ET-Series

Encrypted Ethernet Tunnel

Product Family

User's Guide

Revised January 22, 2014

Firmware Version 2.24

FCC Statement

This device complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

Version 2.0x

RoHS

Some models of this product is available in RoHS versions.

Models ET-6601, ET-6604, ET-3302, ET-6620 are available in RoHS versions.

Models ET-6600, ET-3300, ET-6690, and other models not listed are available in non-RoHS versions. For the latest information on RoHS versions of those models, please contact Data Comm for Business.

TABLE OF CONTENTS

Chapter 1
Introduction

This chapter provides an overview of the EtherSeries Encrypted Ethernet Tunnel Bridge's features and capabilities.

Congratulations on the purchase of your new EtherSeries Encrypted Ethernet Bridge. This is a simple, easily configured tunneling device containing (depending upon individual model) various 10/100/1000BaseT Ethernet interfaces, 10BaseT Ethernet interfaces, Gigabit Ethernet interfaces, a dial-up modem, synchronous or asynchronous RS-232 serial interfaces. Some models contain other interfaces or firmware options.

Two or more bridges connect using standard TCP/IP using any insecure IP connection path, ethernet or serial PPP via any asynchronous WAN media such as digital radios, DSUs, satellite, modems, DSL, orcable modems. They tunnel all Ethernet packets from the secure interface of each device to the other devices.

The bridge transports all valid Ethernet protocols. It provides a virtual private network by bridging the two LANs with an IP tunnel that may be encrypted using the AES ISAAC algorithm. Depending upon the model, AES is available in 128, 192, or 256 bit versions. Filtering is available based upon IP or MAC addresses and Protocol types. 802.1Q VLAN tagging is supported.

When used in its simplest mode, two bridges might "extend" a secure LAN segment to another physical location via an insecure path. They may be used behind firewalls and NAT routers.

EtherSeries ET-Family Applications

The ET-Family connects multiple LAN segments by using standard IP protocols between the bridges. It is commonly used to connect a remote LAN to a central LAN when using an asynchronous PPP link between the two segments. In this application, the bridges connect via PPP, negotiate an encrypted link, and then bridge all traffic between the two LANs. Or, is used to connect two LAN locations via a broadband or IP WAN link.

The encrypted ethernet bridge is also used to connect a single location to multiple remote sites. In this application, remote sites may be "daisy-chained" to allow multiple locations to communicate via insecure links.

In Dial-out mode, it may be configured for always-up connections, dial-upon demand, or dial-upon command modes. It may also be configured to auto-answer an incoming PPP call.

In an installation using a serial port connection, the bridge may be configured to auto-dial upon demand. In this mode, it will dial a remote bridge through a connected modem whenever it senses that a packet needs to be sent off the local LAN segment. It may be configured to dial upon power-up, and disconnect upon inactivity timers.

An auto-answer modem may be used to allow dial-in on a remote LAN segment. Dial-in and Dial-on-demand may be used on the same bridge port.

When using the broadband (Ethernet) connection, the unit may be configured to obtain an external IP address via DHCP. If configured in this manner, it may be used in a "plug-and-play" mode for mobile applications. Simply plug it into an ethernet port at any location offering a dynamic DHCP IP address, and it will self-configure and connect to the bridge at the home location… providing a virtual private network between the two locations.

Other Features

Multi-port Version

The ET-Family products are available with various interfaces such as synchronous ports, asynchronous ports, and multiple LAN ports. LAN ports are available in 10BaseT, 10/100BaseT, and higher speed versions support Gigabit ethernet ports.

Serial Ports

Asynchronous serial port speeds may be any asynchronous speed between 300 bps and 230.4 Kbps. Synchronous ports support speeds up to 1.54 Mbps.

Protocols

The bridge uses the IP protocol to connect to its remote peer. It does pass IP, IPX, AppleTalk, and other non-routable protocols through the encrypted IP tunnel.

DHCP Protocol

The bridge supports the DHCP protocol as a client or server. DHCP may be served through the tunnelled link. In server mode, Dynamic DNS services are available.

Extensive Filtering

The bridge supports filtering based upon IP addresses, MAC addresses, or Protocol type. Filtering may be configured as "shall pass" or "shall deny".

802.1q VLAN

The bridge passes 802.1Q VLAN tagged packets. Each trusted port of the ET-3302 may be configured as a separate VLAN port.

Upgradeable Firmware

Firmware upgrades may be installed using any web browser.

Security and Firewall Features

The bridge supports a number of security features. On the "insecure" side, all traffic is encrypted, including the ET to ET negotiation. TThe encryption methodology is industry-standard AES. Only workstations on the "secure" side of a unit may be used to configure or control it. A user-defined banner may be presented, and administration session time-out is available. Administration password complexity rules and password aging is available. Individual ethernet ports may be disabled for additional security.

On-board Tools

The bridge contains diagnostic tools such as extensive logging, traceroute, ping, and a simple packet sniffer to aid in network troubleshooting.

Radius Authentication Available

The ET-Family bridge uses either Radius back-end authentication or an internal database

Optional Internal Modem

The ET-Family bridge may contain an internal V.92 modem in the place of the second serial port.

Simple Web Proxy

A simple web proxy is included. This operation allows web traffic from the trusted interface to be passed to the un-trusted interface, while all other traffic is tunneled to the other bridge. This is ideal for traveling people to use in hotels that support broadband connections.

Single-Interface operation

The ET-Family bridge may be configured in an "single-headed" mode. See details in the manual.

Package Contents

You should find the following items packaged with your EtherSeries Bridge:

- The ET Bridge
- Power Adapter
- This User's Guide CDROM
- Short cable with RJ-45 connectors (Units with serial ports only)
- 9-pin PC-direct adapter (Units with serial ports only)
- 9-pin Remote-PC adapter (Units with serial ports only)
- 25-pin modem adapter (Units with serial ports only)

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

Software Requirements

The bridge supports IP and associated protocols such as UDP, ICMP, serial PPP, DHCP, multi-cast, and any protocol built upon IP or TCP/IP**. It also bridges any valid Ethernet protocol**. The initial IP address may be entered using any terminal or terminal emulation software on a PC.

Any standard web browser may be used for configuration once the bridge is configured with a valid IP address. Some ET products (including the ET-6604 and ET-6620) require the use of a secure web browser connection for initial configuration (HTTPS://). These may be re-configured to use the standard port 80 (HTTP://) web browser if desired.

The ET-Family of bridges will link only with other ET-Family bridges, however it will connect to the other bridge through any valid link, such as standard serial PPP, or Ethernet IP.

ET-6600 Specific 2-Serial Ports, 2-Ethernet Ports

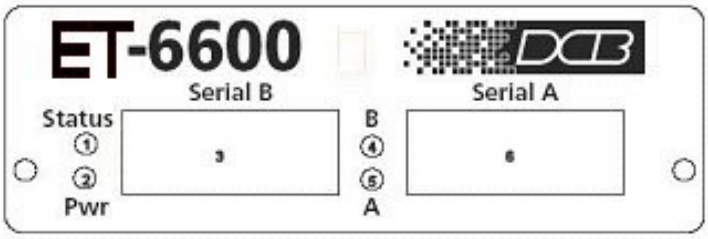
Introduction

The ET-6690 model bridge contains two serial ports and two ethernet ports (one 10BaseT, one 10/100BaseT). It supports up to 8 simultaneous remote ET units.

Front Panel

The ET-6600 model front panel is shown below.

Some units do not contain all ports shown, some units contain an internal modem in the place of Serial B.



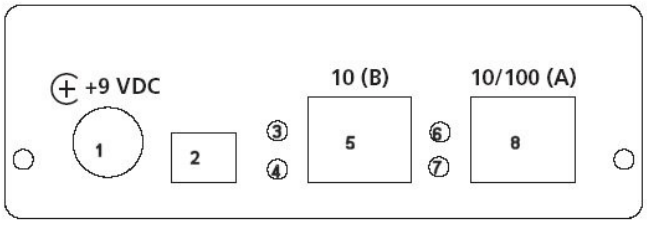
ET-6600 Bridge Front Panel

1	**Red LED**	Status Indicator
2	**Red LED**	Power Indicator
3	**DE-9P**	Serial Port B
4	**Red LED**	Port B Activity
5	**Red LED**	Port A Activity
6	**DE-9P**	Serial Port A

Front Panel LED Indicators

Rear Panel

The ET-6600 rear panel is shown below. Some units do not contain all ports shown.



EtherSeries Bridge Rear Panel

1	**Power port**	Connect the power adapter here.
2	**Switch Bank**	Configuration Switches
3	**Red LED**	LAN B Activity Indicator
4	**Red LED**	LAN B Link Indicator.
5	**Ethernet Port B**	10BaseT Ethernet Port
6	**Red LED**	LAN A Activity Indicator
7	**Red LED**	LAN A Link Indicator.
8	**Ethernet Port A**	10/100BaseT Ethernet Port

Rear Panel Indicators

ET-6600 Configuration Switches

The rear panel contains four small switches, numbered one 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 bridge just as if it had been power cycled.

Switch 2

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

Switch 3 & 4

Factory use only.

LED Indicators

There are two red LED indicators on the rear panel adjacent to each 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.

ET-6690 Specific -Internal Modem

The ET-6600 family consists of various models with different internal hardware or firmware options. The ET-6690 includes an internal V.92 modem.

Introduction

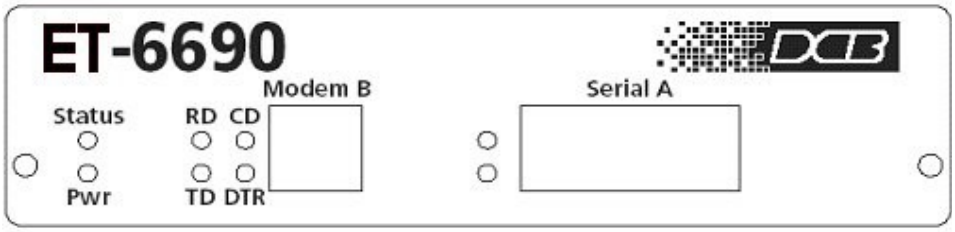
The ET-6690 model bridge contains an internal V.92 modem and one serial port along with two Ethernet ports (one 10BaseT, one 10/100BaseT). The configuration is similar to the ET-6600 model with the following changes. It supports up to 8 simultaneous remote ET units.

Configuration Differences

The internal modem conforms to V.92 specifications. Serial B Operating Modes are either PPP or Disabled. Modem configuration string options may be changed to suit your environment, however the default value of "Internal Modem" is recommended.

ET-6690 Front Panel

The front panel contains modem indicator LEDs for RD, CD, TD, and DTR along with an RJ-11 telephone line jack. Any standard RJ-11 telephone cable may be used for the phone line connection.



EtherSeries Bridge Front Panel

Label	Name	Operation
RD	Receive Data	Flickers along with data received from the telephone line
TD	Transmit Data	Flickers along with data transmitted to the telephone line
CD	Carrier Detect	Indicates carrier is received from another modem
DTR	Data Terminal Ready	Indicates the bridge has raised the internal DTR signal

LED Indicators

ET-3300 Specific – Two Ethernet Ports

The ET family consists of various models with different internal hardware or firmware options. The ET-3300 includes two Ethernet ports. ***The ET-3300 model is discontinued.***

Introduction

The ET-3300 model bridge contains two Ethernet ports and is designed for operation with a broadband or direct Ethernet WAN connection using a public network, DSL modem, or Cable modem. It supports up to 8 simultaneous remote ET units. The configuration is similar to the ET-6600 model with the following changes.

Configuration Differences

This model contains a single serial interface to be used in initial setup (if needed). IF the default IP address is not appropriate for your LAN, then press the hidden button to the right of the LEDs **and hold it depressed while powering up the unit.** If the unit is running, the setup button can be pressed at any time to enable serial setup. The button must be held down for approximately 1 second to be detected. Follow the command line setup instructions. Once a compatible IP address is available, the browser setup screens are much easier to use.

ET-3300 Bridge

ET-3300 showing Panel Layouts

ET-3300 Rear Panel LED Indicators

One set of indicators For Each Ethernet Port

- 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).

ET-3300 Front Panel LED Indicators

- Lower LED is a power indicator.
- Upper LED is a status indicator. It should be on.

