

Encrypted EtherPoll-2

User's Guide

Revised Nov. 17, 2006

Firmware Version 1.0

FCC Statement

This device complies with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Copyright © 2006. All rights reserved.

Version 1.0

All trademarks and trade names are the properties of their respective owners.

TABLE OF CONTENTS

Chapter 1 Introduction	1
Encrypted EtherPoll Functions.....	2
Other Features	3
Physical Details	4
Configuration Switches	5
LED Indicators.....	5
Package Contents.....	6
Software Requirements.....	6
Chapter 2 Installation	7
Overview	7
LAN Installation.....	7
Chapter 3 The Configuration Process	8
Overview	8
Using the Configuration Flexibility.....	8
Configuration Process Examples.....	9
Chapter 4 Terminal/Telnet Configuration.....	10
Overview	10
Terminal Configuration	10
Procedure.....	10
Telnet Configuration	11
Terminal/Telnet Interface.....	12
Entering Data.....	12
Menu Options	12
Main Menu Option 1. Setting Administration Values	13
Main Menu Option 1.4 Setting SNMP Administration Values	13
Main Menu Option 2. Set Serial Port Values	14
Main Menu Option 2.9. Serial Port Advanced Configuration.....	15
Main Menu Option 3. Enter Remote IP addresses.....	16
Main Menu Option 4. Configure Ethernet LAN.....	17
Main Menu Option 5. Display Settings	17
Main Menu Option 6. Display / Reset Current Status	18
Main Menu Option 7. Reset Configuration to Default	19
Main Menu Option 8. Save and Activate	19
Main Menu Option 1.3 Security Configuration.....	20
Main Menu Option 9. Exit without Saving.....	20
Chapter 5 Browser Configuration	21
Overview	21

Connection Procedure	21
Web-based Interface.....	23
Serial Port Configuration Screen	24
Port Activity Screen.....	25
Serial Port Advanced Configuration Screen	26
LAN Configuration Screen.....	28
SNMP Configuration Screen	30
Configure Remote IP Addresses Screen	31
Configuration Summary Screen.....	32
Administrative Tools Screen	33
Admin Password.....	34
Set Clock.....	35
Set All Defaults.....	36
Ping, Traceroute, Sniffer Tools	37
Transfer Configuration File	38
Firmware Upload	39
System Reboot.....	40
Version Information Screen.....	41
Chapter 6.....	42
Security.....	42
Overview	42
Data Security	42
Configuration Security.....	42
Configuration Level 0:	42
Configuration Level 1:	43
Configuration Level 2:	43
Configuration Level 3:	43
Chapter 7 Operation	44
Normal Mode.....	44
Broadcast Mode.....	44
Point-to-Point Mode	44
RTS Toggle Feature	44
Chapter 8 Troubleshooting.....	47
Hardware Problems	47
Can't Connect via the LAN.....	48
Other Problems.....	49
Checking Device Operation	50
Appendix A Specifications.....	51
Encrypted EtherPoll Specifications	51
RS-232 PIN Assignments.....	52

Control Signal Operation.....	52
CABLES.....	53
Appendix B Advanced Operation	54
Introduction	54
Description and Behavior	54
Ports used by the Encrypted EtherPoll	54
Normal Operation Modes	54
Point - to - Point Mode	54
Broadcast Mode	55
Transmit Conditions	55
SCADA Protocols.....	55
Appendix C Open Source Software Information	56
Introduction	56
Obtaining the Source Code.....	56

Chapter 1

Introduction

This chapter provides an overview of the Encrypted EtherPoll's features and capabilities.

Congratulations on the purchase of your new Encrypted EtherPoll. The Encrypted EtherPoll is a SCADA communications serial server that allows multi-drop devices to use Ethernet LAN's. The Encrypted EtherPoll connects any asynchronous serial devices through a LAN and between LAN's via routers. The Encrypted EtherPoll is designed specifically to support asynchronous polling protocols, such as Poll Select, Modbus, DNP, etc. These protocols are often error corrected, and the Encrypted EtherPoll allows these protocols to work through routed LANs and over IP protocol networks. The Encrypted EtherPoll uses the UDP/IP protocol, allowing the necessary data connection over a local LAN and across routed networks.

The Encrypted EtherPoll functions independently of the device protocol, allowing most 8 bit asynchronous protocols to be used with no configuration changes.

The Encrypted EtherPoll can receive data from any Serial device, convert the data to a valid IP packet, and transmit that data over the LAN/WAN in encrypted packets. Serial devices may then be accessed from anywhere on your LAN/WAN by any workstation computer using another Encrypted EtherPoll. Two Encrypted EtherPolls may be used in “nailed-up” mode to build an encrypted “RS-232 path” through the WAN/LAN using UDP/IP packets.

Most Encrypted EtherPolls are used with multi-drop SCADA RTUs; although a pair of Encrypted EtherPolls configured for point-to-point operation may be used by any async serial devices such as alarms, access control devices, and Multiplexers.

For easy connection to your LAN, the Encrypted EtherPoll supports 10BaseT or 100BaseT with autosensing.

NOTE: A similar product, the EtherPath, uses TCP/IP protocol and may be more appropriate for some installations. If the application is not a polled environment, the EtherPath should be investigated. There are also protocol aware products in the EtherSeries line of serial servers and gateways, as well as a single port non-encrypted EtherPoll.

Encrypted EtherPoll Functions

The Encrypted EtherPoll is usually used in a host-to-multiple remote polled environment.

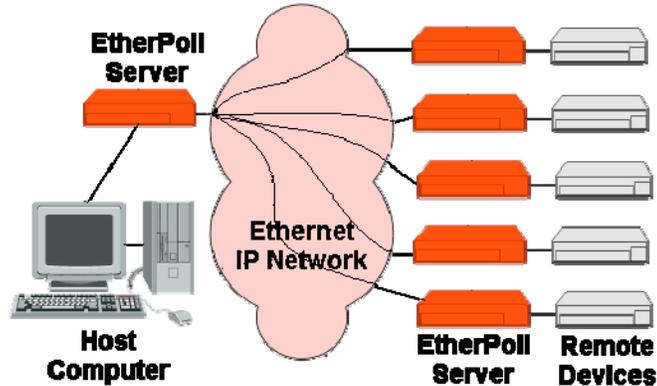


Figure 1: Normal Mode of Operation

Normal Operating Mode (Point-to-Multi-Point)

In this mode, several Encrypted EtherPolls are used. All are connected to serial RS-232 devices. This is the equivalent to using a multi-drop analog modem network... only it uses ethernet as the medium and encrypts the data in transit.

- The "host" Encrypted EtherPoll will be configured with IP addresses of each "remote" Encrypted EtherPoll. It is connected to a polling host computer.
- Each "remote" Encrypted EtherPoll is configured with the IP address of the "host" Encrypted EtherPoll. These are each connected to a remote terminal unit (RTU).
- Whenever the host computer polls the remotes, a copy of the poll block is sent to each remote in the host Encrypted EtherPoll's address list.
- The proper remote RTU will respond to the poll through its Encrypted EtherPoll with a poll response or appropriate data blocks, while other RTUs ignore the poll.

Point-to-Point Mode

This mode requires one pair of Encrypted EtherPolls. Each Encrypted EtherPoll is connected to a serial port device, and to the LAN.

Each Encrypted EtherPoll has only one IP address in its IP address list (that of the other unit). All data received by the RS-232 port of either Encrypted EtherPoll is sent to the other Encrypted EtherPoll and out its RS-232 port.

Broadcast Mode (Point-to-Multi-Point)

Point-to-multi-point (*broadcast*) operation allows a single Encrypted EtherPoll to broadcast all incoming data to multiple Encrypted EtherPolls. Configuration is identical to the normal mode, but since non-polling external devices are used, there is no implicit method to control data being sent back to the host unit. For this reason, it is normally used in "outbound broadcast data only" applications.

Normal Mode with Backup Polling Host

This mode is also similar to the normal mode, but allows a redundant polling host computer to monitor all data traffic, and take control for fail-safe operation should the master host fail. Configuration changes from normal mode are simple. Each remote Encrypted EtherPoll would have both the master and backup host Encrypted EtherPoll IP addresses in its IP address list. The master host would also have the backup host Encrypted EtherPoll address in its IP address list.

Each remote Encrypted EtherPoll sends its data to both the master and backup polling host. If the master host fails, the backup host should be programmed to take over the polling function. It would sense a failure by noting that master host polls are absent.

Other Features

UDP/IP Protocol

The Encrypted EtherPoll uses the UDP/IP protocol. This is much more efficient for a polling system than TCP/IP. Since most polled SCADA systems use protocols that are error corrected, the transport (Encrypted EtherPoll IP network) doesn't need to provide an additional layer of error correction overhead.

Protocol Independent

The Encrypted EtherPoll works well with any byte oriented asynchronous SCADA protocol. It does not require getting "into" the protocol blocks.

Easy Configuration

The Encrypted EtherPoll may be configured with a telnet session, web browser, or directly connected terminal

Encryption

The Encrypted EtherPoll encrypts the data field of every packet prior to placing it on the ethernet. A shared key is used with 128 AES to encrypt the data. One serial port may be used as an encrypted system while the second port is on an un-encrypted system.

Protocol Conversion

The RS-232 device at the client end and the device at the server end of a link do not have to use the same communications parameters on the RS232 link (speed, parity, flow control). The Encrypted EtherPolls will convert the data to the correct parameters (speed, format, parity) at each end.

Upgradeable Firmware

Firmware upgrades are downloadable to the Encrypted EtherPoll. The actual firmware upgrade images are available from your dealer or DCB.

Physical Details

The Encrypted EtherPoll front and rear panels are shown below.



Figure 1: Encrypted EtherPoll Rear

1	Power port	Connect the power adapter here.
2	10/100Base-T port	Connect LAN cabling here.
3	Dip Switches	See next section



Figure 1: Encrypted EtherPoll Front

1	Status LED	Normally On
2	Power LED	Always On
3	A LED	Port A Activity
4	B LED	Port B Activity.
5	Serial A	Serial Port A
6	Serial B	Serial Port B

Configuration Switches

The rear panel contains four small switches, numbered 1 through four (left to right). These are used for configuration.

The normal position for all switches is DOWN.

Switch 1

This switch immediately resets the unit . When placed in the UP position, it resets the unit just as if it had been power cycled.

Switch 2

This switch places the unit in basic configuration mode. It is used to provide a terminal interface for initial configuration. Powering up the unit with this switch UP, provides a terminal attached to the Serial-A port with a login prompt and the ability to manage the unit with a command line. This method is used to install an initial IP address in the unit.

Switch 3

Factory use only.

Switch 4

Factory use only.

LED Indicators

There are two red LED indicators on the rear panel adjacent to the LAN connector and four red LED indicators on the front panel near each 9-pin serial connector.

Rear Panel LED Indicators

- The lower red LED is the Ethernet Status indicator. It is lit when there is a valid Ethernet connection
- The upper red LED is a LAN activity indicator. This LED flashes with activity on the Ethernet (even if the activity isn't directly to this unit).

Front Panel LED Indicators

- Lower Left LED is a power indicator.
- Upper Left LED is a status indicator. It should be on.
- Upper right LED flickers with activity on Serial Port B.
- Lower right LED flickers with activity on Serial Port A.

Package Contents

You should find the following items packaged with your Encrypted EtherPoll:

- The Encrypted EtherPoll Unit
- Power Adapter
- This User's Guide

If any of the above are missing, contact your dealer immediately.

Software Requirements

The Encrypted EtherPoll supports the following Ethernet protocols.

- UDP/IP (used for data transfer)
- TCP/IP (if used for configuration)
- ARP
- ICMP
- TELNET (if used for configuration)
- HTTP (if used for configuration)
- SNMP (if used for management)

It may be configured using any terminal or terminal emulation software on a PC. Any standard web browser may be used for configuration once the Encrypted EtherPoll has a valid IP address configured.

Chapter 2

Installation

This Chapter details the LAN installation process for the Encrypted EtherPoll.

Overview

For *Telnet Mode* or *Web Browser Mode* configuration, LAN installation is performed before configuration. There must also be a valid IP address in the unit prior to configuration with these methods. The default value may not work with your network.

If you use *Terminal Mode* configuration, then the configuration should be performed prior to LAN installation. See Chapter 3 for details.

LAN Installation

1. Connect the Network Cable

The Encrypted EtherPoll network interface is 10/100BaseT auto-sensing. Simply connect your network cable to the appropriate connector on the Encrypted EtherPoll panel.

2. Connect the Power Adapter Cable

Plug in the power adapter cable. After about a boot process the Encrypted EtherPoll is ready for operation.

