network with routers and end devices with the same channel and extended PAN ID that are in range. The Concentrator also implements security on all networks. The security used is the same as is required in Smart Energy Networks. For more information on the WiMetry 802.15 application see the WiMetry Local Wireless Profile Specification.

Channel	There are 16 channels available per the 802.15 standard. The user can select any of these channels or select "Scan Channels" and the wireless module will automatically scan all channels and select the channel that has the least ambient noise. Note: Channels 15, 20, 25 and 26 are the channels least likely to encounter interference with nearby WiFi networks when used in North America. Use these channels if WiFi networks are nearby
Extended PAN ID	The extended PAN ID is used to prevent unwanted devices from joining your network. By default this is set to all 0s. When the default value is used, the concentrator will allow any device to join the network. When the ExPAN ID is set, it will only allow third party devices with a matching extended PAN ID to join the network. If you sent the ExPAN ID, be sure to set all desired third party devices to the same value or they will not be able to join the network.
Allow Join	The Concentrator will allow end devices to join its network for a short time period on power up. After the initial join timer expires the user must command the Concentrator to allow new end devices to join. There are three options: "ON" or "OFF" or a turned on for a set time. When in this mode, the Concentrator will allow joining for the number of seconds entered in the box. Allow at least 120 seconds to ensure new devices will join properly.
Transmit Power	Sets the transmit power of the device. The pull down menu displays valid power settings.
Port Mapping	Each end device on the 802.15 network must be associated with a remote IP and port to allow remote communication over the cellular link. Assign a port number to each address table slot that will be filled with an end device. Do not assign two end devices the same port or assign a port that is used in the serial mapping**.** *Note: This process works exactly the same as the serial port mapping except the data is sent over the wireless link, not on a hardwired serial connection.*
ID	The ID is a user defined name for each end device that can be used for identification purposes. This ID will be included in all data transmissions.

SECTION 7 – LAN SETTINGS

LAN Configuration

The concentrator can serve as an internet router for end devices with access to the Ethernet port on the core module. If you are not connecting a device to the Ethernet port during normal operation the defaults on this screen should be preserved (other than the password).