ET-3300 Front Panel Switch

Press for setup mode. This switch is "hidden" inside the case. Use a small tool to press it (a straightened paper clip works well).

ET-3300 Front Panel Connector

The DE-9 (PC 9-pin) connector is used for command line setup. A cross-over cable is required to use this with any standard PC serial port. Terminal configuration is 9600 bps, 8N1 .

ET-3302 Specific – Multiple Ethernet Ports

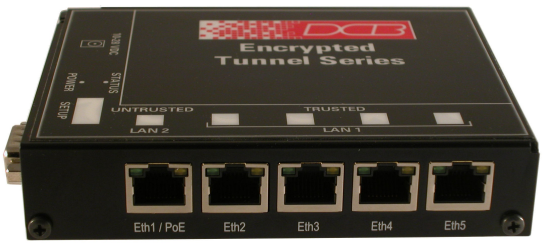
The ET family consists of various models with different internal hardware or firmware options. The ET-3302 includes one untrusted Ethernet ports and a trusted side terminated in a four port switch. The serial port on the ET-3302 may be used for setup, or as a TCP or UDP server port.

Introduction

The ET-3302 model bridge contains six Ethernet ports and is designed for operation with a broadband or direct Ethernet WAN connection using a public network, DSL modem, or Cable modem. It supports up to 8 simultaneous remote ET units. The ET-3302 trusted interface consists of four ethernet ports configured as a four port auto-setting 10/100BaseT switch. The configuration is similar to the ET-6600 model with the following changes. The ET-3302 serial port may be used for setup or as a TCP or UDP server port. The trusted interface ports may be configured as VLAN ports.

Configuration Differences

This model contains a single serial interface to be used in initial setup (if needed). If the default IP address is not appropriate for your LAN, connect a terminal (or PC using configured for 9600,8,N,1. Follow the command line setup instructions. Once a compatible IP address is available, the browser setup screens are used for further configuration.



ET-3302 Front Panel Layout

ET-3302 Side Panel Layout

ET-3302 Ethernet Panel LED Indicators

One set of indicators For Each Ethernet Port

- The green LED to the left of each ethernet port is the Ethernet Status indicator. It is lit when the port is connected to a 100BaseT switch. It is not lit for 10BaseT connections.
- The yellow LED to the right of each ethernet port is a LAN activity indicator. This LED flashes with activity on the Ethernet (even if the activity isn't directly to this unit).

ET-3302 Side Panel LED Indicators

- Lower Blue LED is a power indicator. It should be on.
- Upper LED is not used

ET-3302 RS-232 Panel Connector

The DE-9 (PC 9-pin) connector is used for initial IP addressing setup. A cross-over cable is required to use this with any standard PC serial port. Terminal configuration is 9600 bps, 8N1 . The ET-3302 serial port may also be used as a TCP or UDP server port.

ET-6630 Specific – Two High Performance Ports

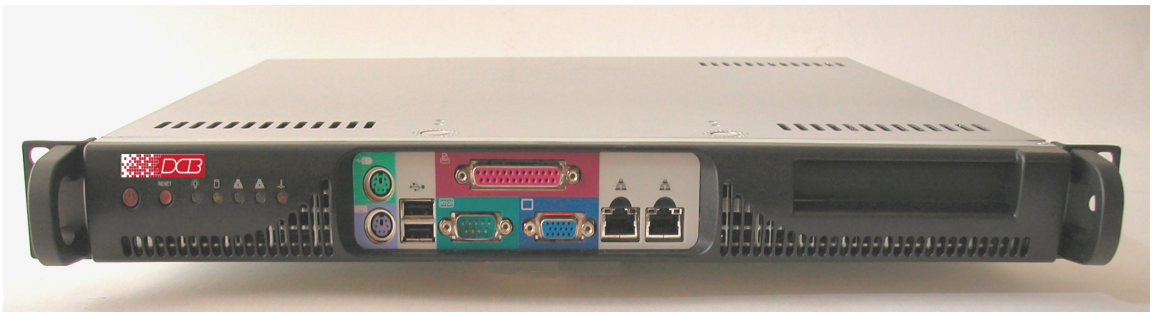
The ET-6600 family consists of various models with different internal hardware or firmware options. The ET-6630 includes two 10/100/1000BaseT High Performance Ethernet ports.

Introduction

The ET-6630 bridge contains two gigabit Ethernet ports and is normally used at the head end to support multiple remote ET products. It is often connected directly to an Ethernet WAN connection using a public high speed network, DSL modem, or Cable modem. This model supports 100 simultaneous remote units 300 Mbps throughput. The configuration is similar to the other ET models with the following changes.

Configuration Differences

This model contains a single serial interface to be used in initial setup (if needed). IF the default IP address is not appropriate for your LAN, then press the setup switch to the left of the LEDs and follow the command line setup instructions. Once a compatible IP address is available, the browser setup screens are much easier to use. This model requires a secure web browser connection for configuration (https:// IP_Address)



ET-6620

ET-6630 Front Panel

The front panel contains LED indicators and two 10/100/1000BaseT auto-switching Ethernet ports.

ET-6630 Front Panel LED Indicators

The front panel contains LEDs for Status and Power, over-temperature alarm, and drive activity. There is also a LAN activity LED, and two status LEDs for each Ethernet port.

ET-6602 Specific – Three High Performance Ports

The ET-6600 family consists of various models with different internal hardware or firmware options. The ET-6602 includes three 10/100BaseT High Performance Ethernet ports and optional internal and USB based interfaces.

Introduction

The ET-6602 model bridge contains three Ethernet ports, two optional USB ports, and one optional internal WLAN port. It is designed for operation with a broadband or direct Ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, or Cable modem and is normally used at the head end to support multiple remote ET products. It is often connected directly to an Ethernet WAN connection using a public high speed network, DSL modem, or Cable modem. This model supports 50 simultaneous remote units with throughput exceeding 30 Mbps on 100BaseT interfaces. The configuration is similar to the other ET models with the following changes.

Configuration Differences

This model contains a single serial interface to be used in initial setup (if needed). Unlike other ET models, this serial port is always available for setup. If the default IP address is not appropriate for your LAN, connect a terminal to the serial port following the instructions in the configuration section. Once a compatible IP address is available, the browser setup screens are much easier to use. This model requires a secure web browser connection for configuration (https://)

ET-6602 Front DE-6602 Rear

Rear Panel LED Indicators

One set of indicators For Each Ethernet Port

- The left LED is the Ethernet Status indicator. It is lit when there is a valid Ethernet connection, and flashes off with receive activity (incoming to the ET) (even if the activity isn't directly to this unit).
- The right LED indicates that the port is functional. It will be lit with a functional port, and will flash off with transmit (from the ET) activity.

Rear Panel USB Connectors

There are two USB connectors. They are interchangeable, and only the first one that senses a USB device connection is activated.

Rear Panel RS-232 Connector

The DE-9 (PC 9-pin) connector is used for command line setup. A cross-over cable is required to use this with any standard PC serial port. Terminal configuration is 9600 bps, 8N1 .

Rear Panel Ethernet Connectors

The three 10/100BaseT connectors are auto-sensing

Front Panel LED Indicators

- Power indicator. It should be on.

Internal WLAN Interface

Some models include an optional internal Wifi interface.

Chapter 2
Installation

This Chapter details the installation process for the EtherSeries Bridge.

Overview

The bridge is normally configured using a web browser directed to its address. If the default address of 192.168.0.1 is appropriate for your local network, then plug it in and simply direct your web browser to the bridge (without using a proxy) and continue with configuration. If this address is not appropriate for your network, the bridge's IP address must be configured using the initial terminal method below.

The remote ET bridges may be pre-configured and centrally managed for remote plug and play operation.

The CDROM contains a Configuration Worksheet document and more detailed step-by-step instructions for several commonly used configurations. Printing that document and using it is highly recommended, and will save time when first configuring the bridges.

Quick Start

Quick start instructions are in the following section. Installation is an easy process, but you are must have a thorough understanding of IP networking, subnetting, and routing. You should have a network diagram illustrating IP addresses, subnetting, and all IP routing that you intend to use prior to installing the bridge.

Help Screens and Field Edits

The field names on all configuration screens are hyperlinks to context sensitive help screens. Simply click on the field name to bring up a second window with the help information. Close that window to return to your entry screen.

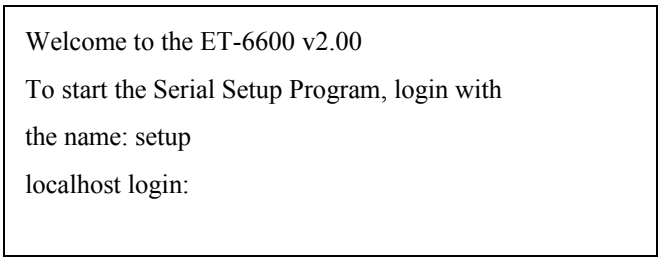
Entries are always tested for valid values. However, there are many "valid" values that are not appropriate for any given configuration. So, "appropriateness" isn't tested. For example, an IP address of 300.400.500.256 will not be accepted, but the field will accept an IP address that is not appropriate for *your* installation.

Installation and Configuration

1. Configure the Bridge's IP address

If the bridge's default address (192.168.0.1) is appropriate for your network, skip to step 2, "Connect the Ethernet Cable".

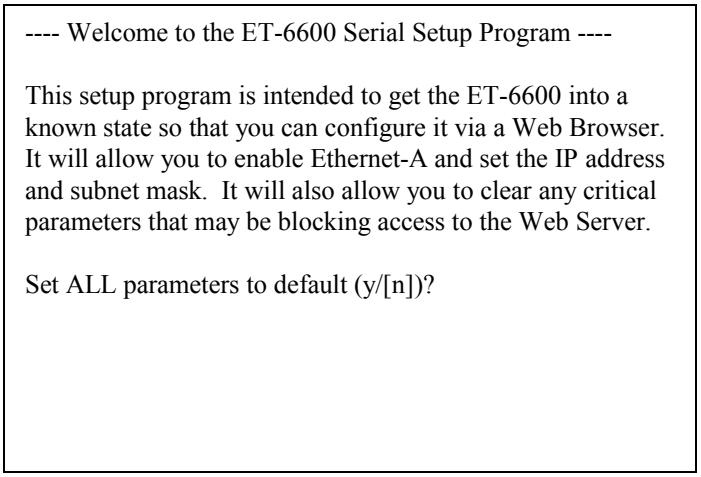
1. Connect a terminal or PC running terminal emulation program (Hyperterm, Procomm, etc) to the serial port of the bridge.
2. Start the terminal emulation program using 9600 bps, 8-bits, No parity, No flow control.
3. Power up the bridge. I required on your model, press the configuration button (small, hidden button on some models, see chapter one).



Login Screen

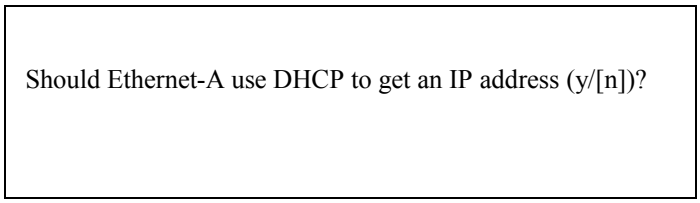
4. The Bridge will reboot pausing at a login screen. For initial setup, enter the login name "setup" in lower case letters. No password is required.

5. You will then be asked if you wish to set ALL parameters to factory defaults. If you have previously changed any values and want to return to the factory defaults, answer "Y", otherwise answer "N".



Default Screen

6.You are then asked if you wish to use the bridge as a DHCP client. If you want the bridge to pick up a DHCP address from a local DHCP server connected to ethernet A, answer "y", otherwise answer "n".



DHCP Screen

7. If you answered no to that question, you will be prompted to enter the unit's IP address and subnet mask. Enter the values for the Ethernet A interface.