3. Connect the Serial Port Device

Connect the serial port device to the serial port on the Encrypted EtherPoll. **If connecting to a PC 9-pin port, a cross-over (null modem) cable is required.** See the Appendix for wiring details.

4. Apply power to the serial port device.

Chapter 3

The Configuration Process

This Chapter describes configuration management process on the Encrypted EtherPoll using a Web Browser.

Overview

The Encrypted EtherPoll contains a quite flexible configuration management system. By using this system correctly, one can remotely configure the unit, save copies of that configuration to a PC, change configuration changes for later activation, and remote transfer firmware upgrades to the unit.

There may be up to three configuration “images” in use at any time.

1. The **active** configuration. Normally, this is the configuration that was loaded from memory when the unit was last booted. However it may have been changed since boot time as described below. This is the configuration that is currently running the unit.
2. The **pending** configuration: This is the current configuration that was loaded from memory when the unit was last booted WITH any changes made by using the configuration screens. This configuration is NOT the configuration running the unit at present.
3. The **stored** configuration. This is the configuration that was last written to the unit’s non-volatile RAM. The next time the unit boots, it will start running this configuration.

Note that any configuration transfer (with the Administration Configuration Transfer screen) is the *working* configuration. You can load a configuration file from the PC, then either activate it to test it. Or, save it without activation if you don’t want to change the currently running.

Using the Configuration Flexibility

When the unit starts from a power-off condition, it loads an active configuration from its non-volatile memory. This active configuration is also copied to the working configuration.

Whenever the configuration screens are used to change values, **only** the *pending* configuration is changed... not the *active* configuration.

Using the configuration screens will change the pending configuration. You may change the active configuration by copying the pending configuration over it. This change is performed using the “Activate Configuration” screen. Going to this screen activates the pending configuration by copying the pending configuration over the top of the active configuration. This does not store the configuration in non-volatile memory. When the unit is next reset or powered up, it will begin using the old stored configuration from before the changes and activate command. Unless...

Using the store configuration screen will copy the pending configuration into Non-volatile memory. It will not cause this configuration to begin running the unit. However, upon the next reset or power cycle, the unit will begin using the stored configuration.

It is possible to activate the pending configuration using the Activate Configuration screen and then store the configuration using the Store Configuration screen. This two step process will cause all three configurations to be identical.

Configuration Process Examples

Make configuration changes, test them with Activate, then save them with Save.

This is the most commonly used method for changing the configuration. It allows you to test the configuration prior to saving it. If, during the testing, you notice an abnormality; you can reset to return to the last good configuration.

Make configuration changes, save them, reset to activate the changes.

This method allows one to configure while not immediately using the new configuration. Make the changes to the pending configuration and save them. Your current session will not be affected, but when reset, the unit will begin using the new configuration. This method is useful when you are configuring to use a new LAN address range while it is on the old LAN.

Transfer a saved configuration to the unit, save it, reset the router to activate the changes.

It is useful to transfer an existing configuration to a PC text file for future use. Then if the unit must be replaced, simply transfer that stored configuration to the new router.

If the PC is in the default IP address range of the new unit (192.168.0.x subnet), then a new, out-of-the-box unit is easily configured using this method. Start the new unit, transfer a stored configuration file, and store it. When it is restarted, it will have the proper configuration.

Note regarding saved configurations

The saved configuration file is a simply formatted raw text file. Advanced users may wish to edit this file using an appropriate text editor , then transfer the changed configuration to a router.

Use care when performing configuration with this technique as the text configuration file must be in the proper format.

This method is ideal for automating the configuration of many units in a large corporate environment.

Chapter 4

Terminal/Telnet Configuration

This Chapter describes how to configure the Encrypted EtherPoll using Terminal, or Telnet mode. Web Browser mode configuration is detailed in Chapter 5.

Overview

The Encrypted EtherPoll can be configured using any of the following methods:

- **Web Browser** - After installing the Encrypted EtherPoll in your LAN, use your Web Browser for configuration. See *Chapter 4 - Browser Configuration* for details.
- **Terminal Mode** - Use a serial cable connection and a communication program. The advantage of this method is that you give the Encrypted EtherPoll a compatible IP Address prior to installation in your network.
- **Telnet Mode** - After installing the Encrypted EtherPoll in your LAN, connect to it using Telnet.

Both *Terminal* and *Telnet* modes provide the same user interface.

Terminal Configuration

Terminal configuration requires the following:

- PC with terminal emulation program, or a dumb terminal.
- Serial cable to connect the PC to the Encrypted EtherPoll. See the Appendix for cable requirements. A Crossover (null modem) cable is required when using a 9 pin PC port.

Procedure

1. Connect the Encrypted EtherPoll to your PC or terminal.
2. Connect the Encrypted EtherPoll to the power supply.
3. Raise switch 2 on the rear of the EtherPoll
4. Configure the terminal program with the following settings.

Setting	Value
Flow control protocol	None
Speed	9600
Data	8 bits
Parity	None
Stop Bit	1

5. Connect your terminal program to the appropriate port (e.g. COM 1).
6. The configuration program should now start and after a few seconds display a sign-on screen.
If nothing appears on your screen, press ESC.
Refer to *Terminal/Telnet Interface* on page XXX for details on using the configuration program.

Telnet Configuration

NOTE: For telnet to work properly, there MUST be compatible IP addresses in both the PC and the Encrypted EtherPoll!

1. Install the Encrypted EtherPoll into your LAN as described in Chapter 2. Ensure that the Encrypted EtherPoll is powered on.
2. Connect to the Encrypted EtherPoll with the command:

```
telnet IP_Address Port_number
```

Where:

IP_Address is the IP address of the Encrypted EtherPoll

Port_number (for configuration) is 8000.

For example, if the default IP address had not been changed, then you would enter the command:

```
telnet 192.168.1.1 8000
```

If you can't connect

If the Encrypted EtherPoll does not respond, check the following:

- The Encrypted EtherPoll is properly installed, LAN connections are OK, and it is powered ON.
- Check that your PC is using a compatible *IP Address* and *Network Mask*.

In Windows, the IP Address and Network Mask can be checked by using *Control Panel-Network* to examine the *Properties* for the TCP/IP protocol. If your PC is NOT using an IP Address within the range 192.168.1.2 to 192.168.1.254, with a Network Mask of 255.255.255.0, then it will not connect to the default Encrypted EtherPoll IP address.

3. Refer to the following section for details on using the configuration program.

Terminal/Telnet Interface

The Signon screen displays the version number.

```
Escape character is '^]'.  
Enter name: admin  
Enter password:
```

Entering the default user name (admin) and press return for the password will then take you to the Main Menu.

```
---- Welcome to the EEP-2 version v0_01 Setup  
Program ----  
  
1 Set Administration Values  
2 Set Serial Port Values  
3 Set/Delete Remote IP Values  
4 Set Ethernet LAN values  
5 Display Settings  
6 Display/Reset Current Status  
7 Reset Default Settings or Reset Unit  
8 Save and Activate  
9 Exit without Saving  
  
Select a function by number ->:
```

Each of these menu options is explained in the following pages.

Entering Data

Enter the number of the field you wish to change, followed (on the same line) by a space and the data for that field.

Example

On screen one, to set the IP address (field 1) to 192.168.1.10

```
=>1 192.168.1.10
```

Menu Options

Main Menu Option 1. Setting Administration Values

Selecting 1 (Set Administration Values) from the Main Menu will result in a screen similar to the following.

```

Username: admin          Password:
---Administration Values -----
 1 Username
 2 Password
 3 Access Control Values [submenu]
 4 SNMP Values          [submenu]
 0 --Return to previous menu.
Press ? for help ->:

```

1. User Name

This field may be a string of 0 to 15 printable characters. Do not use space or control characters. If you leave this field blank, you will need to enter a blank username during authentication.

2. Password

When changing the username and password, this field provides the new password. It may be a string of 0 to 15 characters. If you leave this field blank, you will need to enter a blank password during authentication.

3. Access Control Values

This takes you to a submenu for Access Control management. See the Access Control section for details

4. SNMP Values

This takes you to a submenu for SNMP values. See the SNMP section for details.

Main Menu Option 1.4 Setting SNMP Administration Values

Selecting 1 (Set SNMP Values) from the Main Menu will result in a screen similar to the following. All standard SNMP values are configured using this screen. The EEP-2 responds only to SNMP queries.

```

SNMP server: disable      Contact Person: Supervisor
Device Name: GW3B00414D   Physical Location: Head Office
SNMP Community: public
---SNMP Values -----
 1 SNMP server  [0=disable, 1=enable]
 2 Contact Person
 3 Device Name
 4 Physical Location
 5 SNMP Community
 0 --Return to previous menu.
Press ? for help ->:

```

These are text fields, commonly used in SNMP (Simple Network Management Protocol) Programs to identify this device when browsing or managing the network.

These values have no effect on the data operation of the Encrypted EtherPoll. Other standard MIB values are returned to the SNMP manager along with this information. The Encrypted EtherPoll may not be remotely configured using SNMP.

The MIB file is available from the DCB website.

Main Menu Option 2. Set Serial Port Values

Selecting (2) from the Main Menu will display a prompt asking for the serial port number to configure (1 or 2). Then the configuration menu will be displayed. Each serial port is independently configured.

```
Baud Rate: 57600          Flow Control: none
Parity: none             Data Bits: 8
Stop Bits: 1            Connection Control: nailed-up
Encryption Mode: unsecured  Etherpoll UDP Port: 3000
---Serial Port Values -----
1 Baud Rate              [0=300, 1=1200, 2=2400, 3=4800, 4=9600,
                        5=19200, 6=38400, 7=57600, 8=115200,
                        9=230400, 10=460800]
2 Flow Control           [0=none, 1=xon/xoff, 2=cts/rts,
                        3=rts-toggle]
3 Parity                 [0=odd, 1=even, 2=none]
4 Data Bits              [0=7, 1=8]
5 Stop Bits              [0=1, 1=2]
6 Connection Control     [0=nailed-up, 1=DCD-input]
7 Encryption Mode        [0=unsecured, 1=encrypted]
8 Etherpoll UDP Port
9 Serial 1 Advanced Config Values [submenu]
0 --Return to previous menu.
Press ? for help ->:
```

Baud Rate

Speeds between 300 bps and 230.4Kbps are supported.

This screen allows you to change the settings for the RS232 link. The settings used should match the device connected to the serial port of the Encrypted EtherPoll.

Parity

The choices are “None”, “Odd”, or “Even”.

Flow Control

The choices are “None”, “XON/XOFF”, “RTS/CTS”, and RTS Toggle. See section 6 for detailed information on RTS Toggle is that feature is required.

Data Bits

The choices are 7 or 8.

Stop Bits

The choices are 1 or 2.

Connection Control

Selects whether connections are always allowed (Nailed-up) or only when the serial input pin (DCD) is active.

Encryption Mode

If enabled, encryption using 128 bit AES is applied to data from this port. If not enabled, the data is broadcast over the ethernet in the clear.

UDP Port

The UDP port number associated with this port. Defaults are 3000 for port 1 and 3001 for port 2.

Serial Advanced Values Menu

This brings up another menu for the Advanced Configuration of this port. See that section for details.

Main Menu Option 2.9. Serial Port Advanced Configuration

Selecting (4) from the Main Menu will display the following:

```

Transmit Timer (ms): 20          Timer Mode: transmit-timer
Block Size: 512
Line terminator Character (Decimal 0-255): 13
Transmit On LT Char: off        Local Character Echo: off
Shared secret:
---Serial-B Advanced Values -----
 1 Transmit Timer (ms)
 2 Timer Mode                    [0=transmit-timer, 1=idle-timeout]
 3 Block Size
 4 Line terminator Character (Decimal 0-255)
 5 Transmit On LT Char            [0=off, 1=on]
 6 Local Character Echo           [0=off, 1=on]
 7 Shared secret
 0 --Return to previous menu.
Press ? for help ->:

```

The Encrypted EtherPoll has a built-in buffer to store data, and most of these settings affect the operation of the buffer. The default values should normally be satisfactory.

1. Transmit Timer

If set to "Transmit Timer mode", this is the time period for which data will be stored in the buffer before being sent. It is a free running clock. Upon every "tic" of the clock, if there is data in the buffer, a packet is sent out the ethernet port.

If set to "Idle Timeout mode", this is an idle timer. Any data in the buffer is sent out the ethernet port after the Encrypted EtherPoll detects this length of time with no incoming data on the RS-232 port.

Allowable values range from 1msec to 10,000msec (10 seconds) for both timers. Only one is used at a time. Default value is 20 msec.

2. Timer Mode

When set = 0, the transmit timer is used. If set = 1, the idle timeout mode is used.