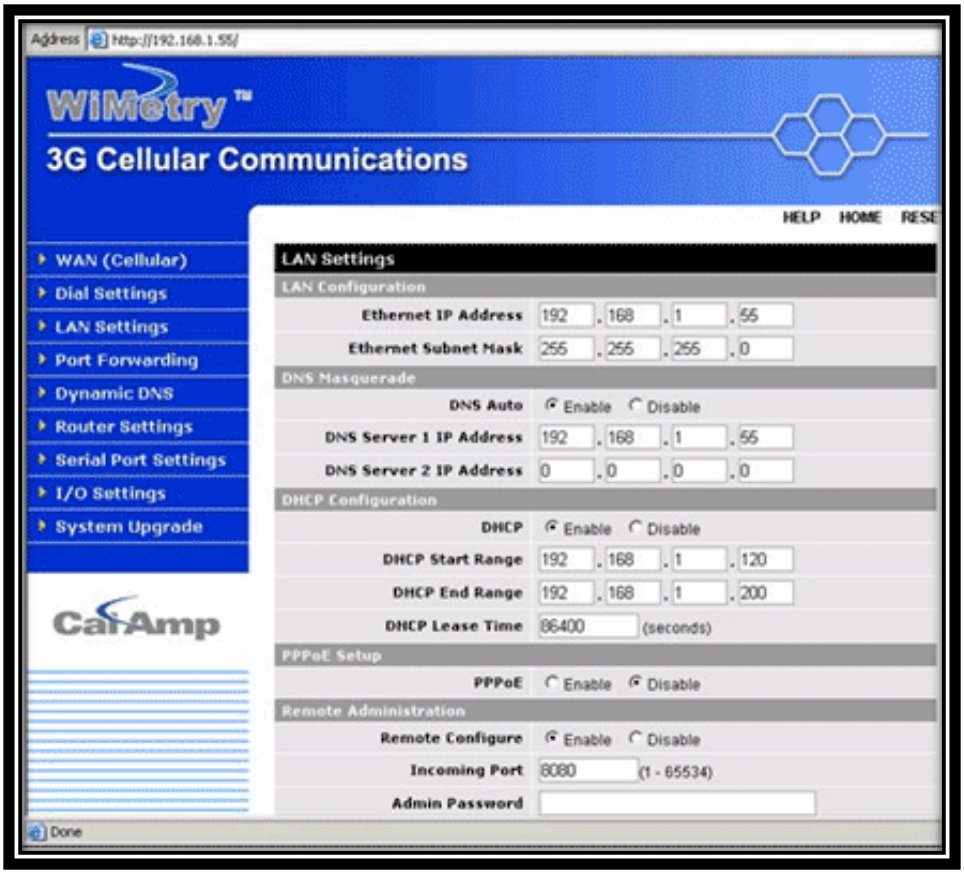


Figure 9: LAN Settings Page

Ethernet IP Address	LAN IP address of the Concentrator. This address is entered into a browser on a local PC when logging into the Concentrator home page. To decrease the chances of unwanted access, this value should be changed from its default prior to use. Changing this value will cause you to lose connection to the Concentrator. Enter the new address in the browser to reconnect. If you forget an address or make a mistake entering the new value, it may be difficult to reconnect to the device.
Ethernet Subnet Mask	The Subnet mask is used in conjunction with the Ethernet IP address to partition the address into the network (subnet) portion and the host portion. This value will be entered automatically by the software based on the class of IP address entered. It is not be necessary to change the default value once the Ethernet IP is entered.

DNS Masquerade

For more information on DNS definitions, refer to Network Basics section.

DNS Auto	This command enables/disables the Concentrator DNS server. Except in special cases, this should always be enabled. One exception to this is if using a PPPoE connection.
DNS Server1 IP Address	The preferred DNS server address. The Concentrator will set DNS server value on all local PCs to this value. Except in special cases, this address should match the Ethernet IP address since the Concentrator will serve as the DNS server for the LAN.
DNS Server2 IP Address	The DNS Server2 IP Address is used if a second DNS server is available.

DHCP Configuration

Dynamic Host Configuration Protocol is used by client devices that are connected to the LAN port of this device to automatically obtain an IP address assigned by this server/router.

DHCP	Selecting Enable will configure this device to assign IP addresses to client devices taken from a pool specified by the values entered in DHCP start range and DHCP end range. If DHCP is disabled, the information must be entered manually on all PCs.
DHCP Start/End Range	Sets the range of IP addresses assigned to the PCs. The user can limit the number of devices allowed on the network by limiting the range of IP addresses. Important: The addresses in this range must be on the same subnet as the Ethernet IP. The Ethernet IP should not be in the DHCP range.
DHCP Lease Time	Number that dictates the length of time a device on the LAN can hold an IP address. In most cases, this should be set to the maximum (default value) of 86400. If this value is set too low, it can cause network connectivity problems.

PPPoE Setup

PPPoE	PPP over Ethernet; PPPoE is used to create a password protected broadband connection. To use this feature, configure a broadband network connection on your PC. The procedure for setting up the broadband connection differs for different versions of Windows. When enabled, the DHCP Server is automatically disabled and configuration is erased. Note: In most cases, PPPoE is not required and the DHCP server should be left enabled.

Remote Administration

Remote Configure	Selecting Enable will allow remote access to the modem's configuration screens through the cellular network connection. Selecting Disable will shut off the ability to remotely access the modem's configuration screens.

Incoming Port	Change the port of incoming requests. It is not necessary to change this parameter unless it conflicts with other devices on the network.
Admin Password	Set the password for **BOTH** remote login and local login. The password must be entered twice for the password to change. Note: Changing any remote administration parameters remotely will cause the remote user to lose contact with the Concentrator. Login using new parameters to re-establish a connection. Users can be logged into a single unit both locally and remotely at the same time. Changes made on one end will not be reflected on the other unless the webpage is refreshed.

Example of Remote Login

The following should be entered into a browser on a remote PC to remote login to the Concentrator. The Concentrator must have remote administration enabled for this functionality to work.

http://70.209.115.93:8080

Where 70.209.115.93 represents the PPP IP Address on the home page and :8080 represents the incoming port on the LAN Settings page.