8. The bridge will now compress these values and save the configuration to flash memory. Do not cycle power during this time or the unit may be rendered inoperable.

```
Saving Configuration. Do not cycle power...
Erasing flash sector 0x10fc0000
Storing file [config.tar.gz], size 1541 bytes
Store complete
Setup complete.
After rebooting the system, you will be able to configure
the unit from a Web Browser.  Use the URL
http://11.22.33.44 .
Return Switch 2 to the off (down) position
press <enter> to reboot system...
```

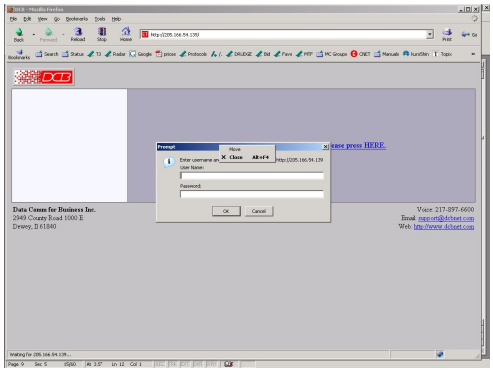
9. The bridge will now reboot.

2. Connect the Ethernet Cable

Connect a LAN cable from your hub or switch to Ethernet Port A. Reboot the bridge with a power cycle. The bridge will now be available to any web browser on the same LAN segment. If your web browser does not see the bridge, verify that you do not have a proxy server configured in the browser. If so, properly configure the browser to bypass the proxy server for this URL. The bridge's default address is 192.168.0.1. This address must be appropriate for your local LAN and workstation, or step 1 above must be followed.

3. Verify the IP Address Configuration

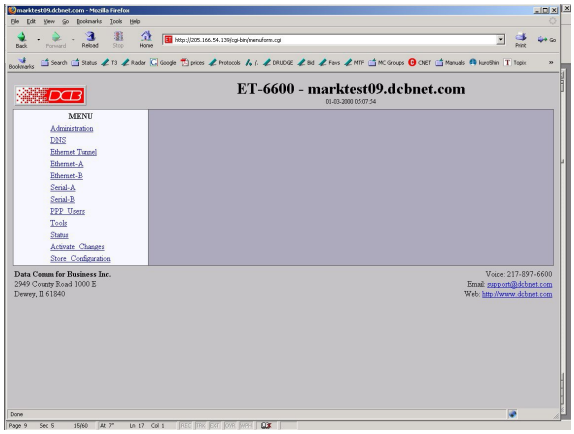
Enter the URL from step 1 (or http://192.168.0.1 if using the default address) into your web browser. The login screen below should be displayed. On some models, (including the IP-6604 and IP-6620), the secure web browser connection is required (such as https://192.168.0.1).



Login Screen

Log in using the user name "admin" and no password (blank field). If this screen doesn't display, check the Troubleshooting Section in Chapter 6.

4. Enter Your Configuration



Initial Main Menu

From this index screen, you can select a section on the left and will be taken to configuration screens for each bridge subsystem.

5. Minimum Configuration

The minimum configuration items required for basic LAN-to-LAN bridging via a serial link or WAN connection are:

1. Secure side ethernet configuration. Configure ethernet port A (IP address, etc. if not using DHCP).
2. Insecure side Serial port or ethernet port configuration. The insecure side may use either an ethernet port or a serial port. Default is to use DHCP on Ethernet port B, and disable the serial ports.
3. IP Tunnel Configuration. Defaults are acceptable for bench-testing, but not for actual use. Please change all items from default values. Default values for pass phrases and user names should NEVER be used.

Configure these items and the bridge is ready for use. Of course, you need to perform a similar installation for the companion bridge on the other LAN so it can do useful work.

Chapter 3
The Configuration Process

This Chapter describes the configuration management process on the ET-Family bridge using a Web Browser.

Overview

The ET-Family bridges contain a quite flexible configuration management system. By using this system correctly, one can remotely configure the bridge, save copies of that configuration to a PC, make configuration changes for later activation, and remote transfer firmware upgrades to the bridge.

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 bridge was last booted. However it may have been changed since boot time as described below. This is the configuration that is currently running the bridge.
2. The ***pending*** configuration: This is the current configuration that was loaded form memory when the bridge was last booted WITH any changes made by using the configuration screens. This configuration is NOT the configuration running the bridge at present.
3. The ***stored*** configuration. This is the configuration that was last written to the bridge's non-volatile RAM. The next time the bridge 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 configuration.

Using the Configuration Flexibility

When the bridge 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 memory and is the "active" 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 bridge is next reset or powered up, it will begin using the old stored configuration from before the changes were made and activate command clicked.

Using the "store configuration" screen will copy the pending configuration into Non-volatile memory. It will not cause this configuration to begin running the bridge. However, upon the next reset or power cycle, the bridge 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 bridge configuration. It allows you to test the configuration prior to saving it. If, during the testing, you notice an abnormality; you can reset the bridge to return to the last good configuration.

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

This method allows one to configure the bridge via a bridge link that will not work using the new configuration. Make the changes to the pending configuration and save them. Your current session will not be affected, but when the bridge is reset, it will begin using the new configuration. This method is useful when you are configuring a bridge to use a new LAN address range while it is on the old LAN. It's also used when a dial-up PPP connection is the management path, and the new configuration will not allow that PPP connection.

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

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

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

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 bridges in a large corporate environment.

Chapter 4
Configuration

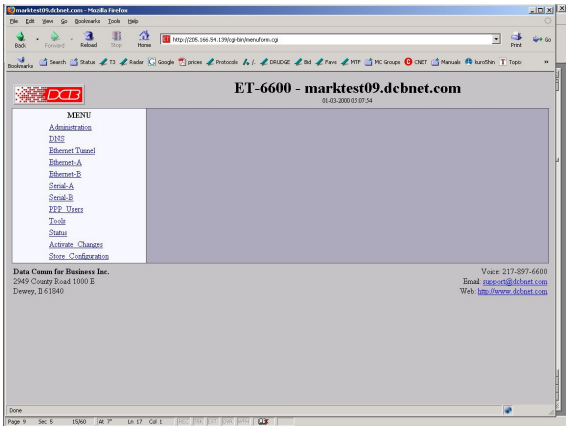
This Chapter describes configuration screens and some configuration hints for the EtherSeries ET-Family Bridge

Overview

The ET-Family bridge is configured using forms displayed on a web browser. In this chapter, we illustrate all entry forms, and describe their use. This is not a tutorial on IP, PPP, bridging, or routing. Familiarity with IP and related information is required before you can configure any ethernet product.

All configuration screens are accessed from the main index screen shown below. They are divided into sections with only one layer of screens below the top level.

Configuration screens should only be made available via the secure interface. This default operation may be changed during configuration, but it is highly recommended that configuration be locked to the secure interface. Some models (including the IP-6604 and IP-6620) requires a secure web browser connection for configuration (https://)



ET-6600 Main Screen

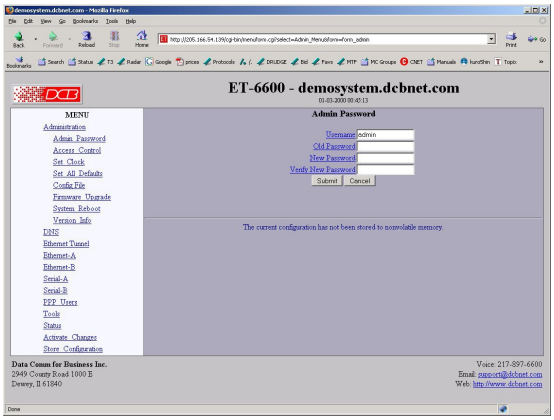
From this index, click on a menu keyword to open the appropriate screen. In this manual, screens are discussed in the order shown on the index screen.

Note that some screens are model specific, and some models do not contain all screens shown.

Administration

The Administration section contains screens used to configure system-wide settings and perform a few high level operations.

Admin Password



Admin Password Screen

The ET web server screens are available ONLY via the secure side of the bridge.

Access to the ET's Web Server is protected by HTTP Basic Authentication and uses the secure web server. 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. For some models (including the ET-6604 and ET-6620), use https: (instead of http:) when addressing ET web browser screens.

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

Fields

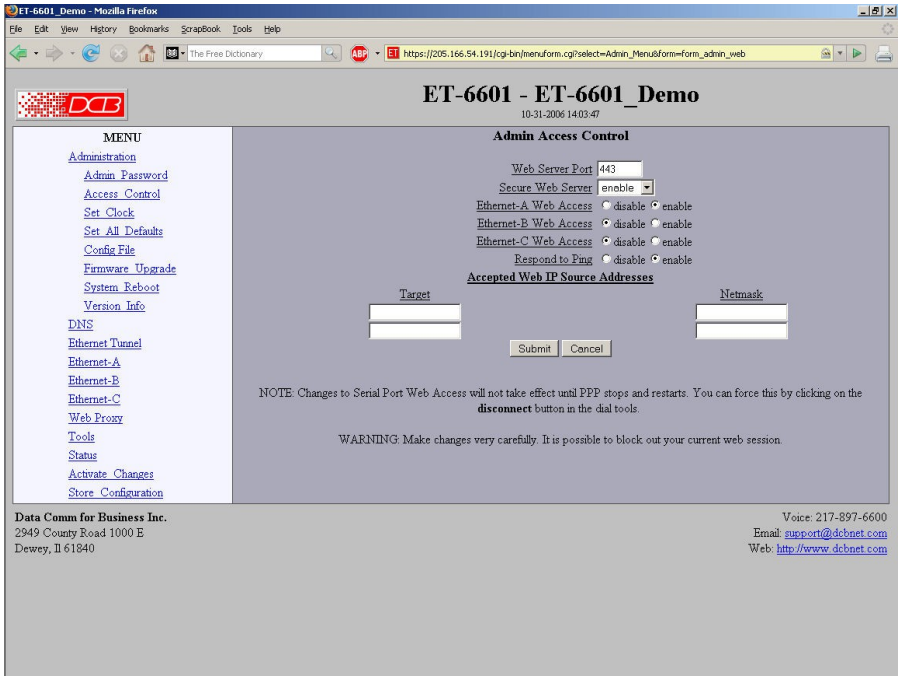
- User Name
  This field may be a string of 0 to 15 printable characters. Do not use space or control characters. If you leave this field blank, you will need to enter a blank username during authentication.
- Old Password
  In order to change the username and password, you must know the old password. 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.
- Verify New Password
  Retype the password to verify that it was correctly entered.

Notes

- If you forget your username or password, you can use the Serial Port Setup to erase the current settings and return the unit to factory defaults.

- Security Note: HTTP Basic Authentication may be easily hacked if the attacker has the ability to sniff network packets. For this reason HTTPS: secure sockets layer methods are used. The username is transmitted in the clear and the password is transmitted in an obfuscated but possibly recoverable format. For this reason, configuration should only be available via the secure ethernet interface on the bridge. This operation is configurable via the Admin Access Control screen.

Admin Access Control



Administrative Access Control Screen

Access Control allows you to place further restrictions on access to the ET's internal web server.

Fields

- Web Server Port
  This is the TCP Port to use for the ET's internal Web Server. Typically it is set to port 80. However you may set it to any value between 1 and 65535.

  There are several reasons that you may want to change the web server port. By changing it to a non-standard value, you reduce the chance that a random attacker will find the ET's web interface and attempt to break in. A different port may be needed to accommodate local firewalling.

  If you change the web server port number to any value other that 80, remember that you will have to include the port number in your URL. For example, https://192.168.0.1:7995 OR http://192.168.0.1:7995 .

- Secure Web Server
  Some high performance versions allow the use of secure sockets web configuration. If this is enabled, instead of http://address, you must use https://address to access the configuration screens. It is much more secure than using the regular web server for configuration.

- Respond to Ping
  This item allows you to block ping requests to the ET. Ping is a valuable tool for diagnosing network problems, but can also become a security problem. Disabling ping causes the ET to not respond to ping requests for one of its IP addresses. It has no effect on the ET's passing of ping request and responses from other network nodes.
- Web Access
  These options allow you to block web access through the specified interface. If you are using the tunnel to bridge across a public network, you are strongly advised to disable web access from the interface attached to the public network.
- Accepted Web IP Source Address
  This table allows you to control what hosts or networks have access to the ET-6600's web server. If empty, any host may access the unit.

  Entries are made by specifying a Target and Netmask. For example, if you want to allow only the host 192.168.10.16 access, you would enter:
  Target: 192.168.10.16 Netmask:255.255.255.255.