3. Block Size

The maximum ethernet packet buffer size. The minimum value is 1 byte, the maximum 4096 bytes (4 K). Note that a minimum ethernet packet is 64 bytes, so extremely small values may be inefficient. The timer (above) usually overrides this value. When "block size" characters are in the buffer, a packet is sent out the ethernet port even if timer criteria has not been met, so the block size should be large enough to prevent fragmentation if data blocks should not be fragmented.

4. Line Terminator Character

This setting is used to change the Line Terminator Character. The Line Terminator Character causes any data in the buffer to be transmitted immediately when the character is received, provided the following setting (Transmit_on_LT_Char) is ON.

5. Transmit_on_LT_Char

When this setting is ON, any data in the buffer will be sent immediately upon receipt of a Line_Terminator_Character (see previous setting). When the setting is OFF, the Line_Terminator_Character has no effect.

This is usually set OFF for SCADA applications.

6. Client Local Character Echo

If ECHO is ON, the Encrypted EtherPoll will locally echo all incoming characters.

If ECHO is OFF, the Encrypted EtherPoll will not echo characters or transmit any status messages to the serial port. This mode should be used if any messages from the Encrypted EtherPoll would create interference.

This is usually set OFF for SCADA applications.

7. Shared Secret

The shared secret is used to generate the secret keys used in the encrypted mode. This shared secret should include numbers and letters and be at least 32 characters long. All nodes in a encrypted network **MUST** use the same shared secret. If two units using the encrypted mode don't have the same shared secret, they will not be able to communicate. The units default to an internal shared secret if the field is blank. This is OK for testing, but **MAKE SURE YOU CHANGE THIS** when the units are deployed. Otherwise, anybody who buys an Etherpoll X2 who can gain access to your Ethernet traffic could decrypt your Etherpoll data!

Main Menu Option 3. Enter Remote IP addresses

Selecting (3) from the Main Menu displays a screen similar to the following example.

```
Enter port (1-2) or 0 to return: 1
---Set/Delete Remote IP Values -----
205.166.54.186
```

Use this screen to enter or delete remote IP addresses from the poll list. Only remote EtherPolls having addresses in this table will be sent the data from this port. Data destined for this port is only accepted from IP addresses on the table.

Main Menu Option 4. Configure Ethernet LAN

Selecting (3) from the Main Menu displays a screen similar to the following example.

```
IP Address: 205.166.54.184      Subnet Mask: 255.255.255.0
Gateway IP Address:

---LAN Values -----
1 IP Address
2 Subnet Mask
3 Gateway IP Address
0 --Return to previous menu.

Press ? for help ->
```

Use this screen to enter the IP configuration values for this unit.

IP Address

Any IP address that is valid for this specific network.

Subnet Mask

The appropriate subnet mask for this specific network

Gateway IP Address

The appropriate gateway IP address for this specific network

Main Menu Option 5. Display Settings

Selecting (5) from the Main Menu displays a screen similar to the following example.

```
-----  
== LAN Values ==  
IP Address: 205.166.54.184          Subnet Mask: 255.255.255.0  
Gateway IP Address:  
-----  
== Administration Values ==  
Username: admin                    Password:  
-----  
== Manager Access Control Values ==  
Web Setup Enable: enable           Web Server Port: 80  
Telnet Setup Enable: enable        Telnet Setup Port: 8000  
Allowed Setup IP Address 1:        Allowed Setup IP Address 2:  
Allowed Setup IP Address 3:        Allowed Setup IP Address 4:  
Respond to Ping: enable  
-----  
== SNMP Values ==  
SNMP server: disable               Contact Person: Supervisor  
Device Name: GW3B00414D           Physical Location: Head  
Office  
SNMP Community: public  
press return for more, ESC to quit:  
-----  
== Serial Port Values - 1 ==  
Baud Rate: 57600                   Flow Control: none  
Parity: none                       Data Bits: 8  
Stop Bits: 1                       Connection Control: nailed-up  
Encryption Mode: unsecured         Etherpoll UDP Port: 3000  
-----  
== Serial Port Values - 2 ==  
Baud Rate: 57600                   Flow Control: none  
Parity: none                       Data Bits: 8  
Stop Bits: 1                       Connection Control: nailed-up  
Encryption Mode: unsecured         Etherpoll UDP Port: 3001  
-----  
== Serial-A Advanced Values ==  
Transmit Timer (ms): 20            Timer Mode: transmit-timer
```

Port-A status

```
== Network Socket 3000 ==  
205.166.54.186 -- rcv'd 0 sent 0 discarded 0 dropped 0  
Network bytes received from unlisted IP addresses : 0
```

== Serial Port ==

```
Baud rate : 57600  
character format : 81N  
Bytes received : 0  
Bytes transmitted : 0
```

Port-B status

```
== Network Socket 3001 ==  
Network bytes received from unlisted IP addresses : 0  
NO DEFINED REMOTES
```

```
Last bounce address 0.0.0.0 tot rcv'd 0 sent 0 discarded 0 dropped 0
```

== Serial Port ==

```
Baud rate : 57600  
character format : 81N  
Bytes received : 0  
Bytes transmitted : 0
```

press return for more, ESC to quit:

Zero port and ethernet statistics? (N,y):n

No
Ma
Al
M
D
Se
the
18

ered

Current Statistics

LAN Receive

Bytes, Packets, and Errors received on the ethernet interface.

LAN Transmit

Bytes, Packets, and Errors sent to the ethernet interface.

Serial Port RX count per port:

Characters received into the RS-232 port.

Serial Port TX count per port:

Characters transmitted out the RS-232 port.

Remote IP Activity counts per port

Displays IP address and packet count for each remote that has exchanged data with this Encrypted EtherPoll. If data has been received from a remote that is not in the IP address list, that information is also displayed along with the IP address of the **first** un-listed IP address. (**These packets are discarded.**)

Main Menu Option 7. Reset Configuration to Default

Selecting (7) from the Main Menu will restore all values to their default values.

```
Select a function by number ->: 7
To reset to default values, Press D.
To reset Unit, press R.
Press return to exit :
```

If using Telnet or web browser configuration, the connection will be lost when the Encrypted EtherPoll reboots. To reconnect, you must use the default IP Address of 192.168.1.1 or change the Encrypted EtherPoll IP address before rebooting with main menu option 7. The preferred method is to restore defaults with menu item 6, and then **BEFORE REBOOTING**, change the IP information using submenu 1 so your PC will still be able to connect to the Encrypted EtherPoll when it reboots.

Main Menu Option 8. Save and Activate

Selecting (8) from the Main Menu will store the configuration details in the Encrypted EtherPoll, and activate any pending changes.

If using Telnet, the connection may be lost when the Encrypted EtherPoll reboots. If you have changed the IP Address, you must use the new IP Address when you reconnect.

Main Menu Option 1.3 Security Configuration

The Encrypted EtherPoll contains extensive configuration security features. See Section 5, Security Configuration, for extensive details.

```
---Manager Access Control Values -----  
1 Web Setup Enable      [0=disable, 1=enable]  
2 Web Server Port  
3 Telnet Setup Enable   [0=disable, 1=enable]  
4 Telnet Setup Port  
5 Allowed Setup IP Address 1  
6 Allowed Setup IP Address 2  
7 Allowed Setup IP Address 3  
8 Allowed Setup IP Address 4  
9 Respond to Ping      [0=disable, 1=enable]  
0 --Return to previous menu.
```

Main Menu Option 9. Exit without Saving

Selecting (9) from the Main Menu will exit the configuration program without saving any data you have entered.

Chapter 5

Browser Configuration

This Chapter describes how to configure the Encrypted EtherPoll using a Web Browser.

Overview

This configuration method uses your Web Browser to configure the Encrypted EtherPoll. This provides a more user-friendly interface than the Telnet/Terminal method.

- The Encrypted EtherPoll must be installed in your LAN and have a compatible IP address before this configuration method can be used.
- Most Browsers will work. The only requirement is that they support HTML tables and forms. If your browser uses a proxy, the proxy function may need to be disabled.
- Some field details are not shown in this section. Refer to chapter 4, "Telnet/Terminal Configuration", for more details about the entry fields.

Connection Procedure

To establish a connection to the Encrypted EtherPoll, follow this procedure:

1. Install the Encrypted EtherPoll in your LAN as described in Chapter 2. Ensure that the Encrypted EtherPoll is powered on.
2. Start your Web browser.
3. In the *Address* box of your browser, enter the following:

```
http://IP_Address
```

(*IP_Address* is the IP address of the Encrypted EtherPoll)

For example, if the default IP address has not been changed, then you would enter the command:

```
Http://192.168.1.1
```

If you can't connect

If the Encrypted EtherPoll does not respond, check the following:

- The Encrypted EtherPoll is properly installed, LAN connections are OK, and it is powered ON.
- Check that your PC is using a compatible *IP Address* and *Network Mask*.

In Windows, the IP Address and Network Mask can be checked by using *Control Panel-Network* to examine the *Properties* for the TCP/IP protocol.

If your PC is NOT using an IP Address within the range 192.168.1.2 to 192.168.1.254, with a Network Mask of 255.255.255.0, it will not be able to communicate with the Encrypted EtherPoll.

4. Once connected, you will see the first screen. Refer to the following section for details on using the Web-based interface.

Web-based Interface

After entering the username and password (the default username is admin, there is no default password), the first screen is similar to Figure 2.

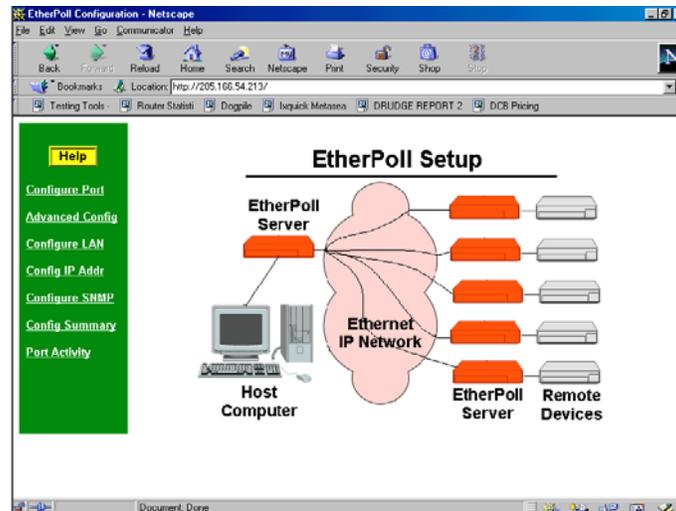


Figure 2: Sign on Screen

- Use the menu bar on the left to navigate to the desired screen.
- On-line help is available on each screen.
- Each screen is explained in the following sections.

Serial Port Configuration Screen

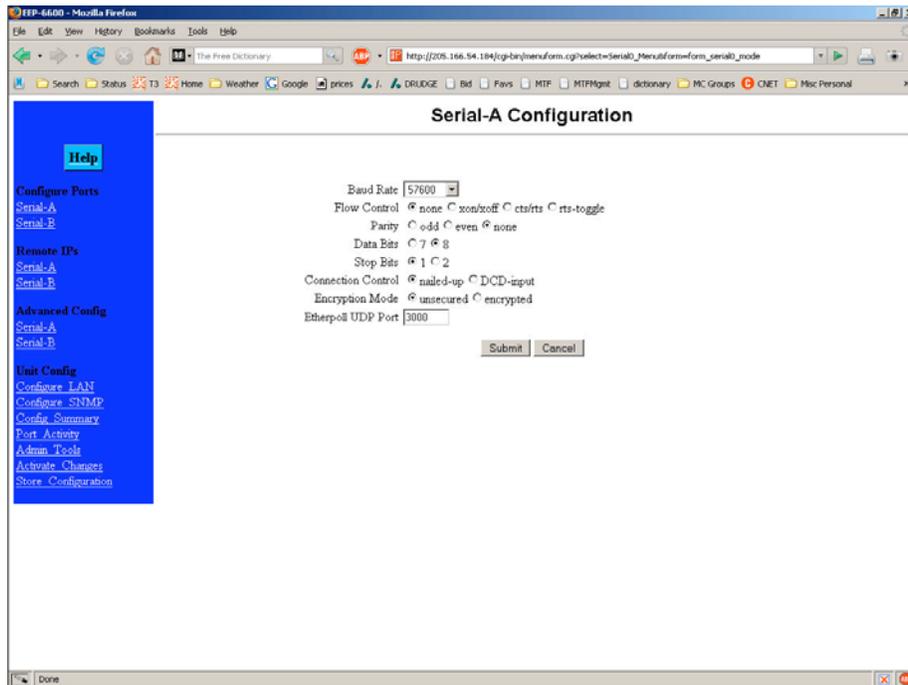


Figure 3: Serial Port Configuration Screen

This screen allows you to configure the Serial Port on the Encrypted EtherPoll. The settings used should match the device connected to the serial port of the Encrypted EtherPoll.