Disabling DHCP

When DHCP is enabled, any PC with physical access to the Concentrator Ethernet port will be assigned an IP address and have access to browse the Internet. This can cause security problems and may increase the amount of data transmitted over the network adding expense to the data contract. Disabling DHCP will allow the user to control which PCs have the ability to connect through the Concentrator. If changes are made to the network settings, be sure to keep a record of the changes for future use.

Disabling DHCP is performed on the LAN settings page. Under the DHCP section, select Disable, then hit **SAVE**. This also disables DNS Masquerading. Disabling DHCP will remove all values in the DHCP and DNS sections. Record all values in these fields prior to disabling in case you are required to go back to the original configuration.

To improve security, change the Ethernet IP of the Concentrator from the default setting. *Important: If the DHCP is disabled, and you do not have a record of the Ethernet IP, you will not be able to login to the Concentrator home page.*

On the network setting page of each PC set the following:

IP address:	Set a unique address on the same subnet as the Concentrator
Subnet Mask:	Set to the same value as the Concentrators Ethernet Subnet Mask field
Default Gateway:	Ethernet IP of the Concentrator
Preferred DNS:	Ethernet IP of Concentrator

When these settings are complete, the PC will have network access.

Static IP Setup

If your network requires each PC to have a statically set LAN IP addresses, follow the previous procedure for all PCs on the network. If the network requires a mix of static and dynamically assigned IP addresses, assign static IPs outside the DHCP address range for PCs that require static IP addresses and allow the Concentrator DHCP to assign the remaining PC IP addresses.

Port Forwarding (Mapping)

Port Forwarding is used to provide remote access to third party devices on the LAN; such as Web Cameras. Port Forwarding routes incoming requests from the WAN, with a specific port to a local device with a static IP.

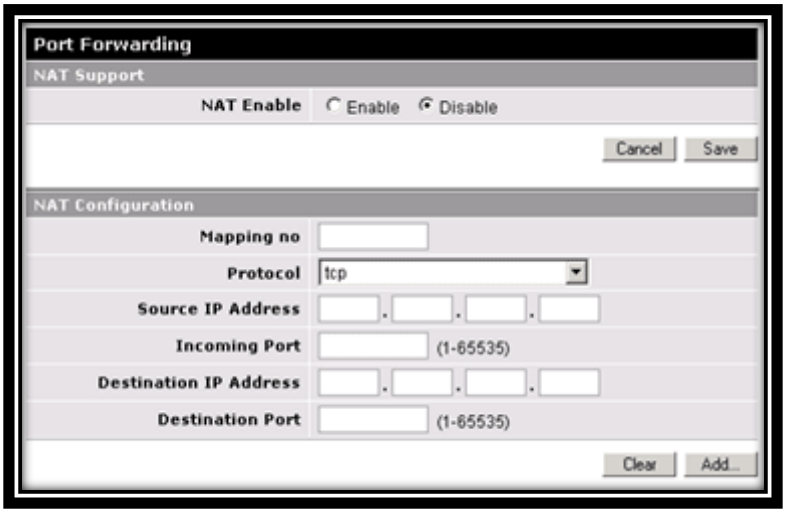


Figure 10: Port Forwarding Screen

NAT Enable	Select enable to allow port forwarding (default is disabled.)
Mapping Number	User selected generic number assigned for this route.
Protocol	TCP or UDP - driven by the protocol used by the third party device
Source IP Address	Enter the IP address of the remote PC connecting to the third party device. (This should only be done if a single PC with a STATIC IP is accessing the device and you want to limit access to the device.) If you will be accessing the third party device from multiple PCs, or from a PC that has a dynamically assigned WAN IP, enter 0.0.0.0 (wildcard) to allow all remote PCs to access the third party device.
Incoming Port	Enter the port of incoming request. This can be any non-conflicting port (can be the same as the destination port). This value must be entered following the

	Concentrator IP address into a browser on a remote PC to access the third party device.
Destination Address	IP address of any third party device. This device must be on the same subnet as the Concentrator.
Destination Port	Enter the port of the third party device. This will be assigned to the device by the third party manufacturer and should be in the user manual of the third party device. Important: The password protection on the Concentrator does not protect logging into a third party device. The third party device must provide its own password protection (confirm if password protection is required).