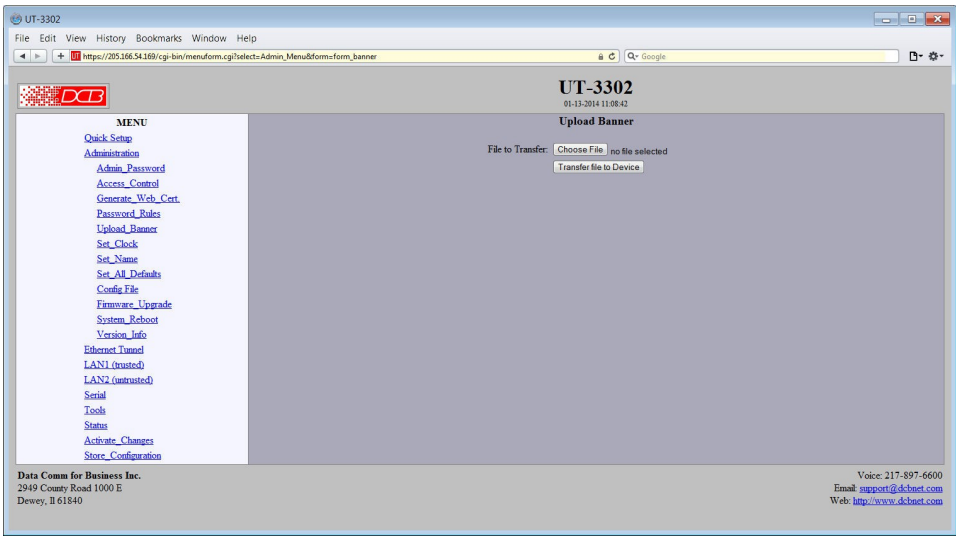
  If you wanted to allow access to all hosts in the range 192.168.10.1 to 192.168.10.255, you would enter:

  Target: 192.168.10.0 Netmask: 255.255.255.0
- Target
  Host or Network address.
- Netmask
  If blank or set to 255.255.255.255, target is assumed to be a host address. Otherwise, target is treated as a network address.

Notes

Remember to submit the change by clicking the “SUBMIT” button.

Upload Banner



Upload Banner Screen

This form allows you to set the upload a custom banner screen that is displayed during administrative log-in.

Fields

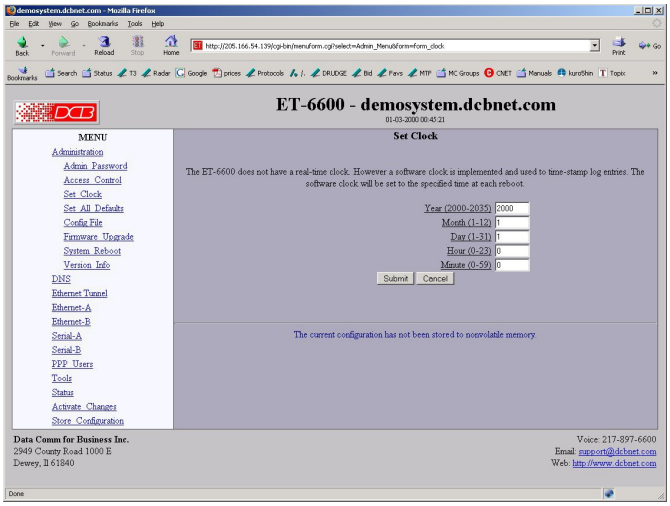
File to Browse Click this button to find and select a banner file to upload. This file accepts standard HTML tag formatting, but it will be embedded into another html file, so use caution with complex tags.

Transfer file to Device Click this button to actually upload the selected file to the tunnel.

Notes

It is good practice to test your uploaded file using a web browser to make sure it has no html tags that will hang the browser.

Set Clock



Set Clock Screen

This form allows you to set the ET'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.

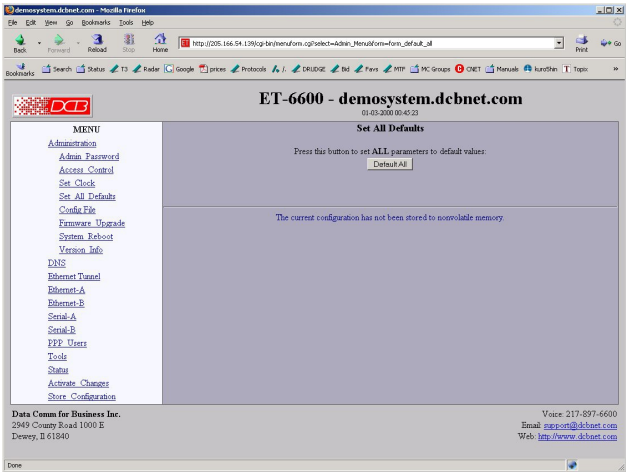
Hour Hour of the day in the range 0 to 23.

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.
- Some models of the ET do not contain a real-time clock, nor have 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 for those products are the “boot” values… not the current time.

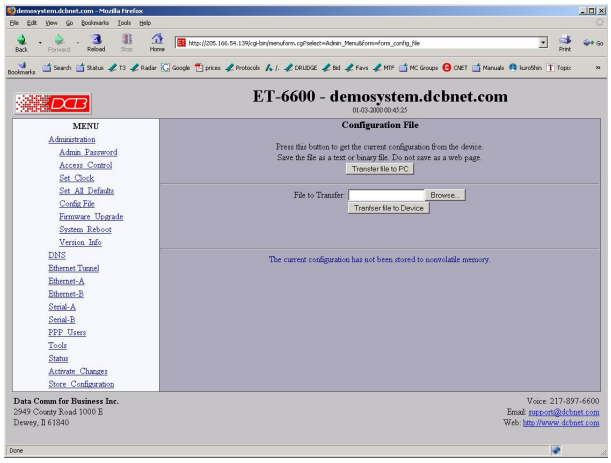
Set All Defaults



Set All Defaults Screen

This form will allow you to set all tunnel parameters to their default value. Before you "Activate Changes", you should configure the interface that you are using to access the tunnel. Otherwise, all interfaces except Ethernet-A will be disabled and Ethernet-A will be configured with the IP address of 192.168.0.1.

Configuration File



Configuration File Screen

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

Fields

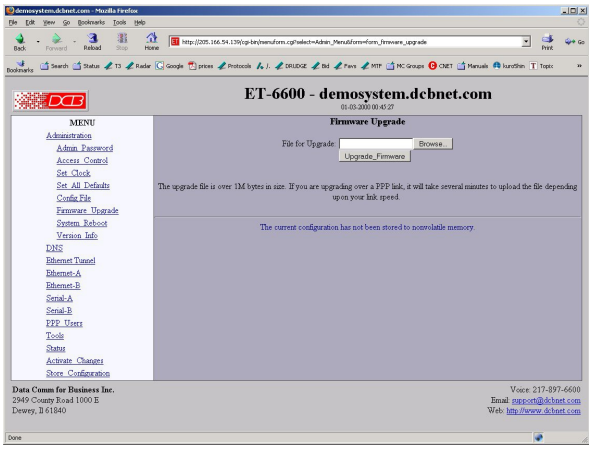
- File to Transfer
  This is the name of the configuration file on your PC to be transferred to the bridge.
- Transfer file to PC (action)
  Transfers the current bridge configuration file to this PC.

- Transfer file to Bridge (action)
  Transfers the named file to the bridge.

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 bridge, 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 bridge will immediately begin using the new configuration. If the changes are stored, the bridge will use the new configuration only after a reboot or reset.
- If you activate the new configuration, first be sure that you can access the bridge using its new configuration. Otherwise, it may be necessary to return to the old stored configuration with a reset.
- You must SECURE this text file on your PC with encryption, or move it to a secure place. Access to the saved configuration file may compromise the security of your ET

Firmware Upgrade



Firmware Upgrade Screen

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

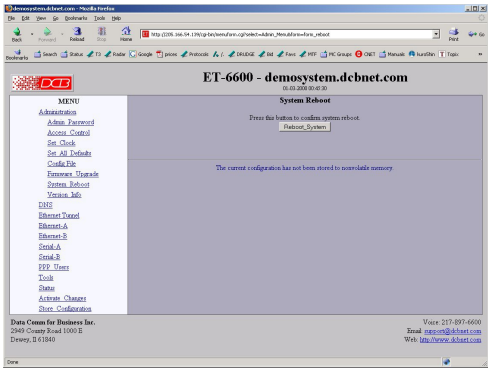
Fields

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

Notes

You should only use a firmware image obtained directly from DCB. The firmware image is encrypted, so be sure to use the correct file name as it was supplied by DCB.

System Reboot



System Reboot Screen

This form will allow you to reboot the ET. 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.

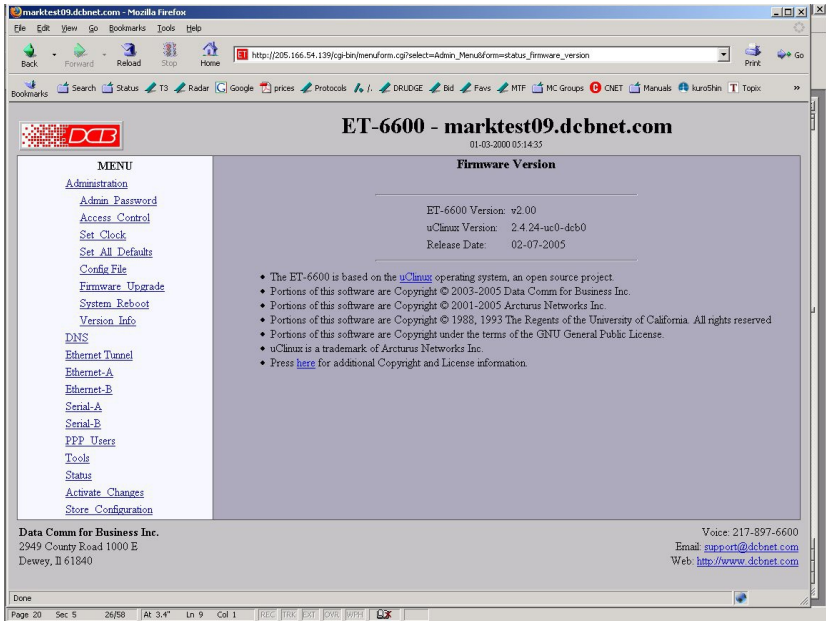
Fields

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

Notes

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

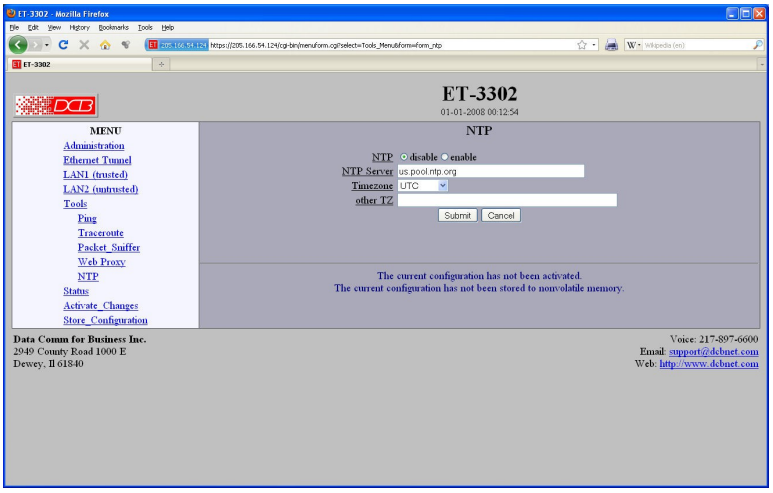
Version Information Screen



Version Information Screen

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

NTP



NTP Screen

Some models of the ET provide for setting the internal clock with a NTP server. Use of NTP is optional. If NTP is used, there must be a valid path to the NTP server from either the secure or insecure side of the ET.