- Consult the documentation of your serial port device to determine the appropriate settings to match the device connected to this port.
- Connection Control Mode, See Section 6. Operation for details on how to set this. Normally “From Interface”.
- Encryption mode may be turned on or off for each serial port. All remotes using that port must use the same encryption secret if encryption is turned on. One port may be encrypted while the other is used in the clear.
- RTS Toggle is used with radio transmitters. See Appendix B for more information if this is required.

Port Activity Screen

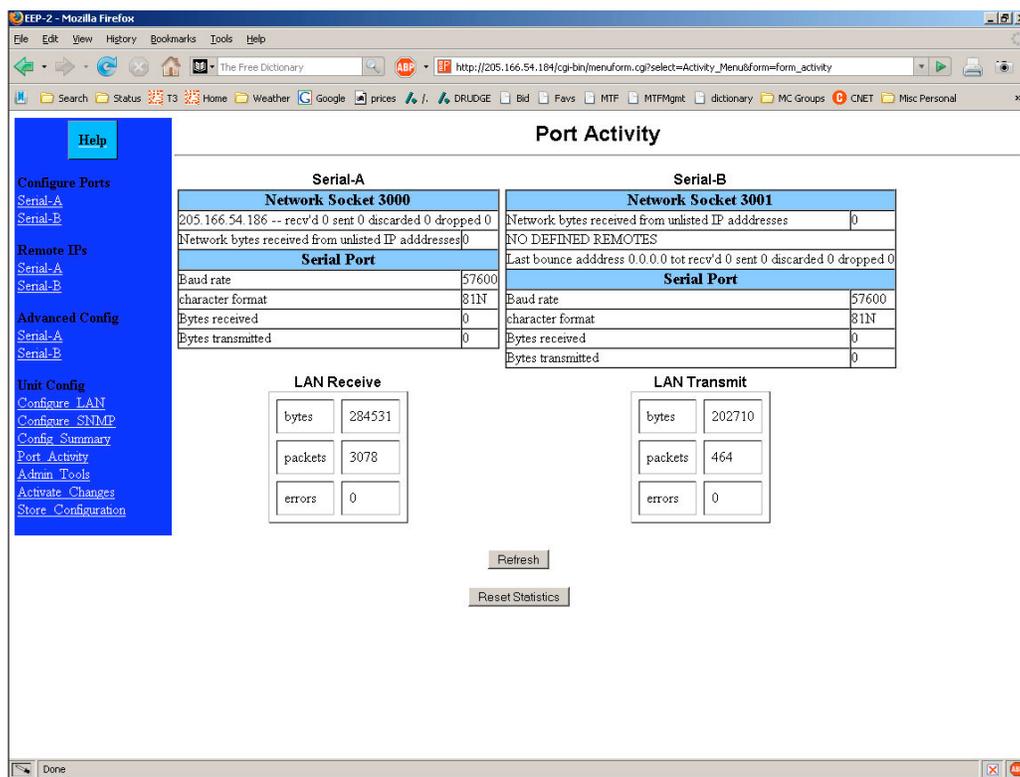


Figure 4: Port Activity Screen

This screen displays details about the data currently being transmitted or received, either through the LAN or each Serial port. The display is updated every 10 seconds.

Data - Network Per Network Port

Packets received:	Number of packets received by the Encrypted EtherPoll through the LAN connection.
Packets Transmitted	Number of packets transmitted by the Encrypted EtherPoll through the LAN connection.
Network Bytes Received from Unlisted Addresses	This is the number of bytes received from IP addresses that are not in this ports' poll list. This should be zero in a properly functioning system. These packets are discarded.
Packets with Errors	Number of packets transmitted or received by the Encrypted EtherPoll through the LAN connection which contained errors. (Should be zero)

Data - Serial Port

Bytes Received	Number of bytes received, through the serial (RS232) connection, from the Serial port device
Bytes Transmitted	Number of bytes transmitted through the serial (RS232) connection to the Serial port device (or PC, if in Client mode).

Data – Remote IP Addresses

Remote IP Address	Number of bytes transmitted to that address
-------------------	---

LAN Receive, LAN Transmit

Total LAN bytes in and out the ethernet port	Total packets received, transmitted, and in error. This includes management packets.
--	--

Serial Port Advanced Configuration Screen

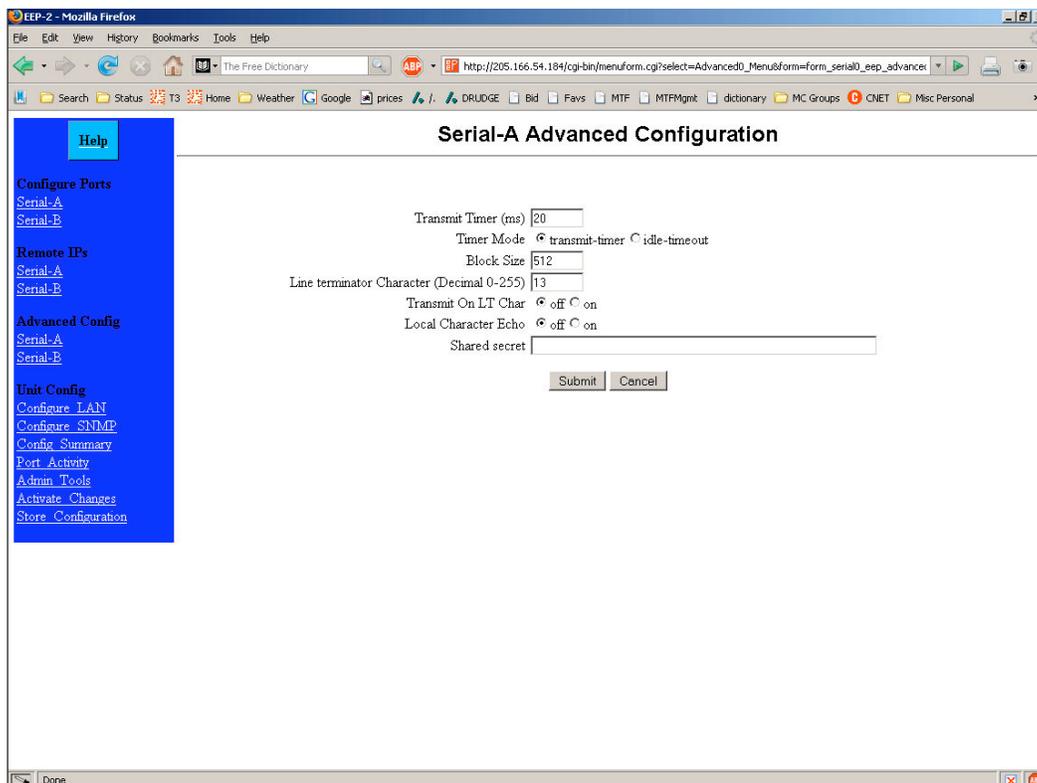


Figure 5: Advanced Configuration Screen

These settings affect the Encrypted EtherPoll's internal buffer, which is used for temporary storage of data, and how some characters are processed. These values strongly affect efficiency and throughput. They may be “tuned” for your application.

Transmit Timer (msec)	<p>When in Timer Mode, the maximum time period data will be stored in the buffer before being sent.</p> <p>When in Idle Timeout Mode, the time that the RS-232 port must be idle before data in the buffer is transmitted to the ethernet port.</p> <p>Allowable values range from 1ms to 10,000ms (10 seconds). Default is 20 ms.</p>
Timer Mode	<p>When set for Transmit Timer, a free-running clock triggers the Encrypted EtherPoll to send a packet of data at every tic if there is any data its buffer.</p> <p>When set for Idle Timeout a packet of data is transmitted to the ethernet when there is not RS-232 data received for the specified idle time and any data is in the buffer.</p>

Block Size (bytes)	The size of the ethernet packet buffer. The minimum value is 1 byte, the maximum 4096 bytes (4 K.). Note that ethernet packets are at least 64 bytes long, so extremely small values are quite inefficient.
Flow OFF buffer level (%)	If the amount of data stored in the buffer reaches this point, and the Encrypted EtherPoll is unable to transmit the data, then no further input will be accepted from the serial port. The RS-232 port will be “flowed off”. Under normal operation, this will not happen.
Flow ON buffer level (%)	Once flow control has stopped input characters, the "no-input accepted" mode will continue until the Encrypted EtherPoll has transmitted enough data to reduce the buffer contents to this point.
Line terminator character (decimal)	Enter the ASCII/ANSI number (1..128) to represent the <i>Line Terminator Character</i> . The <i>Line Terminator Character</i> causes any data in the buffer to be transmitted immediately when the character is received, provided that the following setting (Transmit on LT Char) is ON. The default value is 0x13, a carriage return character.
Transmit on LT char	When this setting is ON, any data in the buffer will be sent immediately upon receipt of a <i>Line Terminator Character</i> (see above). When this setting is OFF, the <i>Line Terminator Character</i> has no effect. This should normally be set to OFF for SCADA networks.
Transmit filter mode	This setting turns the filter function ON or OFF. If ON, when a CR/LF (Carriage Return, Line Feed) character pair is received, it is converted to a CR only. CR/LF pairs are normally used in the MS-DOS environment to mark the end of a line, but may cause problems in other environments which expect a CR only. CR/NULL character pairs are also converted to a CR only. If this setting is OFF, then no conversion is done. It is normally OFF for SCADA networks.
Local character echo	If ECHO is ON, all characters received from the serial port are echoed back out that port when connected. If ECHO is OFF, the Encrypted EtherPoll will not echo input characters. This mode should be used if any messages from the Encrypted EtherPoll would create interference with other software.
Shared Secret	When Encrypted Etherpoll units are operating with encryption, each Encrypted EtherPoll port in the network must have the same exact shared secret. This string should include numbers and letters, and be at least 32 characters long. The units default to an internal shared secret if the field is blank. This is OK for testing, but MAKE SURE YOU CHANGE THIS when the units are deployed. Otherwise, anyone who buys an Encrypted Etherpoll could decrypt your data.

LAN Configuration Screen

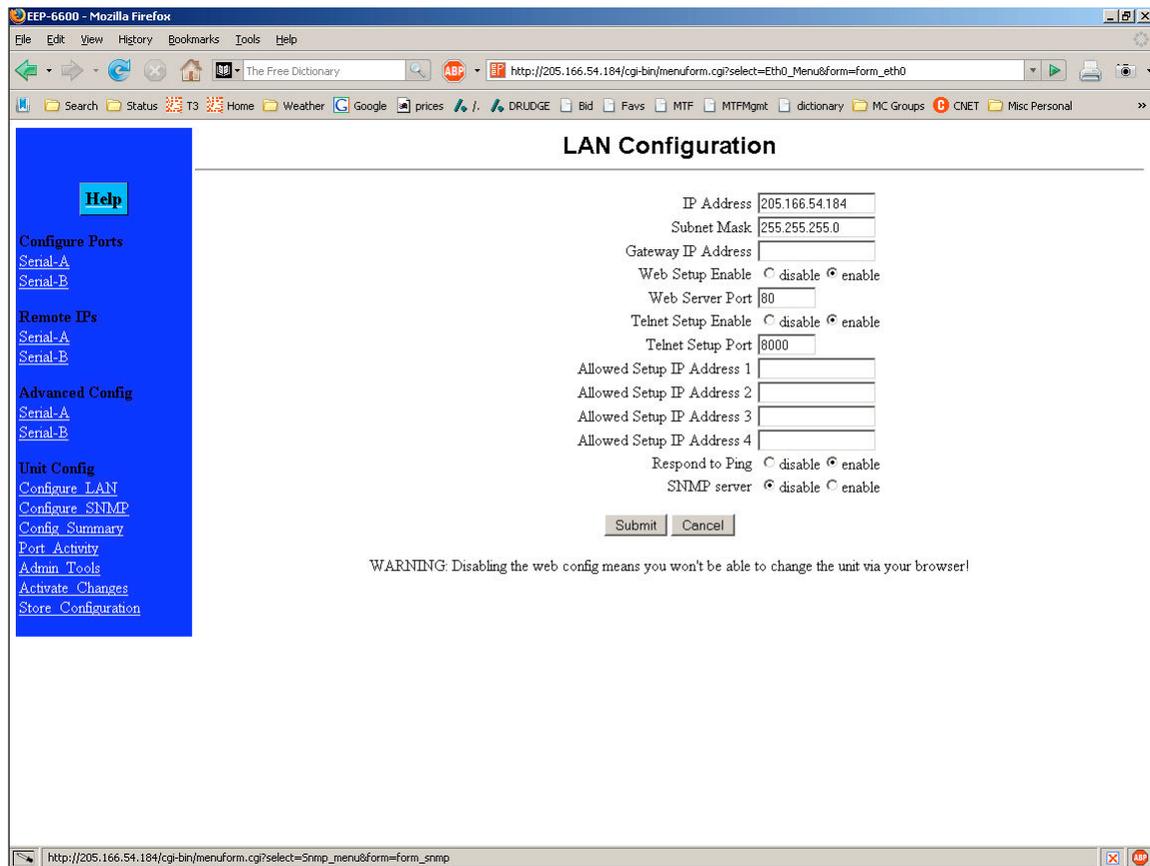


Figure 6: LAN Configuration Screen

This screen allows you to set all data relating to your LAN.