Click ***Add*** when route configuration is complete. The route will be displayed at the bottom of the page. Additional routes may be added but require a unique mapping number and port number. Routes can be deleted if no longer needed.

Once the route of the third party device is added you can enter the following on a remote PC to access the third party device.

http://70.209.115.93:81

Where 70.209.115.93 represents the PPP IP Address on the home page and :81 presents the incoming port on the NAT Configuration Menu page.

Dynamic DNS (NO-IP Configuration)

Dynamic DNS is an option for remote monitoring if a static WAN IP address is not available or not yet assigned. When Dynamic DNS is activated, the Concentrator will register its dynamically assigned IP address with NO-IP's application, allowing the user to login to the device remotely without knowing the IP address of the Concentrator.

A number of providers offer services to track dynamic IP addresses and map them to constant domain names. **The use of static IP is recommended whenever possible**.

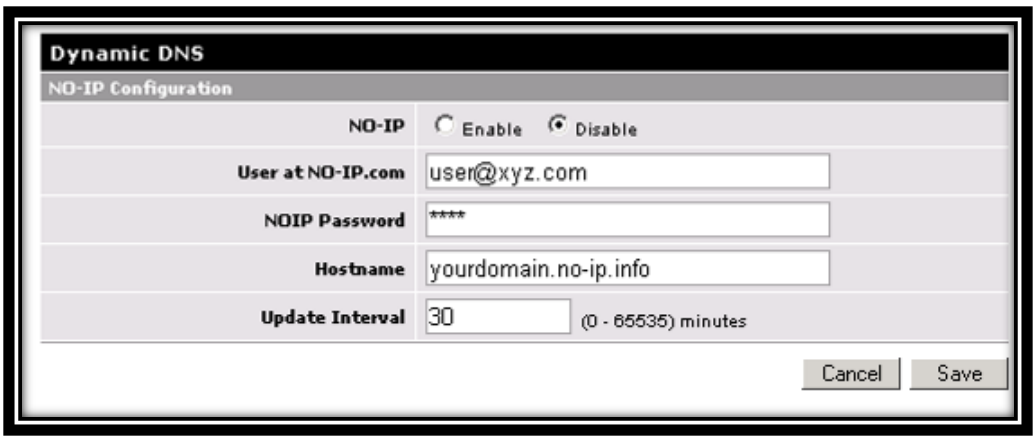


Figure 11: Dynamic DNS (NO-IP Configuration) Setup Screen

NO-IP	Enable/Disable, default is disabled
User at NO-IP.com	User name setup at NO-IP.com. This information is required when logging into your account
NOIP Password	Password used when logging into your account at NO-IP
Hostname	This is unique domain name setup on your NO-IP account. This is the domain name entered into a browser to remotely login to the Concentrator. You may have multiple host names registered on the same account. See section below for instructions to set up NO IP account and host name. *Important: Do not assign more than one Concentrator the same domain name.*
Update Interval	This setting determines how often the device will update its IP information at NO-IP. The IP addresses assigned by the carrier are dynamic; therefore it is necessary to update the registered IP periodically. Setting a high value in this field may cause extended periods of no connection but will reduce the number of times the Concentrator registers, decreasing the amount data used on the contract. Setting a low value minimizes the chance of lost network connection but will increase the total amount of data used on the contract. The Concentrator will always register when first powered up or hardware reset.

Instruction for NO IP setup

To setup an account at NO-IP.com, enter http://www.no-ip.com/ in your web browser. You will need to setup a user name and password on your account.

1. On No-IP, create a host account for each device you want to remotely monitor. The domain name you set up here will be used to remotely login to the device.
2. On the Concentrator, click “Dynamic DNS” on the left side of the web Browser.
3. Enable NO-IP
4. Enter your NO-IP username, password and hostname for this device (do not assign the same host name to multiple devices.)

5. Set the update interval (30 minutes is the default).

After registration is complete, you can login into the unit or use the port forwarding feature by entering the hostname into a web browser followed by the port.

Example: http://Concentrator_user.no-ip.biz:8080

System Upgrade

It is possible to update the system by receiving an update file from Calamp Corp. This may be done periodically to add features or fix errata. When you receive an update file, perform the following to update the unit. Upgrading can only be performed from a local PC, not remotely.