Fields

- NTP
  Enable/Disable the NTP client. When enabled the NTP client will request the current time from a time server and set the software clock. It will repeat this process every 24 hours.
- NTP Server
  This field is set to the IP address or host name of a NTP server. If a host name is used, DNS must also be configured.
- Time Zone
  NTP servers report the time in Coordinated Universal Time (UTC). If you wish to convert UTC time to your local time, you must specify the timezone. If your timezone is not in the preconfigured list you may select *other TZ* then encode your timezone in the following field.
- Other TZ
  The timezone is encoded as follows:

```
stdoffset[dst[offset][,start[/time],end[/time]]]
```

std and dst Three to five characters that are the designation for the standard (std) or the alternate (dst) timezone. Only std is required; if dst is missing, then the alternate time will not apply.

offset Indicates the value added to the local time to arrive at UTC. The offset has the form:

```
hh[:mm[:ss]]
```

The hour (hh) is required and may be a value between -24 and 24. The minutes (mm) and seconds (ss) are optional.

rule Indicates when to change to and from alternate time. The rule has the form:

```
date[/time],date[/time]
```

The first date describes when to change to alternate time and the second date describes when to change back to standard time. Date is encoded as follows:

```
Mm.n.d
```

Month (m) is 1 - 12. Week (n) is 1 - 5, where 5 indicates the last occurrence of the day in the month. Day (d) is 0 - 6 where 0 represents Sunday.

Time is optional. If not specified, it will default to 2am. Time is entered as:

```
hh[:mm[:ss]]
```

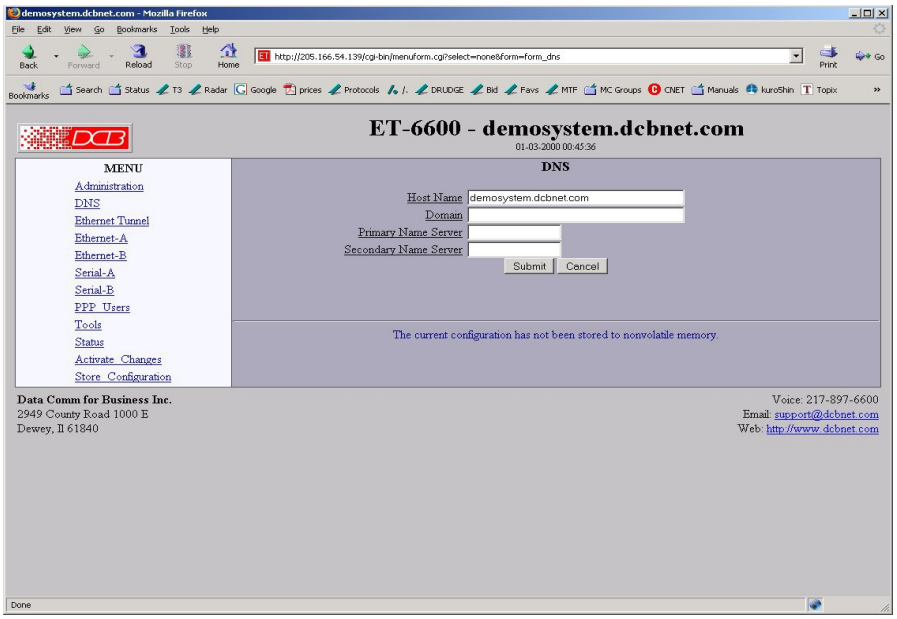
As an example, US Central time is 6 hours behind UTC during standard time and 5 hours behind UTC during daylight savings time. Daylight savings time takes effect the 2nd Sunday in March at 2am. Standard time resumes the 1st Sunday in November at 2am. It would be encoded as follows:

```
CST6CDT5,M3.2.0/2,M11.1.0/2
```

Notes

- The bridge does not act as a NTP server.
- Use of NTP is optional.
- See the help screens for more information

DNS



DNS Screen

The Domain Name System, DNS, is a distributed database used by applications to map between IP addresses and hostnames. The ET has support for the client side of DNS. It does not act as a DNS server. The DNS settings are passed to remote PPP users and DHCP clients. Use of DNS is optional.

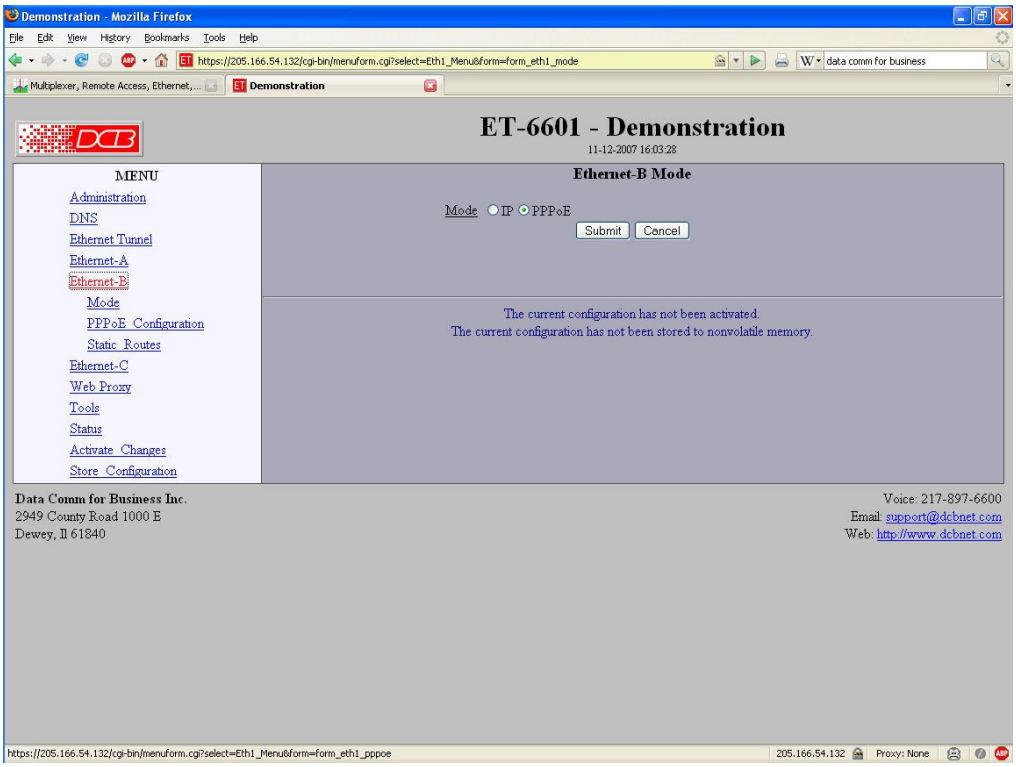
Fields

- HostName
  The name given to the ET. If you enter a name, it will also be displayed on the title of the web pages.
- Domain
  The name of the local domain. For example: widgets.com
- Primary DNS Server
  The IP address of the primary DNS server. This value will be provided to remote PPP users during option negotiation.
- Secondary DNS Server
  The IP address of the secondary DNS server. This value will be provided to remote PPP users during negotiation.

Notes

- The bridge does not act as a DNS server.
- The DNS settings are passed to remote PPP users
- Use of DNS is optional.

Ethernet Mode



Ethernet Mode Screen

The ET may contain multiple Ethernet interfaces.

Some models may use PPPoE. On those models, there will be an Ethernet Mode screen, used to select the mode for each ethernet port (other than Port A, which cannot use PPPoE). See the Ethernet PPPoE configuration screen section for information pertaining to PPPoE.

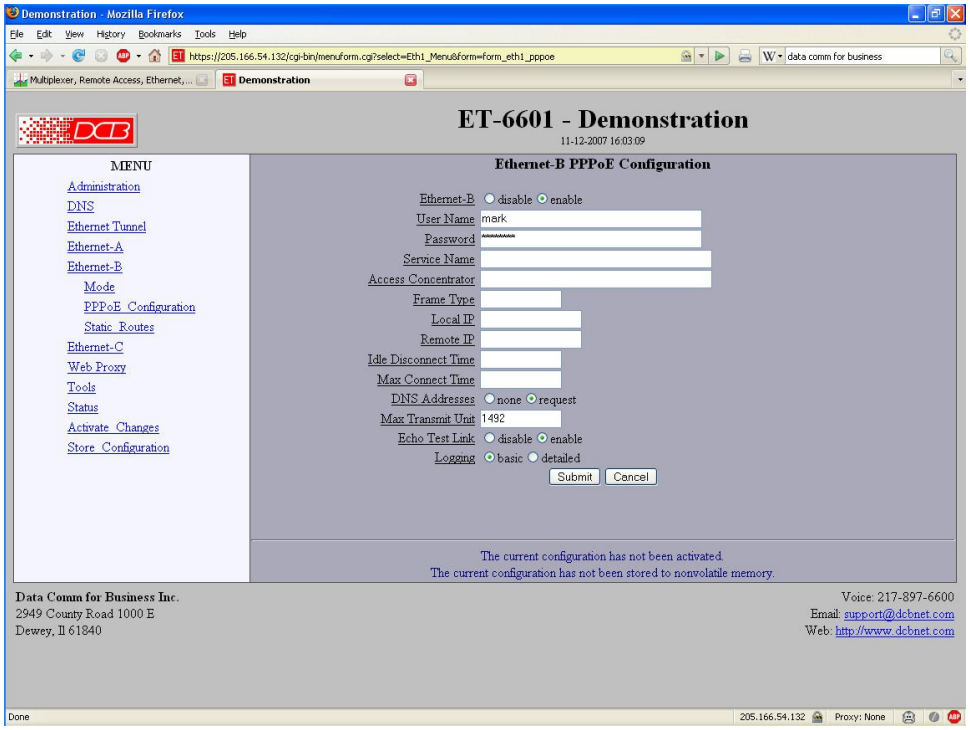
Fields

- Mode
  Each Ethernet interface (other than Ethernet A) may be configured as an IP interface or a PPPoE (Point to Point Protocol Over Ethernet) interface. Select the appropriate one for this interface. Unless you are certain the interface will use PPPOE, IP is the correct default selection.

Notes:

The selection on this screen will determine which Ethernet configuration screen is displayed in the menu. Either the IP configuration screen or the PPPoE configuration screen will be available.

Ethernet PPPoE Configuration



Ethernet PPPoE Configuration Screen

Some models may use PPPoE. On those models, there will be an Ethernet Mode screen, used to select the mode for each ethernet port (other than Port A, which cannot use PPPoE). This screen is only available for those interfaces that have the mode configured to PPPoE.

Fields

- Enable/Disable
  Each interface may be individually enabled or disabled. If you do not plan to use an interface, it is a good idea to disable it. Doing so will free up system resources.
- User name
  This is the user-name to use when authenticating to a PPPoE Server. In other words, this is the user-name sent to the remote server. The user-name may be a string of 1 to 39 printable characters. No space or control characters.
- Password
  This is the password to use when authenticating to a PPPoE Server. In other words, this is the password sent to the remote server. The password may be a string of 1 to 39 printable characters. No space or control characters.
- Service name
  This is an optional field that specifies the desired service name. If set, PPPoE will only initiate sessions with access concentrators which can provide the specified service. Only set this field if instructed to by your ISP.

- Access Concentrator
  This is an optional field that specifies the name of the desired access concentrator. If set, PPPoE will only initiate sessions with the named access concentrator. Only set this field if instructed to by your ISP.
- Field Type
  This is an optional field that sets the Ethernet frame type for PPPoE discovery and session frames. This field is only used if your ISP uses non-standard PPPoE frame types. The frame types are specified as hexidecimal numbers separated by a colon. For example: 8863:8864. Only set this field if instructed to by your ISP.
- Local IP
  Each side of a PPP connection will have an IP address. This is the IP address to use for the local PPP device. With PPPoE, you will normally leave this field blank. The PPPoE server will automatically assign an IP address upon connection.