- **Encrypted EtherPoll IP Address** and network mask are required.
- **Default Gateway** Required if operating through a router.
- **Web Setup** may be disabled for security reasons.
- **Web Server Port** may be changed for security or other reasons.
- **Telnet Setup** may be disabled for security reasons.
- **Telnet Setup Server Port** may be changed for security or other reasons.
- **Administrator Access Rights** data is required if you wish to restrict access to the Encrypted EtherPoll's configuration data. If any values are entered, then only those PCs will be able to access the Encrypted EtherPoll and change the configuration.
- **Remote Device Listen Port** is the UDP port number with which this Encrypted EtherPoll will communicate.
- **Respond to Ping** packets may be disallowed based upon this configuration.
- **SNMP server** may be disabled.

Data - Encrypted EtherPoll

IP Address:	The IP address of this Encrypted EtherPoll device on your LAN in dotted decimal format. The default IP Address is 192.168.1.1 Note: If you change the IP Address, the connection will be lost when you "Save". You must reconnect using the new IP Address.
Network Mask:	The network mask indicates what class of TCP/IP network you have. The default value (255.255.255.0) is for a class "C" network, with up to 255 users. This value should work in small networks. If in doubt, consult your network administrator.
Gateway IP Address:	If your LAN contains a router, enter the IP Address of the Router. Otherwise, leave this value at 0.0.0.0

Data – Telnet Configuration

Telnet configuration enable and port	This device may be configured by a telnet connection on the given port. Some installations require higher security and disable telnet configuration.
--------------------------------------	--

Data - Administrator Access Rights

Manager IP Address [1] to [4]	Enter the IP Addresses of the PCs which you wish to have access to the Encrypted EtherPoll configuration data. If these are left blank (default) then all PCs have access.
-------------------------------	--

Data - Remote Device

Remote IP Port	This is the port with which the Encrypted EtherPoll will send and receive data. The default is 3000.
----------------	--

Data – Web Server

Web server configuration enable and port	This device may be configured by a web server on the given port. Some installations require higher security and disable web server configuration.
--	---

SNMP Configuration Screen

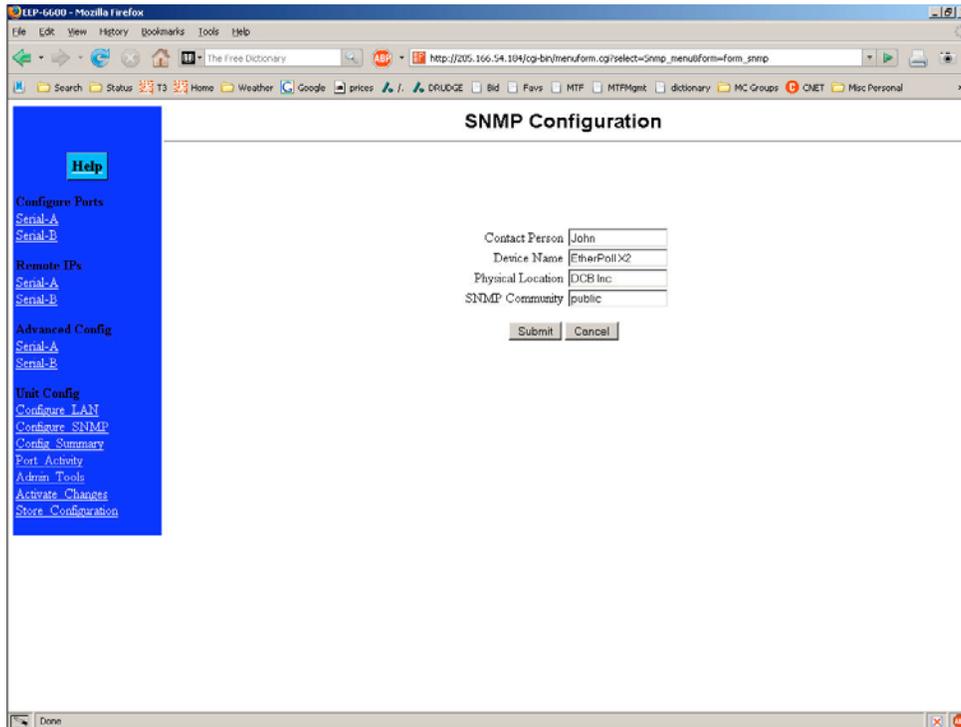


Figure 7: SNMP Configuration Screen

Overview

This screen may be ignored if SNMP is not used.

These are text fields, commonly used in SNMP (Simple Network Management Protocol) Programs to identify this device when browsing the network.

These values have no effect on the data operation of the Encrypted EtherPoll. Other standard MIB values are returned to the SNMP manager along with this information. The Encrypted EtherPoll may not be configured using SNMP.

The MIB file is available from the DCB website.

Configure Remote IP Addresses Screen

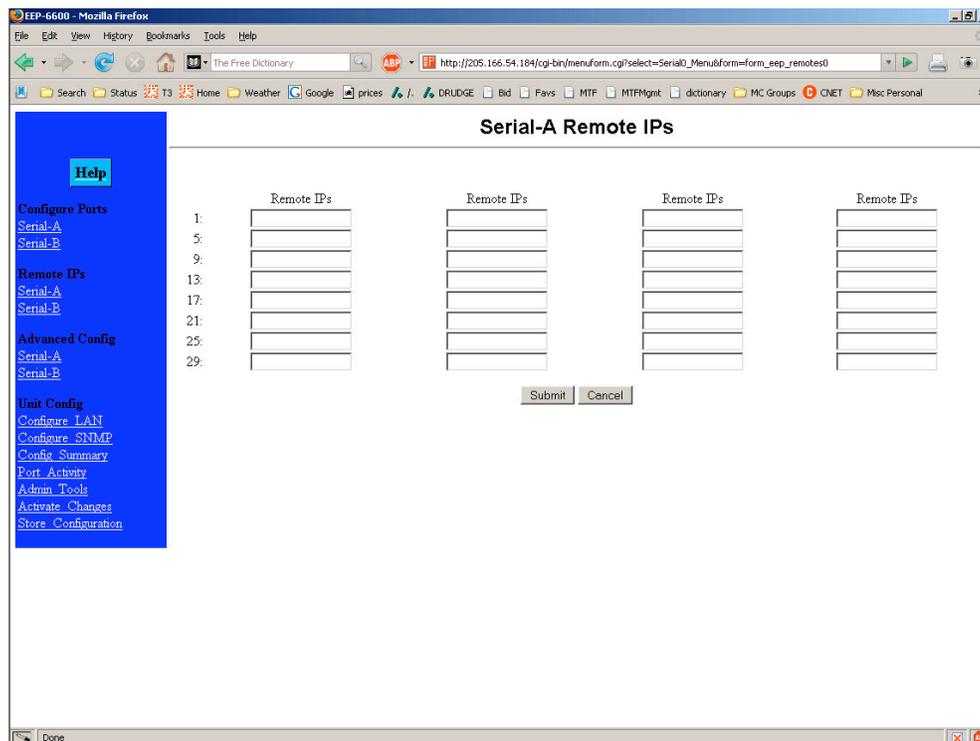


Figure 8: IP Addresses Configuration Screen

Overview

This screen is used to add or delete remote device IP addresses for each serial port.

These are the IP addresses of all devices this serial port on the Encrypted EtherPoll will communicate with.

The Encrypted EtherPoll will discard any packet received from a device that is not on this list.

Up to 32 remote device addresses are allowed.

Every packet received into the serial port will be forwarded to all IP addresses in this table.

Configuration Summary Screen

The screenshot shows the 'Config Summary' page in a Mozilla Firefox browser. The browser's address bar shows the URL: `http://205.166.54.184/cgi-bin/menuform.cgi?select=Summary_Menu&form=form_summary`. The page content is organized into several sections:

- SNMP Table:**

Contact Person	Supervisor
Device Name	GW3B00414D
Physical Location	Head Office
SNMP Community	public
- LAN Table:**

MAC address	3B00414D
IP Address	205.166.54.184
Subnet Mask	255.255.255.0
Gateway IP Address	
Web Setup Enable	enable
Web Server Port	80
Telnet Setup Enable	enable
Telnet Setup Port	8000
- Manager IPs Table:**

Allowed Setup IP Address 1
Allowed Setup IP Address 2
Allowed Setup IP Address 3
Allowed Setup IP Address 4
- Serial-A Config Table:**

Baud Rate	57600
Flow Control	none
Parity	none
Data Bits	8
Stop Bits	1
Connection Control	nailed-up
Encryption Mode	unsecured
Etherpoll UDP Port	3000
- Serial-A 1 Advanced Table:**

Transmit Timer (ms)	20
Timer Mode	transmit-timer
Block Size	512
Line terminator Character (Decimal 0-255)	13
Transmit On LT Char	off
Local Character Echo	off
Shared secret	
- Serial-A Remote IPs:** (Listed but empty table)
- Serial-B Config Table:**

Baud Rate	57600
Flow Control	none
Parity	none
Data Bits	8
Stop Bits	1
Connection Control	nailed-up
Encryption Mode	unsecured
Etherpoll UDP Port	3001
- Serial-B Advanced Table:**

Transmit Timer (ms)	20
Timer Mode	transmit-timer
Block Size	512
Line terminator Character (Decimal 0-255)	13
Transmit On LT Char	off
Local Character Echo	off
Shared secret	
- Serial-B Remote IPs:** (Listed but empty table)

The left sidebar contains a 'Help' button and several configuration categories: 'Configure Ports' (Serial-A, Serial-B), 'Remote IPs' (Serial-A, Serial-B), 'Advanced Config' (Serial-A, Serial-B), 'Unit Config' (Configure LAN, Configure SNMP, Config Summary, Port Activity, Admin Tools, Activate Changes, Store Configuration).

Figure 9: Configuration Summary Screen

Operation

- This screen displays all current settings for this Encrypted EtherPoll

Data

All values on this screen are described in earlier sections.

Administrative Tools Screen

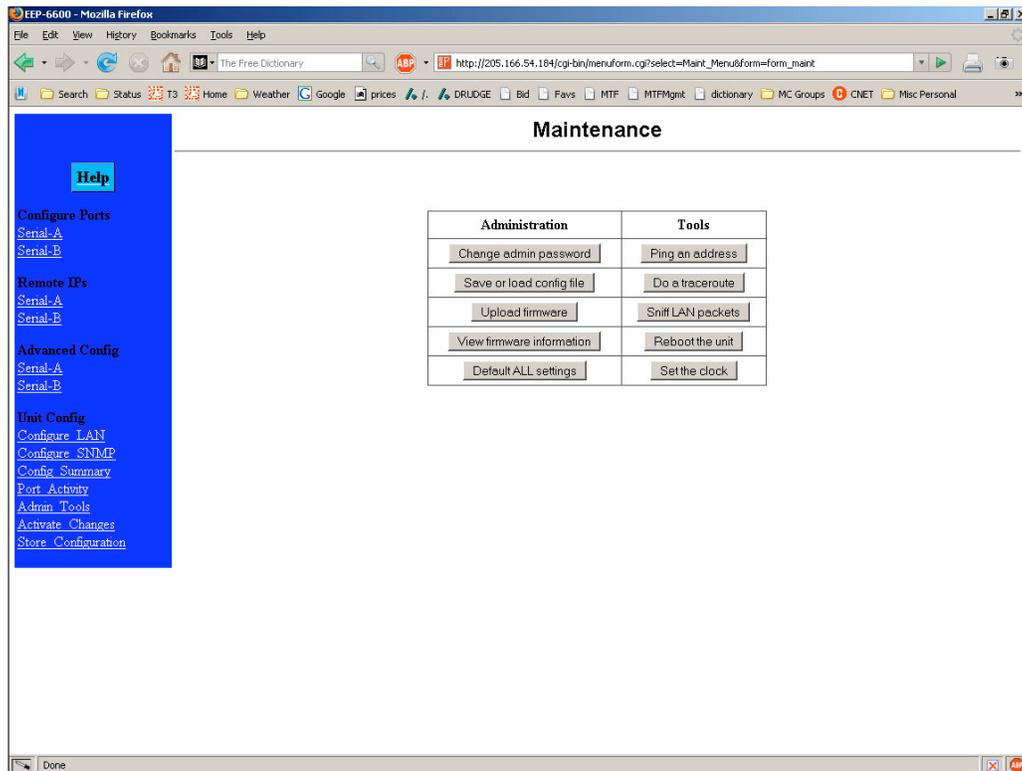


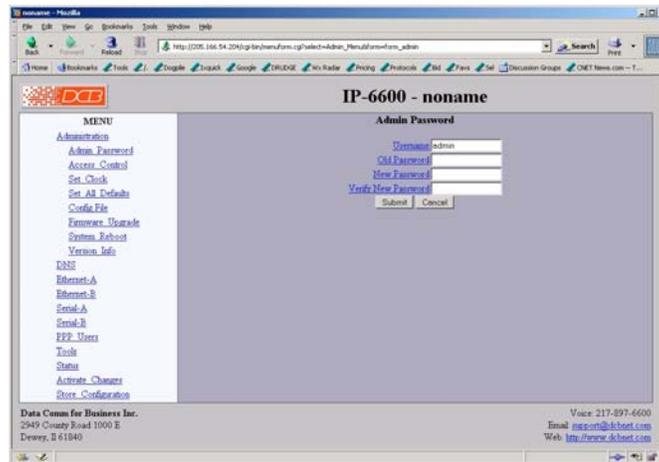
Figure 10: Administrative Tools Maintenance Screen