1. Save the file on a local drive or network accessible directory.
2. On the System Upgrade page, browse to the update file and select it.
3. Click Save. The system update can take up to 4 minutes. The unit will restart when the upgrade is completed. This will not delete your configuration settings.

SECTION 8 – TROUBLESHOOTING

This section lists some of the most common problems occurred while setting up the Concentrator unit and troubleshooting tips to fix the problem.

Cannot Connect to the Home Page

Step 1: Open a DOS command prompt on your PC, using Start → Programs → Accessories → Command Prompt. Enter the command "**ipconfig**" at the prompt to display all IP information assigned to the PC including the IP address, subnet mask and gateway.

The Default gateway should be "192.168.1.55" if you are using a new Concentrator, this should be whatever was assigned as the Ethernet IP of the Concentrator during previous configurations.

If this is the address, skip to step 2.

If the address is other than expected, but is a private IP (see Network basics) and the IP address and gateway are on the same subnet, enter that address in a browser to establish connection. If this does not fix the problem, skip to step 2

If the gateway is not the expected value and does not follow the above format,

1. Close all active browsers
2. On the "Network and Dial-Up Connections Page" confirm that the network settings are set to automatically detect an IP and DNS server.
3. Verify that there are no other active connections; specifically be sure that all wireless cards are disabled.
4. Disable, and then Re-enable the network connection. (Some older versions of Windows do not update network setting automatically, you need to re-enable the network settings or restart the PC to set updated network settings.)
5. Enter "ipconfig" in the command prompt; verify that the Default gateway is now correct.
6. Enter the gateway IP address into a browser, if this does not fix your problem skip to step 2. If the gateway is still not in the correct format, skip to step 3.

Step 2: Enter "ipconfig" in the command prompt as instructed above. The IP address should be of the format 192.168.1.xxx if you have new unit or should be on the same subnet if you have changed the Ethernet IP, but should not be the same as the Default gateway. If the IP address is in the correct format and not the same as the Gateway, skip to step 3. If it is not correct, open the properties window of the network connection. Manually enter a unique IP address on the same subnet as the gateway (use

192.168.1.100 if you have not changed the default) and save the properties. (Note: You may need to disable/re-enable the connection to get the new settings to take affect). This should allow you to connect to the device. Once you are connected, check the DHCP settings, the DHCP server may be disabled.

Step 3: Check the following

1. Confirm you are using a working Ethernet cable. Try a second Ethernet cable if necessary.
2. Confirm the Ethernet port you are plugging into on your PC is active
3. Confirm power supply for your unit is functioning. You should see LEDs flashing.

Cannot Connect to the Internet

1. Check the Signal Strength on the home page. If the signal strength is poor, check your antenna connections and placement. Try a different antenna if possible.
2. On the "Dial Settings" page, confirm that the autodial is enabled. If it is disabled, enable it and cycle power.
3. On the "WAN Cellular" page. Check that the correct mobile identification number is displayed, if an incorrect number or no number is displayed, it is an indication that your carrier contract is not activated, or the device has not been initiated. If you have not performed an over the air activation (OTASP for Verizon, IOTA for Sprint) perform that now.
4. If you have confirmed all of the above, or the over the air activation fails, contact your network provider to confirm that your contract is active.

Internet Connection is Slow or Intermittent

The speed and strength of your Internet connection can be affected by many things out of the control of the Concentrator such as your location and the overall level of network traffic. CalAmp does not guarantee any speed or coverage.

1. Check the signal strength on the home page. If it is listed as good or medium, skip to the next step. You may want to refresh the home page a few times to make sure the signal strength is consistent. If the signal strength is poor, check you antenna connections or try a new antenna if possible. If this does not fix the problem, verify network coverage in your location with your network provider.
2. Check the Service type. If EVDO is listed, skip to the next step. If 1xRTT is listed, WiMetry has not found an available EVDO network. The Concentrator will provide network access when only a 1xRTT connection is available but the speed of the network connection will be much slower. Contact your service provider to confirm EVDO coverage.