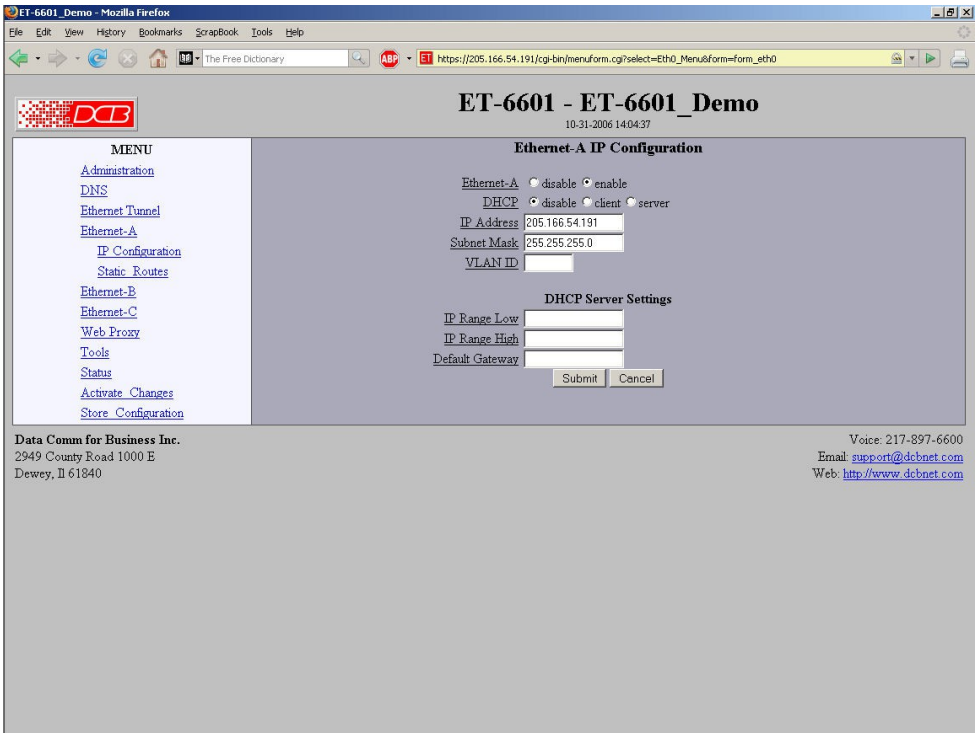
  If you leave this field blank when connecting on-demand, the ET will temporarily assign a local address to the PPPoE interface until actual PPPoE connection is brought up.
- Remote IP
  Each side of a PPP connection will have an IP address. This is the IP address to assign to the remote PPP device. With PPPoE, you will normally leave this field blank. The PPPoE server will report the IP address upon connection.
- Idle Disconnect Time
  Setting an *Idle Disconnect Time* will enable connecting on-demand. The PPPoE connection will come up where there is IP traffic to route out the PPP link and will terminate when the link is idle for the specified amount of time (in minutes).

  This feature is typically used when your ISP charges for service based on connect time.
- Max Connect Time
  Setting *Max Connect Time* will cause the PPPoE connection to terminate when the time limit has been reached, regardless of activity. The time is set in minutes.

  This feature is normally not needed and only used as a workaround for various ISP problems.
- DNS Address
  When set to *request*, the local ET will request DNS addresses from the PPPoE Server during PPP option negotiation. When set to *none*, the local ET will not request DNS addresses, and will use the static DNS configuration.
- MTU
  This selects the maximum transmit unit and maximum receive unit for the PPPoE interface. Outgoing network packets will be limited to the specified size. The peer will be asked to limit its MTU to this size. The peer may negotiate a smaller size. The value may be between 128 to 1500. For PPPoE, the recommended setting is 1492.
- Echo Test Link
  When enabled, an LCP level echo request will be sent periodically (30 seconds) to the PPPoE Server. If the server fails to respond to 4 consecutive requests (2 minutes), the link will be taken down and reestablished.
- Logging
  This selects the level of information placed in the PPP log file.

Notes:

Ethernet A/B Configuration



Ethernet Configuration Screen

The ET may contain multiple Ethernet interfaces. Depending upon the actual model, Ethernet-A is typically a higher speed 10/100 (or 10/100/1000) controller configured for auto-sense and typically used for the "local" trusted LAN. Ethernet-B often is 10BaseT only. Ethernet port A is always a local, secure side of the tunnel. The public network interface may be either Ethernet port B, port C, or a serial port. On two port models, Ethernet B is always the insecure side, and is usually used with a broadband WAN or public Internet connection. This screen is used to configure both IP parameters and DHCP server parameters (if the DHCP server function is used)

Some models may use PPPOE. On those models, there will be an Ethernet Mode screen, used to select the mode for each ethernet port (other than Port A, which cannot use PPPOE). See the Ethernet PPPOE configuration screen section for information pertaining to PPPOE.

Fields

- Enable/Disable
  Each interface may be individually enabled or disabled. If you do not plan to use an interface, it is a good idea to disable it. Doing so will free up system resources.
- DHCP Fields
  Dynamic Host Configuration Protocol, DHCP, is a client/server protocol automating the configuration of systems using TCP/IP. Client systems will broadcast a request asking for configuration. Server systems will respond, assigning the client system an IP address and providing other related configuration information such as subnet mask, DNS, and gateway addresses.

  If you enable DHCP Client, the tunnel will request and IP configuration from a DHCP server. It is

common to enable DHCP client on a broadband interface to an Internet Service Provider. In the case of the tunnel, that would be Ethernet-B.

When DHCP Client is enabled, the IP Address and Netmask fields are ignored.

- IP Address
  an IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. If you are directly connected to the Internet, it must globally unique.
  This field is not used if DHCP Client has been enabled. The DHCP server will assign the IP address.
- Subnet Mask
  A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, many subnets have a mask of 255.255.255.0. This means the first 24 bits of the address is the subnet identifier and the last 8 bits is the host identifier.

  This field is not used if DHCP Client has been enabled. The subnet mask will be assigned by the DHCP server.
- VLAN ID
  If the ethernet interface is attached to an 802.1Q trunk, you must specify a VLAN ID number for the interface. The IP address will be then be bound to this VLAN. This will allow you to access the tunnel's web server through the 802.1Q trunk from the specified VLAN. Valid range is 0 - 4095. Leave blank to disable.
- DHCP Server Settings
  If this unit is to be a DHCP server, the low and high limits for assigned addresses and default gateway must be entered in this section.
- Monitor Link
  When this option is set to *yes* the Ethernet port will be monitored for link loss. If the link goes down, the unit will try to renew or reaquire an IP address from the DHCP server when the link is restored.

  This option only applies when the interface is configured to automatically acquire an address from a DHCP server. It is not available on all models, and is only available on the WAN ports.

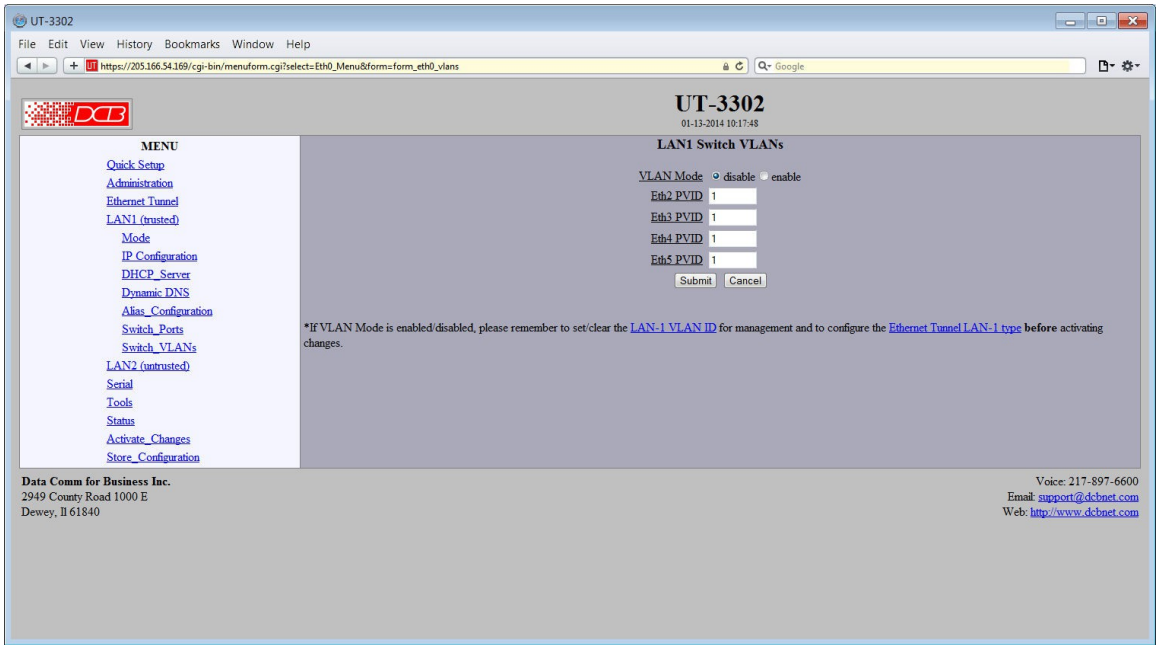
Notes:

The DHCP Client may not be used on Ethernet-A if it is configured for an 802.1Q VLAN.

If DHCP client mode is used, the IP address fields are ignored.

For maximum throughput, always disable unused interfaces.

Switch VLANs



LAN 1 Switch VLANs Screen

This configuration applies to the integrated 4-Port Ethernet switch attached to LAN-1 of the ET-3302 model. In common installations, the switch operates as a basic Ethernet switch, transparently passing Ethernet frames between ports and also across the tunnel connection.

However, the switch can also operate in 802.1Q VLAN mode. In this mode, each port is assigned to a VLAN. Ethernet frames received on a port will have an 802.1Q VLAN tag added to the frame. Out-bound frames must have a matching VLAN tag and the VLAN tag will be removed on output. This allows the individual Ethernet ports to be segregated into VLAN groups that extend across the tunnel connection.

Use of the feature requires that the peer tunnel device likewise operate in 802.1Q mode or that the peer tunnel device has an external 802.1Q switch connected to the trusted port.

Before **activating** this feature, make sure to also configure LAN-1 with a VLAN ID, assigning it an accessible VLAN (either on one of the switches or via a separate VLAN switch using the VLAN trunk connection. This is the VLAN from which you will manage the tunnel device.

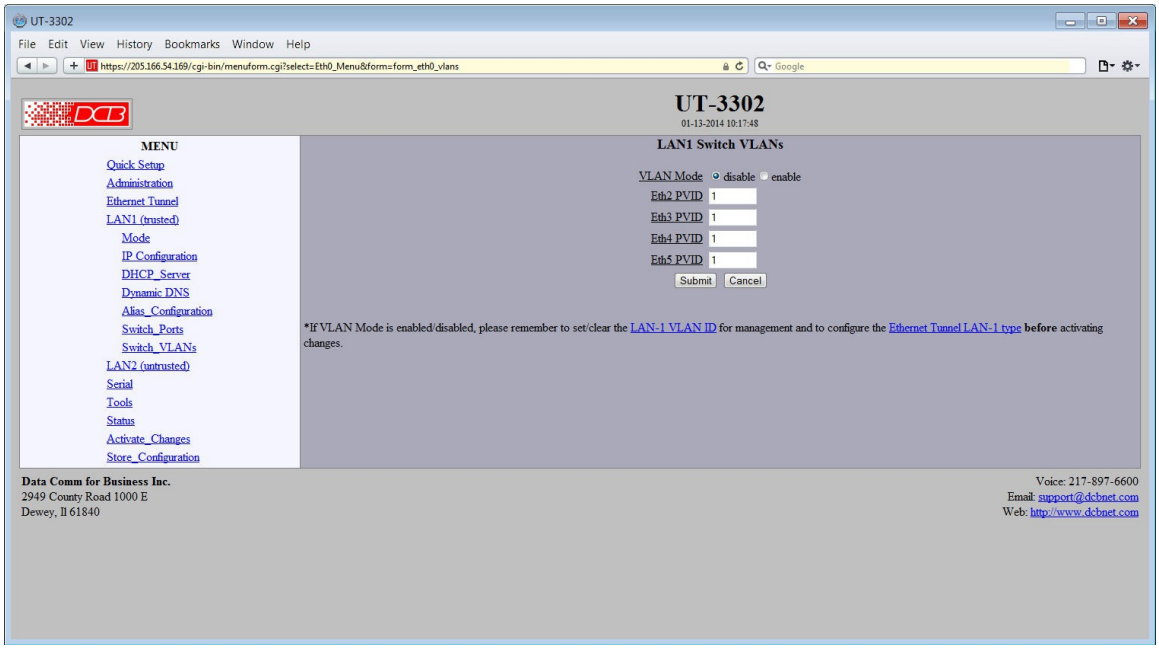
Fields

- VLAN Mode
  Disable or enable. The default is disabled.
- Port Eth#
  Eth# port VLAN ID (0 - 4095).

Notes:

If VLAN Mode is enabled/disabled, please remember to set/clear the LAN-1 VLAN ID for management and to configure the Ethernet Tunnel LAN-1 type **before** activating changes.