Overview

This screen contains command buttons for a multitude of administration and diagnostic tools. With it, you may:

- Change the administration login user name and password.
- Save or load a new configuration file.
- Upload a new firmware image.
- View firmware version and other information.
- Reset all configuration settings to factory default
- Perform a "Ping" from the EEB-2 to any other IP device.
- Perform a "Traceroute" from the EEB-2 to any other IP device.
- "Sniff" packets on the ethernet interface. Only packet header information is shown.
- Reboot the unit.
- Reset the system clock. Note that there is no hardware clock in this unit.

Admin Password



Admin Password Screen

Access to the Web Server is protected by HTTP Basic Authentication. This is a simple methodology where the Web Server will require a Web Browser to provide a username and password for each page requested. The Web Browser will typically ask the user to enter the username and password once, then will remember it for the duration that the Web Browser is running.

The Administration screen allows you to change the user name and password for the router administrator. This is the only user allowed to configure the router. If you forget the administrator name or password, the router can only be configured by returning it to factory defaults as described in the quick start chapter.

Fields

- **User Name**
This field may be a string of 0 to 15 printable characters. Do not use space or control characters. If you leave this field blank, you will need to enter a blank username during authentication.
- **Old Password**
In order to change the username and password, you must know the old password. When making a change, enter the current password in this field.
- **New Password**
When changing the username and password, this field provides the new password. It may be a string of 0 to 15 characters. If you leave this field blank, you will need to enter a blank password during authentication.

Notes

- If you forget your username or password, you can use the Serial Port Setup to erase the current settings.
- **Security Note:** HTTP Basic Authentication may be easily hacked if the attacker has the ability to sniff network packets. The username is transmitted in the clear and the password is transmitted in an obfuscated but easily reversed format.

Set Clock

Set Clock

The EEP-2 does not have a real-time clock. However a software clock is implemented and used to time-stamp log entries. The software clock will be set to the specified time at each reboot.

Year (2000-2035)	<input type="text" value="2000"/>
Month (1-12)	<input type="text" value="1"/>
Day (1-31)	<input type="text" value="1"/>
Hour (0-23)	<input type="text" value="0"/>
Minute (0-59)	<input type="text" value="0"/>

Set Clock Screen

This form allows you to set the unit's software clock. The setting will take effect when you "Activate Changes".

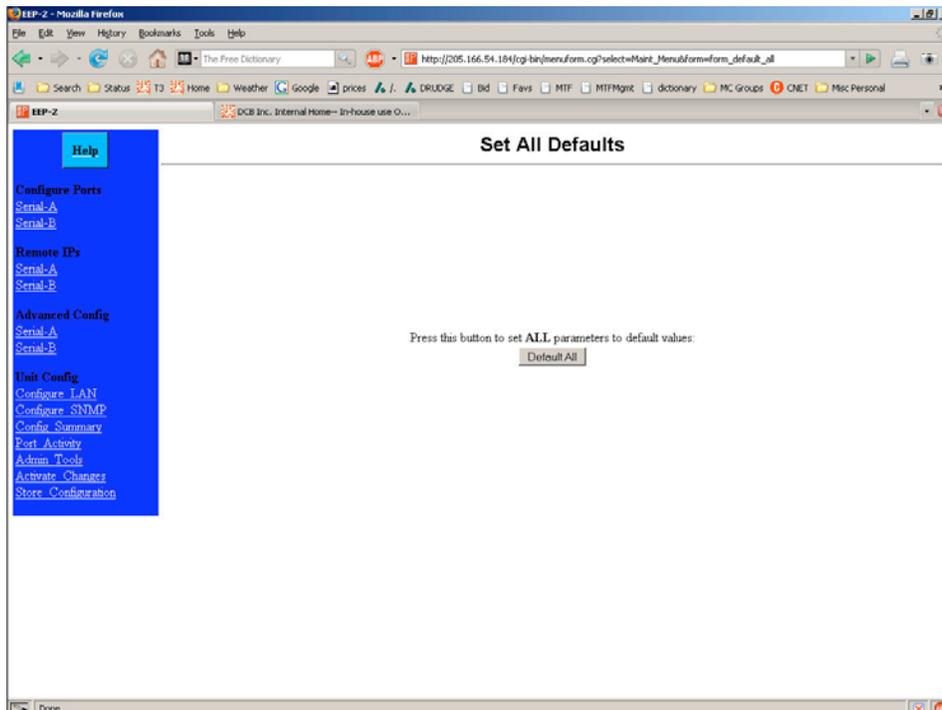
Fields

- Year Year in the range 2000 to 2035.
- Month Numeric value of month in the range 1 to 12.
- Day Day of month in the range 1 to 31.
- Hour Hour of the day in the range 0 to 23.
- Minute Minutes in the range 0 to 59.

Notes

- If you save the time to non-volatile memory, the clock will be set to the specified time at each reboot.
- The EEB-2 does not contain a real-time clock, nor has the ability to remember the current time across reboots. The software clock is used for time stamping log entries.
- The default values shown on this screen are the "boot" values... not the current time. Set the values for the time to be when the unit is next restarted.

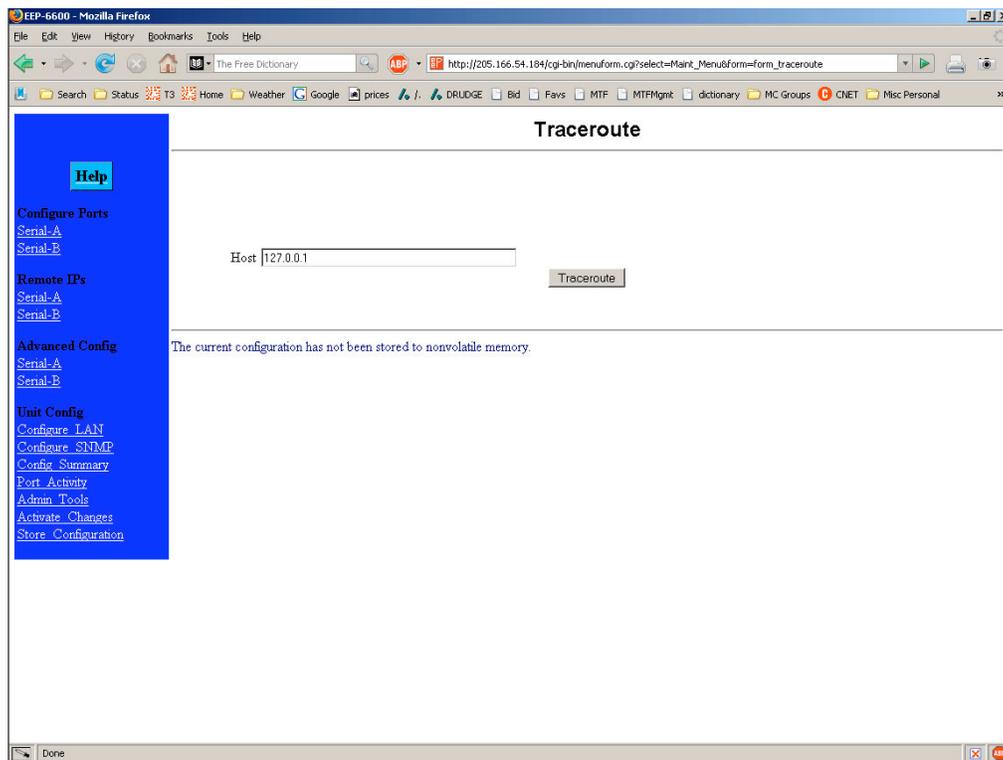
Set All Defaults



Set All Defaults Screen

This form will allow you to set all configuration parameters to their default value. Before you "Activate Changes", you should configure the interface that you are using to access the unit. Otherwise, the ethernet interface will be configured with the IP address of 192.168.0.1.

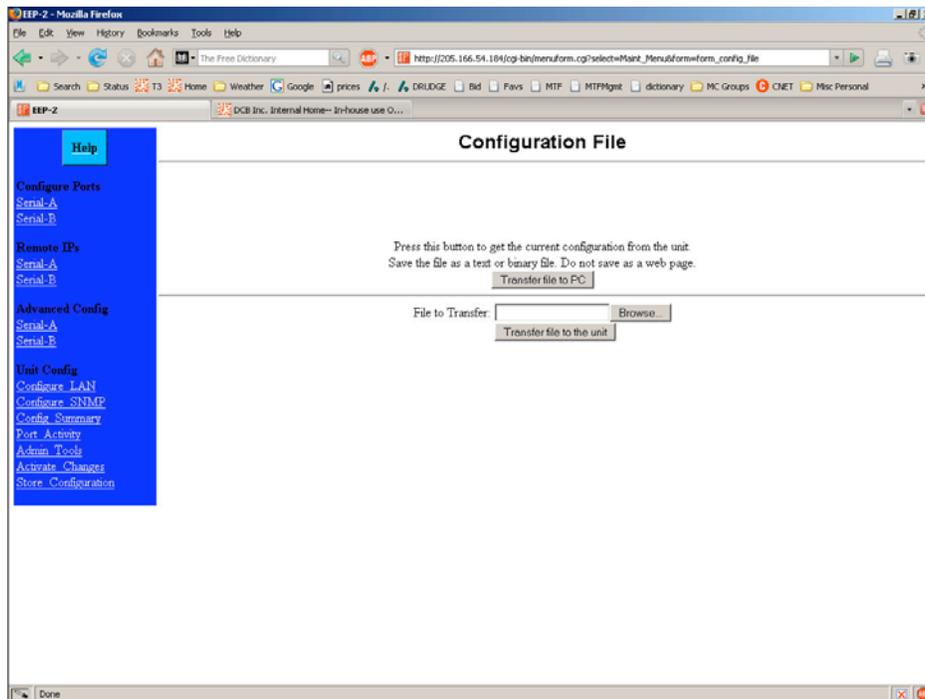
Ping, Traceroute, Sniffer Tools



Typical Tool Screen

These screens provide tools that are used to diagnose network problems. All are similar to the Traceroute screen shown above. Once the button is activated, the tool runs until completion, which would be receipt of four ping packets or a valid traceroute, or a timeout. The packet sniffer runs until 100 packets are captured or 30 seconds elapse

Transfer Configuration File



Configuration File Screen

This form will allow you to copy the unit's configuration to a file on your PC. You can also use the form to transfer a configuration file from your PC to the unit.

Fields

- File to Transfer
This is the name of the configuration file on your PC to be transferred to the unit.
- Transfer file to PC (action)
Transfers the current configuration file to this PC.
- Transfer file to the unit (action)
Transfers the named file to the router.

Notes

- The configuration file is a specially formatted text file. It may be edited with any text editor.
- You may save multiple configuration files on the PC by using different names for them.
- After transferring a configuration file to the router, you may either activate the changes (with the activate screen), or store the changes (with the store configuration screen). If you activate the changes, the router will immediately begin using the new configuration. If the changes are stored, the router will use the new configuration only after a reboot or reset.
- Be sure that you can access the router using its new configuration if you activate the new configuration. Otherwise, it may be necessary to return to the old stored configuration with a reset.