3. Check the DHCP lease time. If this is set to a high value (>1000 seconds), skip to the next step. If the lease time setting is set to 0 or a low value, reset to a higher value. Unless you have a specific reason for limiting the lease time, this should always be set to the maximum value.

4. If you have completed all steps above and still have poor network performance, perform a speed test on the device to confirm the connection speed (example: speakeasy.net). If the speed test shows acceptable download and upload speeds, the problem is most likely with the specific Internet site you are trying to connect to and not the Concentrator.

Cannot Access Serial Ports

1. Verify that the cables are correct. Depending on the end device you are using, a null serial cable or a cross over cable may be required.

2. Verify that the port mapped to this serial port is not being used by any other function in the concentrator – including remote login, port forwarding or wireless channels.

3. Check the baud rate setting; verify that it matches the third party device baud rate setting.

4. Check the hardware flow control settings. A third party device that requires hardware flow control will not communicate on a serial channel that does not have hardware flow control active and vice versa.

Cannot Communicate on Local Wireless Network

Refer to “WiMetry IEEE802.15 Profile Specification” for information on wireless setup. Complete setup of wireless network is beyond the scope of this document.

SECTION 9 – SPECIFICATIONS

General Specifications

Product specifications are subject to change without notice.

Interface Connectors

- RJ45 Serial (RS-232) Connectors (x8)
- RJ9 Serial (RS-422/RS-485) Connector
- Standard USB Host port
- Standard USB Client port
- RJ45 Ethernet Connection 10/100
- DB9 RS-232 Serial Port
- Molex 43045-1010 MicroFit 3.0, 10 pin header

Power Connector
Molex 43045-4000 MicroFit 3.0, 4 pin header

LED Indicators
POWER, SERVICE, ACTIVITY, SIGNAL, ZIGBEE

Antenna Interface

- Primary Antenna: 50 ohm TNC Female
- IEEE 802.15.4 Antenna: Internal PCB antenna
- SMA connector for external antenna (optional)

Size
6.875 L x 6.875 W x 3.0 H (inches) – does not include external connectors or antennas

Weight
2.65lb (1.2 kg)

Power Input
95-264VAC, 50/60Hz

Maximum TX Power

CDMA	+23.5 dBm min
802.15.4	23 dBm max

Rx Sensitivity

CDMA	>-104 dBm
802.15.4	TBD

Frequencies

Cellular	TX: 824-849 MHz; Rx: 869-894 MHz
PCS	TX: 1850-1910 MHz; Rx: 1930-1990 MHz

802.15.4 2460 – 2535 MHz

Temperature

Operating	-40°C to +85°C 100%; Cellular TX power may be reduced >70°C and <-30°C
Storage	-40°C to +85°C (-67° to 185°F)

Vibration

Certified by MIL-STD-810F Method 514.4

Shock

Certified by MIL-STD-810F, Method 516.5

Emissions

Passed FCC Part 15b testing

Transport Protocols

UDP/TCP

Command Protocol

Web Interface

Certifications

FCC ID (Cellular)	N7N-MC5725
IC (Cellular)	2417C-MC5725
FCC ID (802.15.4)	J26-500004

Power consumption while transmitting is dependent on the TX power level of the cellular module. The TX power level of the module is controlled by the cellular base station, not the Concentrator software

SECTION 11 – SERVICE AND SUPPORT

Product Warranty

CalAmp Corp guarantees that every WiMetry Concentrator Cellular Modem will be free from physical defects in material and workmanship for one (1) year from the date of purchase when used within the limits set forth in the Specifications section of this manual.

The manufacturer's warranty statement is available in Appendix 1. If the product proves defective during the warranty period, contact CalAmp Customer Service to obtain a Return Material Authorization (RMA).

RMA Request

Contact Customer Service:
Mon-Fri, 8:00 AM - 5:00 PM CST
Phone: (507) 833-8819; Toll Free: (800)-992-7774; E-Mail: imcsupport@calamp.com

BE SURE TO HAVE THE EQUIPMENT MODEL AND SERIAL NUMBER, AND BILLING AND SHIPPING ADDRESSES ON HAND WHEN CALLING.

When returning a product, mark the RMA clearly on the outside of the package. Include a complete description of the problem and the name and telephone number of a contact person. RETURN REQUESTS WILL NOT BE PROCESSED WITHOUT THIS INFORMATION.