Switch VLANs



LAN 1 Switch VLANs Screen

This configuration applies to the integrated 4-Port Ethernet switch attached to LAN-1 on the ET-3302 model only. In common installations, the switch operates as a basic Ethernet switch, transparently passing Ethernet frames between ports and also across the tunnel connection.

However, the switch can also operate in 802.1Q VLAN mode. In this mode, each port is assigned to a VLAN. Ethernet frames received on a port will have an 802.1Q VLAN tag added to the frame. Out-bound frames must have a matching VLAN tag and the VLAN tag will be removed on output. This allows the individual Ethernet ports to be segregated into VLAN groups that extend across the tunnel connection.

Use of the feature requires that the peer tunnel device likewise operate in 802.1Q mode or that the peer tunnel device has an external 802.1Q switch connected to the trusted port.

Before **activating** this feature, make sure to also configure LAN-1 with a VLAN ID, assigning it an accessible VLAN (either on one of the switches or via a separate VLAN switch using the VLAN trunk connection. This is the VLAN from which you will manage the tunnel device.

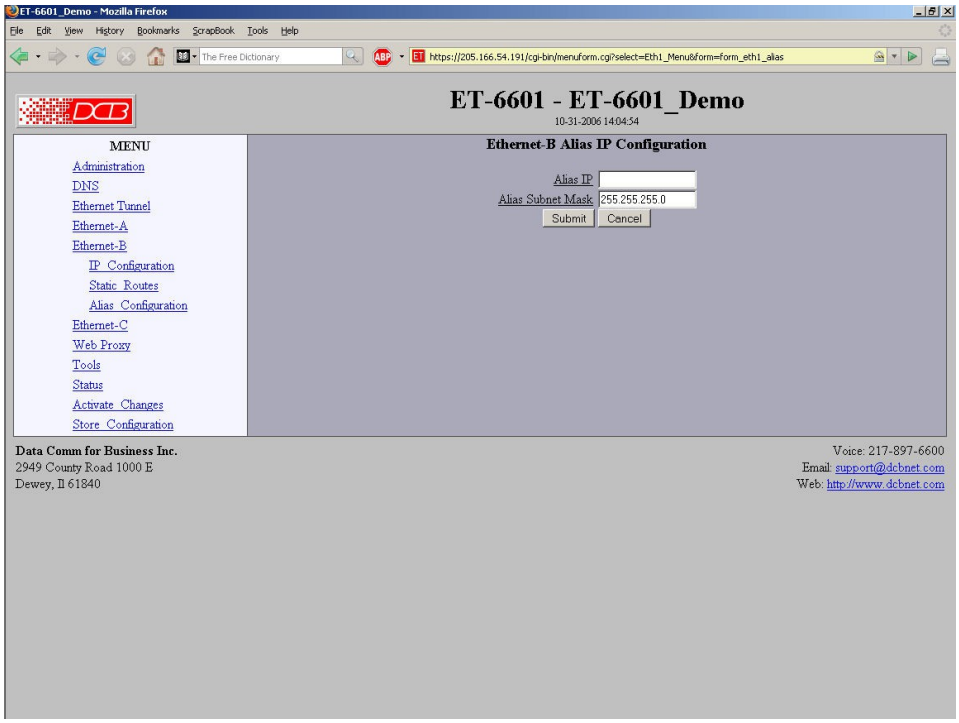
Fields

- VLAN Mode
  Disable or enable. The default is disabled.
- Port Eth#
  Eth# port VLAN ID (0 - 4095).

Notes:

If VLAN Mode is enabled/disabled, please remember to set/clear the LAN-1 VLAN ID for management and to configure the Ethernet Tunnel LAN-1 type **before** activating changes.

Ethernet Alias Configuration



Ethernet Alias Configuration Screen

An Alias IP Address can be used to ease setup of an Ethernet to Wireless adapter. When using an adapter, you often run into a problem where you need Ethernet-B to acquire a DHCP address, but to do so, you must access the wireless adapter to select the wireless network. However, you are unable to access the wireless adapter because Ethernet-B does not have an address. To solve this problem, you can assign Ethernet-B an alias IP address, and assign the wireless adapter an address on the same subnet. This is useful when the ET is used along with a wireless broadband connection, such as from a hotel room.

Fields

- Alias IP Address
  An Alias IP address is a secondary IP address given to an interface. This is an optional field.
- Subnet Mask
  The subnet mask for the alias IP address

Notes:

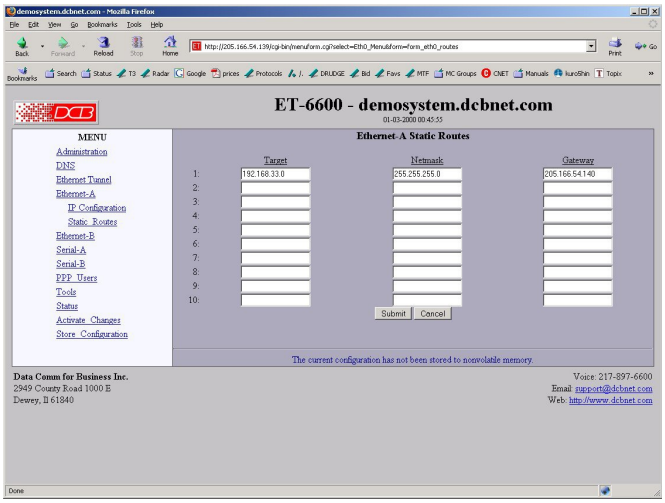
Here are the basic steps to setting up access to the wireless adapter.

- If your wireless adapter has an IP address that is on the same subnet as your private (Ethernet-A) network, you will need to change it before you attach it to Ethernet-B. Please see the recommended addresses below.

- Set the Ethernet-B alias IP and subnet mask to an address compatible with the address of your wireless adapter.
- Enable the Web Proxy Server in your ET device.
- Set your computer's Web Browser to use the ET as a Web Proxy.
- You can now web browse to the wireless adapter and select the wireless network.

Wireless adapters often have a default IP address on the 192.168.0.x or 192.168.1.x subnet. These addresses will often conflict with the public network or may conflict with your own private network. To reduce the chance of conflict, we recommend you change the IP address to a less used address on a small subnet. For example, set the Wireless device to 192.168.70.113, the Ethernet-B alias IP to 192.168.70.114, and the subnet mask to 255.255.255.252.

Static Routes Screen



Static Routes Screen

The tunnel maintains several tables of Static Routes. There is one for each possible interface. The routes defined in the associated table are applied when an interface comes up and are automatically removed when an interface goes down. It is important that routes be placed in the correct table. The rule-of-thumb is to **apply a route to the interface that the routed packet should go out**. For example, if you want your default route to go out the PPP link on Serial-A, you would add the default routing entry to Serial-A's static routing table. If you want packets to address 192.168.10.54 to go out Ethernet-A, you would add a routing entry to Ethernet-A's table.

The tunnel will automatically create a route for each interface. For Ethernet, this will be a network entry based on the IP address and netmask of the interface. For PPP links, this will be a host entry for the IP address of the remote PPP device. Routes for the PPP links do not have a default gateway as that is implied as being the PPP link.

You can view that Active Routing Table from the Status Menu/Routing Table.

Fields

Target
Destination Host or Network address. Use a target address of 0.0.0.0 to specify a default route.

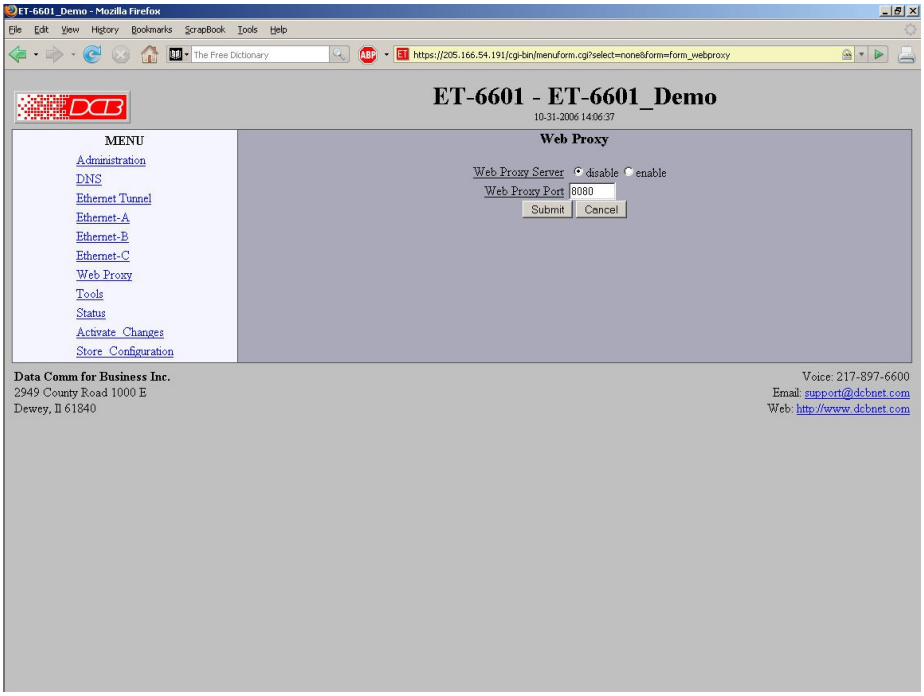
Netmask
If left blank or set to 255.255.255.255, the target is assumed to be a host address. Otherwise, the target is assumed to be a network address and the netmask specifies which address bits are significant.

Gateway
The IP address of where to forward packets to. The Gateway field is only available for Ethernet interfaces. If you leave it blank, the ET-6600 will assume the target is on the local network segment.

Notes

- Use a netmask of 0.0.0.0 to specify a default route.
- PPP links do not need a gateway address as the remote PPP device is the only possible gateway

Web Proxy Configuration Screen



Web Proxy Configuration Screen

The Web Proxy Server allows you to use the tunnel as a local HTTP proxy, directing HTTP requests directly onto the insecure network instead of tunneling them to your remote network.

The Web Proxy server can be helpful when using the tunnel on a hotel network, which requires authentication before access is allowed to the Internet.

In order to use the web proxy server, you will need to configure your web browser. For Internet Explorer, this can be found in Tools - Internet Options - Connections - LAN Settings. For Firefox, this can be found in Edit - Preferences - Connection Settings. Do not use the auto-detect feature. Manually set the IP address and port number. Use the IP address of the Ethernet-A interface as the proxy server address.

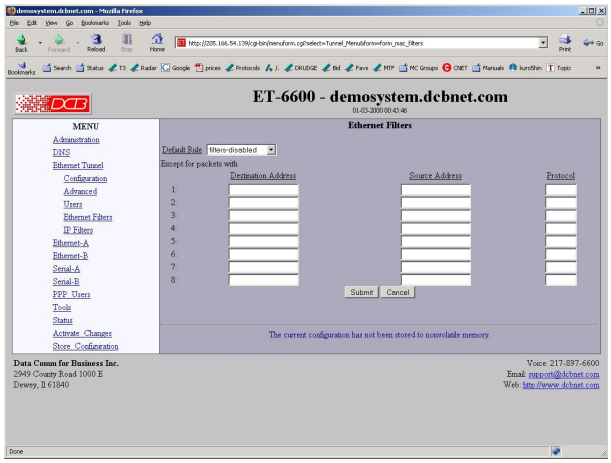
Fields

- Web Proxy Server
  This item enables/disables the web proxy server.
- Web Proxy Port
  The TCP port number that the web proxy will listen to for connection requests. This will need to match the port number in your web browser's configuration.

Notes:

In order to use the web proxy server, you will need to configure your web browser. For Internet Explorer, this can be found in Tools - Internet Options - Connections - LAN Settings. For Firefox, this can be found in Edit - Preferences - Connection Settings. Do not use the auto-detect feature. Manually set the IP address and port number. Use the IP address of the Ethernet-A interface as the proxy server address.

Ethernet (MAC) Address Filters Screen



Address Filters Screen

The tunnel can be configured to drop all packets except those with an approved source or destination MAC address. This is configured separately for each interface and occurs as packets are received on the interface.

This feature allows one to limit tunnel client connections from the public side of the bridge.

If all entries in the table are blank, all addresses are accepted.