Firmware Upload

The screenshot shows a web browser window titled "EEP-6600 - Mozilla Firefox". The address bar contains the URL "http://205.166.54.184/cgi-bin/menuform.cgi?select=Main_Menu&form=form_firmware_upload". The main content area is titled "Firmware Upload". It features a "File for Upload:" label followed by a text input field and a "Browse..." button. Below the input field is an "Upload_Firmware" button. A message below the button reads: "The upload file is over 1M bytes in size. Depending on the speed of your connection, it may take several minutes to upload the file." Below this message, another line of text states: "The current configuration has not been stored to nonvolatile memory." On the left side, there is a blue sidebar with a "Help" button and several menu items: "Configure Ports" (with sub-items "Serial-A" and "Serial-B"), "Remote IPs" (with sub-items "Serial-A" and "Serial-B"), "Advanced Config" (with sub-items "Serial-A" and "Serial-B"), and "Unit Config" (with sub-items "Configure LAN", "Configure SNMP", "Config Summary", "Port Activity", "Admin Tools", "Activate Changes", and "Store Configuration").

Firmware Upgrade Screen

This form will allow you to load new firmware into the EEP-2. The firmware will be saved to non-volatile memory, replacing the current firmware.

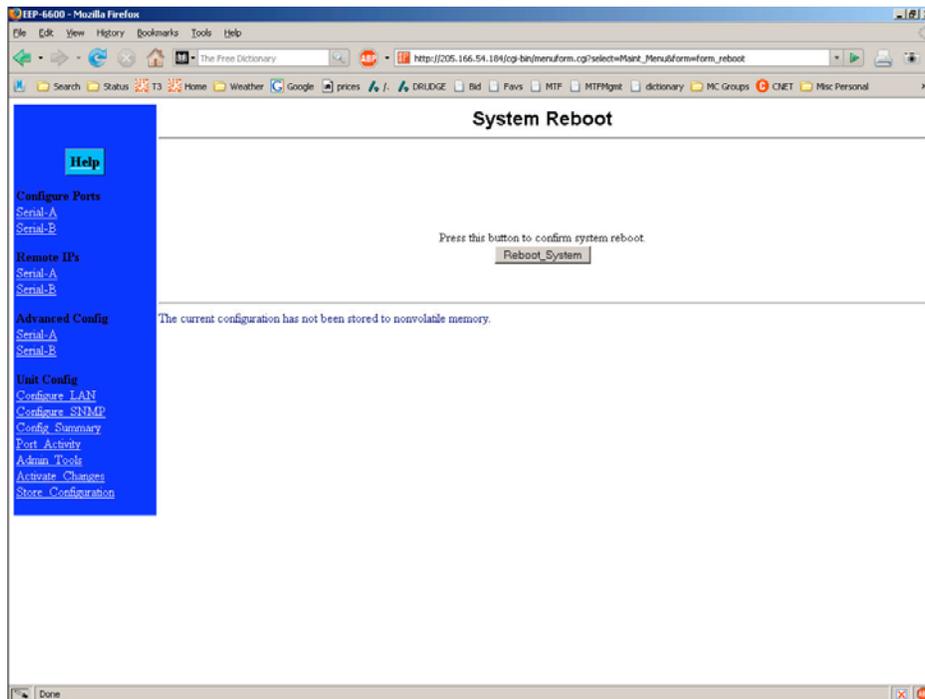
Fields

- File Name
This is the name of the firmware image file to be transferred to the unit.
- Upgrade Firmware (action)
Pressing this button transfers the firmware image to the unit and upgrades it.

Notes

You should only use a firmware image obtained from DCB.

System Reboot



System Reboot Screen

This form will allow you to reboot the unit. If you have configuration changes that have not been saved to non-volatile memory, they will be lost.

This is a way to revert back to your previously stored configuration.

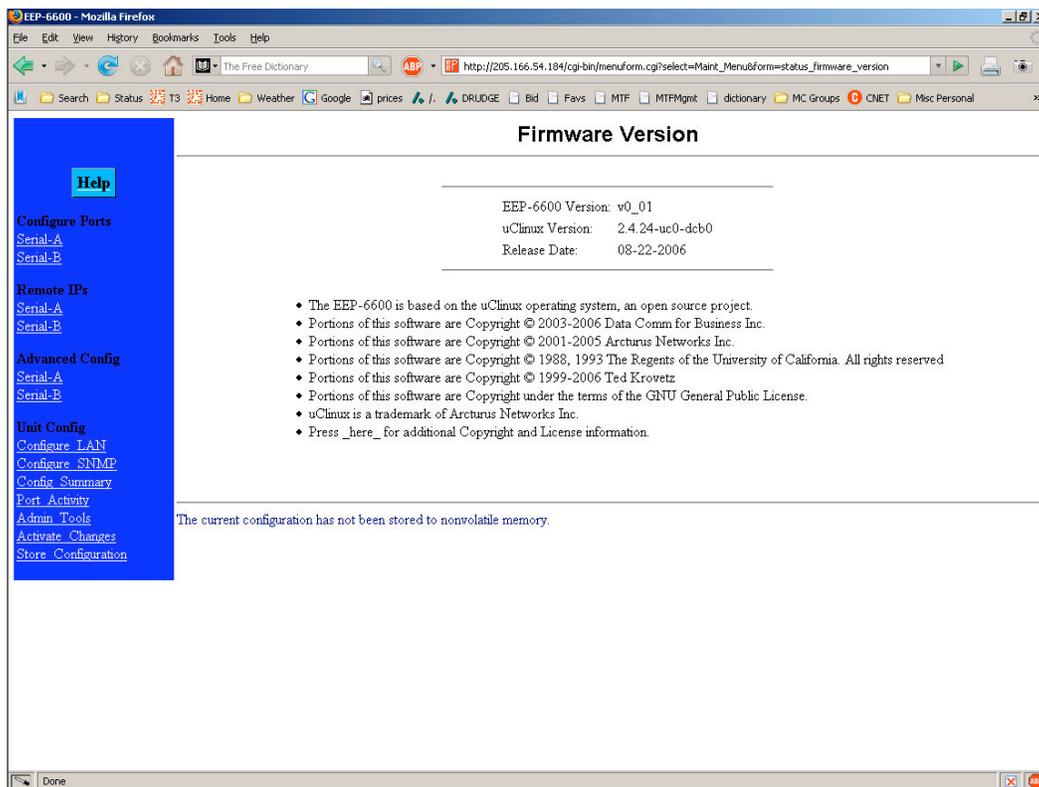
Fields

- Reboot System (action)
This causes the unit to reboot and use its stored configuration.

Notes

- The current configuration is not retained unless it has been previously stored.

Version Information Screen



The screenshot shows a web browser window titled "EE-6600 - Mozilla Firefox". The address bar displays the URL: `http://205.166.54.184/cgi-bin/menuform.cgi?select=Main_Menu&form=status_firmware_version`. The browser's toolbar includes various icons for search, status, home, weather, and other utilities. The main content area is titled "Firmware Version" and contains the following information:

EE-6600 Version: v0_01
uClinux Version: 2.4.24-uc0-dcb0
Release Date: 08-22-2006

Below this information is a list of copyright notices:

- The EE-6600 is based on the uClinux operating system, an open source project.
- Portions of this software are Copyright © 2003-2006 Data Comm for Business Inc.
- Portions of this software are Copyright © 2001-2005 Arcturus Networks Inc.
- Portions of this software are Copyright © 1988, 1993 The Regents of the University of California. All rights reserved.
- Portions of this software are Copyright © 1999-2006 Ted Krovetz.
- Portions of this software are Copyright under the terms of the GNU General Public License.
- uClinux is a trademark of Arcturus Networks Inc.
- Press `_here_` for additional Copyright and License information.

At the bottom of the screen, a message states: "The current configuration has not been stored to nonvolatile memory."

The left sidebar of the browser contains a blue menu with the following items:

- [Help](#)
- Configure Ports**
- [Serial-A](#)
- [Serial-B](#)
- Remote IPs**
- [Serial-A](#)
- [Serial-B](#)
- Advanced Config**
- [Serial-A](#)
- [Serial-B](#)
- Unit Config**
- [Configure LAN](#)
- [Configure SNMP](#)
- [Config Summary](#)
- [Port Activity](#)
- [Admin Tools](#)
- [Activate Changes](#)
- [Store Configuration](#)

Version Information Screen

This screen displays current firmware and hardware version information as well as some copyright notices.

Chapter 6

Security

This section discusses configuration options that restrict configuration as well as overall security issues.

Overview

Data Security

The Encrypted EtherPoll uses the industry standard AES encryption standard and the standard UDP/IP protocol. Since UDP/IP is a well known standard, its security vulnerabilities are also well known and may be exploited. Several Encrypted EtherPoll options are available to enhance the inherent security of your Encrypted EtherPoll network. However, since network security is a moving target and absolute security is never achievable, every network installation should be designed and implemented with care to minimize security risks in a way that is appropriate for the application and perceived risks.

The actual data transferred between the EEP-2 units may be encrypted using the AES 128 bit encryption standard by enabling the encryption option for a given serial port. Each unit shares a key that must be manually entered. The secrecy and uniqueness of this key is essential to the secure operation of the system. You should never use the default key supplied in the units (a blank key). If you wish to use an unencrypted EEP network, it is best to turn off encryption for the port being used.

Configuration Security

The Encrypted EtherPoll may be configured with several levels of security configuration and authentication. These restrict the ability of an unwanted user from changing the configuration of the Encrypted EtherPoll. They do *not* restrict the ability of a remote device to deliver packets to the Encrypted EtherPoll's data port, only using the encryption feature does that.

At the level 0, any workstation may be used to configure the Encrypted EtherPoll via either telnet or web browser configuration. Level 1 restricts configuration to workstations claiming to be from one of four IP addresses previously stored in the Encrypted EtherPoll. Either web-based or telnet configuration is allowed. Level 2 disables remote configuration using web browser, telnet, or SNMP in any combination. Level 3 requires a user name and password for remote configuration. Combinations of Level 2 and Level 3 are possible (ie. One may disable web browser configuration and SNMP and require a username/password for telnet configuration. The most secure method would be to disable all remote configuration.

The Encrypted EtherPoll may always be configured using the direct connected terminal method. This requires physical access to the hardware, and pressing the configuration button while a terminal (or PC) is connected to the serial port.

Configuration Level 0:

No specific security configuration is required. Make sure that no IP addresses have been entered in menu item 2, "Set Manager/Telnet IP Address" screen (or the "Administrator Access Rights" of the web browser "Configure LAN" screen). Also, any user name/password pairs that may have been entered on the terminal configuration/telnet "Security Configuration" screen should be cleared.

Configuration Level 1:

Using any configuration method, configure Administrator Access IP addresses. Enter the IP addresses that should have the ability to change the Encrypted EtherPoll configuration. If configuring this remotely, insure that the workstation you are using is one of the valid addresses.

Configuration Level 2:

Using telnet or direct connection configuration, selectively enable or disable remote configuration via Telnet, via web browser, and SNMP. This setting may not be performed from the web configuration screen.

Configuration Level 3:

Configure Level 1 and Level 2 security as needed. Using the telnet or direct connection configuration, enter up to three user name and password pairs. If there is at least one user name in this list, then a password prompt will be issued upon establishing a telnet configuration session.

There may be up to 3 user names and passwords configured. If no users are configured, password protection is disabled. User names and passwords are limited to 8 characters each. There is a six failed login attempt limit. After six failed attempts in a row, the unit will lock out all logins for a period of about 10 minutes.

Each user name has an associated user ID or index. The user with ID 1 is considered the master user. It has the ability to change the other user names and passwords. The other two user ID's are limited to only changing their own user name and password. All users may modify any other system parameters.

Chapter 7

Operation

This Chapter explains how to use the Encrypted EtherPoll, once it is installed and configured.

Normal Mode

- All Encrypted EtherPolls must be connected as described in Chapter 3. Configuration is complete, and serial port configurations match the associated serial port device (Polling host or RTU). LAN configuration is complete with appropriate IP addressing.
- Power up all Encrypted EtherPolls and associated hardware.
- Start the polling program on the polling host computer. It should automatically poll each RTU connected to an Encrypted EtherPoll whose IP address was stored during configuration of the host Encrypted EtherPoll.
- The serial DCD input must be HIGH or Forced ON for the unit to send and receive packets.
- If using encryption, all units with encrypted ports must have the same secret key entered.

Broadcast Mode

- Install and connect the Encrypted EtherPolls and Serial Port Devices as described above.
- Send some characters from a PC or terminal device connected to the host Encrypted EtherPoll to its RS-232 port.
- The characters should appear on the RS-232 port of all Encrypted EtherPolls whose addresses are configured in the host Encrypted EtherPoll IP address list.
- DCD must be HIGH or Forced ON for the unit to send and receive packets.