For units in warranty, customers are responsible for shipping charges to CalAmp. For units returned out of warranty, customers are responsible for all shipping charges. Return shipping instructions are the responsibility of the customer.

Product Documentation

CalAmp reserves the right to update its products, software, or documentation without obligation to notify any individual or entity. Product updates may result in differences between the information provided in this manual and the product shipped. For the most current product documentation, visit www.calamp.com.

Technical Support

Contact Technical Support:
Mon-Fri, 8:00 AM - 5:00 PM CST
Phone: (507) 833-8819; Toll free: (800)-992-7774
E-Mail: imcsupport@calamp.com

APPENDIX 1 – WARRANTY STATEMENT

CalAmp warrants to the original purchaser for use ("Buyer") that data telemetry products manufactured by Dataradio ("Products") are free from defects in material and workmanship and will conform to published technical specifications for a period of, except as noted below, one (1) year from the date of shipment to Buyer. CalAmp makes no warranty with respect to any equipment not manufactured by Dataradio, and any such equipment shall carry the original equipment manufacturer's warranty only. CalAmp further makes no warranty as to and specifically disclaims liability for, availability, range, coverage, grade of service or operation of the repeater system provided by the carrier or repeater operator. Any return shipping charges for third party equipment to their respective repair facilities are chargeable and will be passed on to the Buyer.

If any Product fails to meet the warranty set forth above during the applicable warranty period and is returned to a location designated by CalAmp. CalAmp, at its option, shall either repair or replace such defective Product, directly or through an authorized service agent, within thirty (30) days of receipt of same. No Products may be returned without prior authorization from CalAmp. Any repaired or replaced Products shall be warranted for the remainder of the original warranty period. Buyer shall pay all shipping charges, handling charges, fees and duties for returning defective Products to CalAmp or authorized service agent. CalAmp will pay the return shipping charges if the Product is repaired or replaced under warranty, exclusive of fees and duties. Repair or replacement of defective Products as set forth in this paragraph fulfills any and all warranty obligations on the part of CalAmp.

This warranty is void and DRL shall not be obligated to replace or repair any Products if (i) the Product has been used in other than its normal and customary manner; (ii) the Product has been subject to misuse, accident, neglect or damage or has been used other than with CalAmp approved accessories and equipment; (iii) unauthorized alteration or repairs have been made or unapproved parts have been used in or with the Product; or (iv) Buyer failed to notify CalAmp or authorized service agent of the defect during the applicable warranty period. DRL is the final arbiter of such claims.

THE AFORESAID WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED AND IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. DRL AND BUYER AGREE THAT BUYER'S EXCLUSIVE REMEDY FOR ANY BREACH OF ANY OF SAID WARRANTIES IT AS SET FORTH ABOVE. BUYER AGREES THAT IN NO EVENT SHALL DRL BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT OR EXEMPLARY DAMAGES WHETHER ON THE BASIS OF NEGLIGENCE, STRICT LIABILITY OR OTHERWISE. The purpose of the exclusive remedies set forth above shall be to provide Buyer with repair or replacement of non-complying Products in the manner provided above. These exclusive remedies shall not be deemed to have failed of their essential purpose so long as DRL is willing and able to repair or replace non-complying Products in the manner set forth above.

This warranty applies to all Products sold worldwide. Some states do not allow limitations on implied warranties so the above limitations may not be applicable. You may also have other rights, which vary from state to state.

EXCEPTIONS

THIRTY DAY: Tuning and adjustment of telemetry radios

NO WARRANTY: Fuses, lamps and other expendable parts

Effective 1/2008

APPENDIX 2 – ABBREVIATIONS

CDMA	Code Division Multiple Access
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DNS	Domain name Server
ESN	Electronic Serial Number
EVDO	Evolution Data Optimized
GPS	Global Positioning System
IOTA	Internet Over the Air
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
NAT	Network Address Translation
OTA	Over the Air
OTASP	Over the Air Service Provisioning
PAD	Packet Assembly/Disassembler
PRL	Preferred Roaming List
RSSI	Receive Signal Strength Indication
RTS	Request to Send
WAN	Wide Area Network
USB	Universal Serial Bus