Point-to-Point Mode

- This is similar to the above operations, however only ONE remote IP address is configured into each Encrypted EtherPoll.
- DCD must be HIGH or Forced ON for the unit to send and receive packets.

RTS Toggle Feature

- This feature is sometimes used to key the push-to-talk line on radio transmitters and specialty modems.
- One of the above normal modes is used.
- DCD must be HIGH or Forced ON for the unit to send and receive packets.
- When a frame of data is in the serial output buffer, the RTS signal is asserted prior to transmitting the data. Approximately 5 msec. after the data is sent, RTS will again be lowered.

Chapter 8

Troubleshooting

This chapter outlines some problems that may occur during installation or operation and some possible solutions to them.

If you follow the suggested troubleshooting steps and the Encrypted EtherPoll still does not function properly, please contact your dealer for further advice.

Hardware Problems

Before anything else, check that all cables are wired correctly and properly connected. If connecting to a 9 pin PC port, a crossover (null modem) cable is required.

P: All the Encrypted EtherPoll's LEDs are off.

S: Check the power supply or power connection.

P: When using 10/100Base-T cabling, the Encrypted EtherPoll unit does not work.

S: Check the Hub's link LED for the port to which Encrypted EtherPoll is connected. If it is off, make sure the network cable between the Encrypted EtherPoll and hub is in good condition.

Can't Connect via the LAN

P: Can't connect to the Encrypted EtherPoll using Telnet or Web Browser.

S: Check the following:

- Start troubleshooting from a known state. Power the Encrypted EtherPoll OFF and ON to reboot.
- “Ping” the Encrypted EtherPoll to see if it responds. From the Windows command prompt or “Run” dialog box, use the command:

```
ping IP_Address
```

Where `IP_Address` is the IP Address of the Encrypted EtherPoll (e.g. `ping 192.168.1.1`). If it does not respond, then check all LAN connections. If the LAN connection are OK, the problem is in the LAN addresses or routing. You should be able to ping all Encrypted EtherPolls.

The most common problem cause is incorrect IP addressing. Make sure the workstation and Encrypted EtherPolls have compatible IP addresses.

- If using a LAN without routers, you can connect to the Encrypted EtherPoll ONLY IF your PC and the Encrypted EtherPoll are using IP Addresses from the same address block. The Encrypted EtherPolls default IP Address (192.168.1.1) requires that your PC is using an address from the address block 192.168.1.2 to 192.168.1.254, and a *Network Mask* of 255.255.255.0. If a router is between the devices, a gateway address must be configured in both devices.

Check your PC's IP Address using *Control Panel - Network - TCP/IP (Adapter) Properties* or *Windows98 WINIPCFG.EXE*. If you are using a different Address block, use *Terminal Mode* configuration to set a compatible IP Address in the Encrypted EtherPoll.

- It may be that your "arp table" contains invalid entries. You can clear the "arp table" by rebooting, or, on Windows95, by typing the following command at the command prompt or *Run* dialog box.: `arp -d`
- Check that you have used the correct port address on all units. The default port addresses are “3000” and “3001”
- MOST Encrypted EtherPoll connection problems are due to incorrect RS-232 wiring. The second most common errors are incorrect IP addressing on either the Encrypted EtherPoll or on the PC used for testing.
- In some cases, “smart” hubs and switches must be power-cycled to clear their internal arp cache. This is often a problem on test bench setups where IP addresses are moved between different equipment or a unit is moved between ethernet switch receptacles.

Other Problems

P: Can't run the configuration program using a serial cable connection.

S: Check that:

- The communication parameters are set properly.
- Disconnect and reconnect the power supply to the Encrypted EtherPoll.
- Power is available... a LED is on.
- The terminal program is operating properly. Try a loopback connector at the Encrypted EtherPoll end of the cable to verify program operation and the proper COM: port.
- The most common problems causing this symptom are incorrect RS-232 wiring or the Windows Hyperterm program not operating correctly. First, restart Hyperterm.

P: The "host" Encrypted EtherPoll doesn't automatically send data to the "RTU" Encrypted EtherPolls.

S: Check that:

- A workstation on the host Encrypted EtherPoll LAN can successfully ping all remotes.
- If a firewall is between the Encrypted EtherPolls it must pass the ports in use for UDP.
- The Encrypted EtherPolls should either be configured for "Pin 6 Control" forced ON or the interface must be wired in such a way that that pin 6 is asserted.
- The "RTU's" IP addresses were correctly entered into the "HOST's" Encrypted EtherPoll IP Address list.
- The Gateway IP Address is set correctly.
- The Subnet Mask is set correctly.
- All encrypted units have the same shared key.
- The communication parameters between the host computer and the local ("host") Encrypted EtherPoll match.
- The communication parameters between the serial port RTU device and the remote ("RTU") Encrypted EtherPoll match.

P: Throughput is extremely low. There seems to be a long delay when transmitting data.

- S:** The first time an Encrypted EtherPoll sends data to a remote device, it must ARP that device's IP address. If that device does not exist on the network, the ARP command is repeated, and allowed to timeout. If non-existent devices are configured in the Encrypted EtherPoll's remote address table, then the addresses are ARP'd (and allowed to timeout) every time there is data to send. This problem does not occur after a device has been located at least once, as the Encrypted EtherPoll's internal ARP table never times out... It's only a problem for non-existent devices after a power cycle.
- Do not configure IP addresses in the remote device table for devices that do not exist.

P: The Encrypted EtherPoll's IP Address is unknown. Is there any way of finding it, other than using *Terminal Configuration* mode?

- **S:** No, it must be restarted in terminal configuration mode with a terminal connected. The existing IP address will be displayed in the startup sequence.

Checking Device Operation

Once the Encrypted EtherPoll is installed on your Network, you can connect to it using Telnet, to verify its operation. The procedure is as follows.

1. Use telnet to connect to the Encrypted EtherPoll with the command:
telnet IP_Address 8000

2. Where IP_Address is the IP Address assigned to the Encrypted EtherPoll, and 8000 represents the Port number.

The port number is “8000” for configuration, but “3000” is the default for normal operation. The actual data connections to the Encrypted EtherPoll on port 3000 are not TCP/IP as used with telnet programs, but are UDP/IP, so you can not telnet to the Encrypted EtherPoll to send test data through it.

If the “Manager IP Addresses” have been entered in the Encrypted EtherPoll, then only a PC having one of those addresses can change the configuration.

3. Choose item 5 (“Display Settings”) from the Main Menu, and examine the data shown. See page 16 for an explanation of each of the data items.

Appendix A

Specifications

Encrypted EtherPoll Specifications

- Flash Memory: 4 Mbytes
- SRAM: 8 Mbytes
- LAN Interface: 10/100BaseTx, Autosense
- RS-232: Two male DE-9 connectors (PC –9 Pin)
- RS-232 speed: Up to 230.4.2 Kbps
- CPU: Motorola Coldfire 5272 CPU 66 Mhz
- OS: uClinux
- Power: 9 to 12 VDC 600mA or Optional power supplies
- Switch: Configuration, Reset
- LED:8 (Status, Serial Activity, LAN Activity, Power)
- Default IP address: 192.168.1.1
- Browser Management port: 80
- Telnet Management port: 8000
- Default Receive ports: 3000, 3001
- Operational Temperature -40C to +70C

RS-232 PIN Assignments

The RS-232 port wiring is identical to a standard PC 9 pin DE-9P COM: port. It operates as a DTE device. The chart below details signal directions and names.

Serial Port Pin Assignments		
Pin	Signal Name	Type
1	Carrier Detect (DCD)	In
2	Receive (Rx)	In
3	Transmit (Tx)	Out
4	Data Terminal Ready	Out
5	Signal Ground (GND)	Power
6	Data Set Ready (DSR)(Not used)	In
7	Request to Send (RTS)	Out
8	Clear to Send (CTS)	In
9	Ring Indicator (RI) (Not used)	In

Control Signal Operation

DCD

Input DCD Must be asserted before the EEP-2 will transmit packets.

Receive Data

Input, data into the port

Transmit Data

Output, Data from the port. The unit only transmits when it has characters to send and it is not flowed-off with RTS/CTS flow control.

Signal Ground

Common ground

DSR

Input. Ignored

RTS

Output. Input flow control. When the internal buffer reaches the "Flow Off" buffer level, this signal is lowered. When the buffer level decreases to the "Flow ON" buffer level, this signal is raised

CTS

Input. When Flow Control is set for CTS/RTS, lowering this signal will halt data flow from the RS-232 port.

Ring Indicator

Not used

CABLES

Commonly used cable connections:

To PC 9-pin COM: port

Port	PC
1,6	4
2	3
3	2
4	1,6
5	5
7	8
8	7

This null-modem crossover cable is easily made by combining “PC-Direct” and “Remote PC” adapter hoods with a straight-through line cord.

Encrypted EtherPoll to Modem

Use any commercially available PC-to-modem cable.

Ethernet Cross-Over Cable

Used to connect two Encrypted EtherPoll ethernet connections “back-to-back” without using an ethernet hub for test purposes. Also used to connect a Encrypted EtherPoll directly to a PC’s LAN connection for testing.

RJ-45	RJ-45
1 — WHT / ORG	3
2 — ORG / WHT	6
3 — WHT / GRN	1
4 — BLU / WHT	N/C
5 — WHT / BLU	N/C
6 — GRN / WHT	2
7 — WHT / BRN	N/C
8 — BRN / WHT	N/C

Appendix B

Advanced Operation

This Appendix explains the Encrypted EtherPoll's operation in more detail. This information is not needed in most applications.

Introduction

The Encrypted EtherPoll must be configured with proper ethernet addressing and serial port parameters. It has been used successfully with common SCADA protocols such as Modbus ASCII, Modbus RTU, DNP3, and other 8-bit asynchronous protocols. This section explains how the Encrypted EtherPoll operates for the technician who needs to understand the internals in more detail.

Description and Behavior

Ports used by the Encrypted EtherPoll

The Encrypted EtherPoll uses 3 ports, as follows:

Port	Description
Configurable default - 3000 & 3001	Encrypted EtherPoll listens at ports 3000 and 3001 and offers a raw UDP connection. This port number is configurable.
8000	Provides a telnet configuration service for all modes.

Normal Operation Modes

In Normal Mode, the Encrypted EtherPoll runs under the UDP/IP network protocol. It will listen on a configured port number. The server will wait for incoming data after initialization.

The Encrypted EtherPoll constantly checks for data on both Ethernet and Serial Ports.

If data from the Ethernet network is received, it will first check for a special control symbol, and then send the data to the serial port.

If data from the serial port is received, it will read the data from the serial buffer, move the data into the network buffer and send it by ethernet when the buffer is full, when it senses an idle timeout, or on the next tick of the transmit timer.

The data being sent via ethernet is packaged into UDP packets and a separate copy is sent to each IP address in the Encrypted EtherPoll's IP address list.

Each configured port number is associated ONLY with a single serial port.

Point - to - Point Mode

Encrypted EtherPolls configured for Point-to-Point mode function the same. The only difference between the "normal" operation and point-to-point is the number of IP addresses in the IP address list. For point-to-point operation, there is only one address in the list (the other unit's).

Broadcast Mode

Broadcast mode is also identical to “normal” mode. There is simply no polling taking place over the network.

Transmit Conditions

The Encrypted EtherPoll will transmit an ethernet packet of data whenever one of the following conditions is met...

- Timer is up. In Timer Mode, a free running clock triggers a transmission when it ticks if there is data in the buffer.
- Idle time is up. In Idle Timeout mode, a (configured) time period elapses with no incoming data if there is data in the buffer.
- Transmit Buffer full.

SCADA Protocols

The Encrypted EtherPoll is protocol-transparent. It has been successfully used with many 8-bit asynchronous protocols. However, some protocols work best with specific settings. If in doubt, call Tech Support for additional information on your application.

Appendix C

Open Source Software Information

This product was designed in conjunction with Open Source Linux software..

Introduction

This product was designed and programmed with Open Source Linux software in mind. The core Linux operating system is uClinux, available from <http://www.uclinux.org>. DCB supports the Open Source software effort and is appreciative of the contribution many open source developers have made to the community.

Other open source software used in this product may be obtained from the original developers, and is made available in accordance with GNU licensing terms.

Obtaining the Source Code

For more information on obtaining the source modules for open source code used in this product, send a written request to the following address. Code is provided on CDROM. According to GNU licensing terms, a duplication fee may be charged.

Open Source Software Administrator
Data Comm for Business, Inc.
2949 CR 1000 E
Dewey, IL. 61840