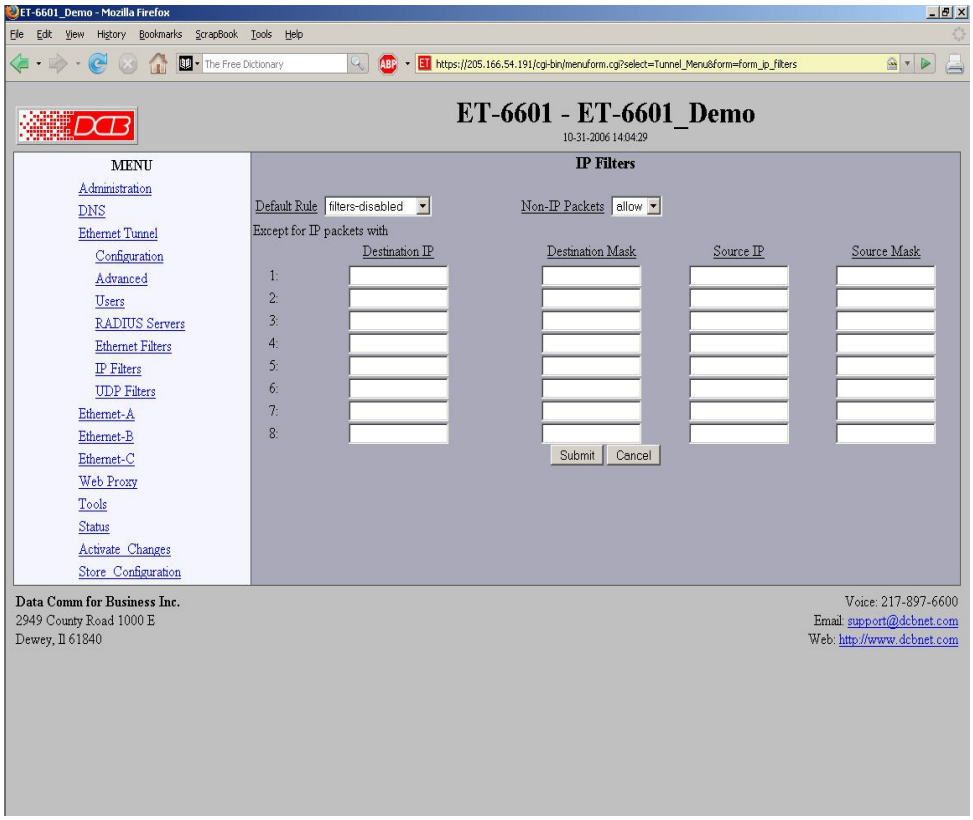
Fields

- Default Rule
  The table may be configured with the defaults of "allow all packets except", "drop all packets except", or filters disabled.
- IP Address
  Host or Network source IP address to allow.
- Netmask
  If the Netmask is blank or 255.255.255.255, the IP address is treated as a host address. Otherwise the IP address is treated as a network address and the netmask indicates the significant bits.

Notes

CAUTION: Keep in mind that you may prevent access to the ET's internal web server through the associated interface filters.

IP Address Filters Screen



Address Filters Screen

IP filters are used to limit the Ethernet packets sent from the local tunnel to a remote tunnel. This level of filtering is performed on IP(0800) and ARP(0806) packets by comparing the destination and source addresses against a table of rules. To use IP filtering, you first select a default rule. That is, you choose to allow all IP packets by default, or to drop all IP packets by default.

Next, you enter one or more exceptions to the default rule. An exception consists of a destination and a source IP address. Any packet matching both the destination address and the source address will be considered an exception, causing the opposite of the default rule to be performed. Addresses are entered in address, mask format. This allows you to specify a single host address or a subnet range. An entry of 0.0.0.0, 0.0.0.0 will match any address.

Please note that IP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

IP filtering is performed after Ethernet Filtering. Any packets discarded by Ethernet filtering will not reach IP filtering.

Fields

- Default Rule

  This field specifies the action to be taken when an IP or ARP packet does not meet any of the exception rules.

- Non-IP Packets
  This field specifies the action to be taken when an Ethernet packet is not an IP or ARP type packet. This is simply a shortcut to setting up Ethernet Filters to block all non 0800 and 0806 type packets.
- Destination IP Address
  This field specifies the Destination IP address for comparison with the packet. The Destination Mask is applied, allowing a single host or a subnet range. If blank, the field is assumed to mean any address and is the same as entering an IP of0.0.0.0 and a mask of 0.0.0.0. If both the destination and source address is blank, the entire rule is ignored.
- Destination Address Mask
  This field specifies the address mask. The mask is logically ANDed with the Destination IP address to extract the significant portion of the IP address. If the mask is blank, but the IP address is not blank, the mask is assumed to be 255.255.255.255. In other words, the IP address is treated as a host address.Notes
- Source IP Address
  This field specifies the Source IP address for comparison with the packet. The Source Mask is applied, allowing a single host or a subnet range. If blank, the field is assumed to mean any address and is the same as entering an IP of0.0.0.0 and a mask of 0.0.0.0. If both the destination and source address is blank, the entire rule is ignored.
- Source Address Mask
  This field specifies the address mask. The mask is logically ANDed with the Source IP address to extract the significant portion of the address. If the mask is blank, but the IP address is not blank, the mask is assumed to be 255.255.255.255. In other words, the IP address is treated as a host address.

Notes

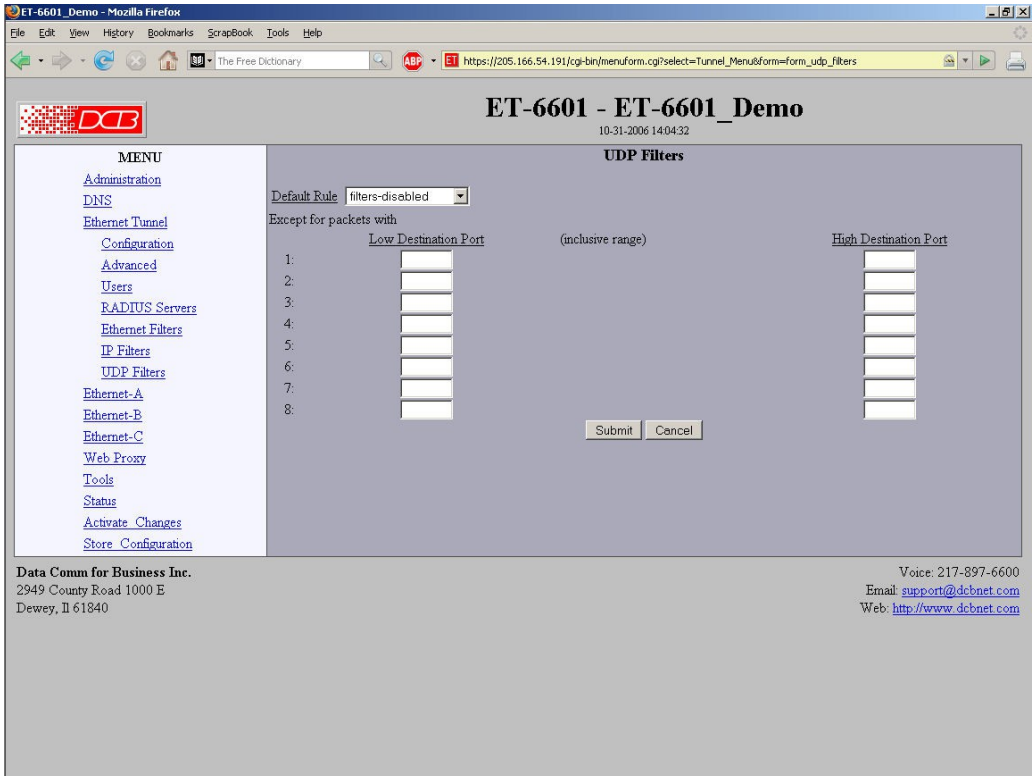
Please note that IP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

IP filtering is performed after Ethernet Filtering. Any packets discarded by Ethernet filtering will not reach IP filtering.

Please note that IP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

IP filtering is performed after Ethernet Filtering. Any packets discarded by Ethernet filtering will not reach IP filtering.

UDP/TCP Address Filters Screen



UDP/TCP Address Filters Screen

There are two screens that apply to TCP and UDP packets. This discussion will use the UDP filter as an example.

UDP filters are used to limit the UDP packets sent from the local tunnel to a remote tunnel. This level of filtering is performed on the UDP Destination Port Number. It would typically be used to eliminate certain types of UDP broadcasts. For example, you may not want DHCP requests to cross between local and remote networks. In this case you would block UDP ports 67 and 68.

To use UDP filtering, you first select a default rule. That is, you choose to allow all UDP packets by default, or to drop all UDP packets by default.

Next, you enter one or more exceptions to the default rule. An exception consists of a range of destination port numbers. Any UDP packet with a destination port number in the specified range will be considered an exception, causing the opposite of the default rule to be performed.

Please note that UDP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

UDP filtering is performed after IP Filtering. Any packets discarded by IP filtering will not reach UDP filtering.

Fields

- Default Rule
  This field specifies the action to be taken when an UDP packet does not meet any of the exception rules.

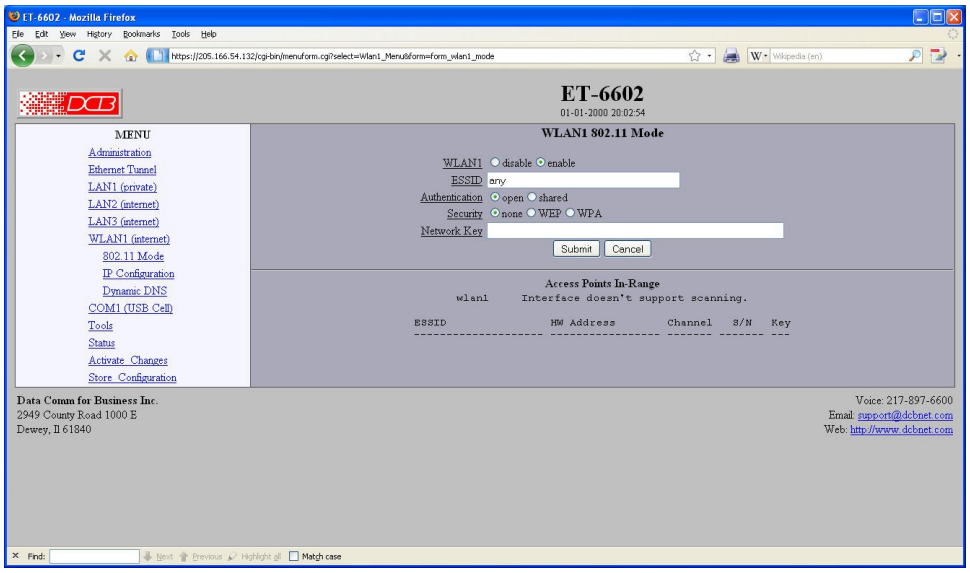
- Low Destination Port
  This field specifies the Low Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.
- High Destination Port
  This field specifies the High Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.

Notes

Please note that UDP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

UDP filtering is performed after IP Filtering. Any packets discarded by IP filtering will not reach UDP filtering.

WLAN 1 802.11 Configuration



WLAN 1 802.11 Configuration Screen

An Alias IP Address can be used to ease setup of an Ethernet to Wireless adapter. When using an adapter, you often run into a problem where you need Ethernet-B to acquire a DHCP address, but to do so, you must access the wireless adapter to select the wireless network. However, you are unable to access the wireless adapter because Ethernet-B does not have an address. To solve this problem, you can assign Ethernet-B an alias IP address, and assign the wireless adapter an address on the same subnet. This is useful when the ET is used along with a wireless broadband connection, such as from a hotel room.

Fields

- WLAN 1
  Enable/Disable the internal 802.11 interface.
- ESSID
  The ESSID selects the name of the network in which to join. The special string ***any*** may be used, in which case the 802.11 interface will join any available network with compatible authentication and security modes. Please note that *any* may not be used with WPA security.
- Authentication
  In *open* mode, no authentication is used and the 802.11 interface will accept encrypted and non-encrypted connections. In *shared* mode only encrypted connections are allowed. This configuration item only applies to WEP security.
- Security
  This field selects the security mechanism. Choose between *none*, *WEP*, and *WPA*. If WEP or WPA is selected, a network key must also be set.

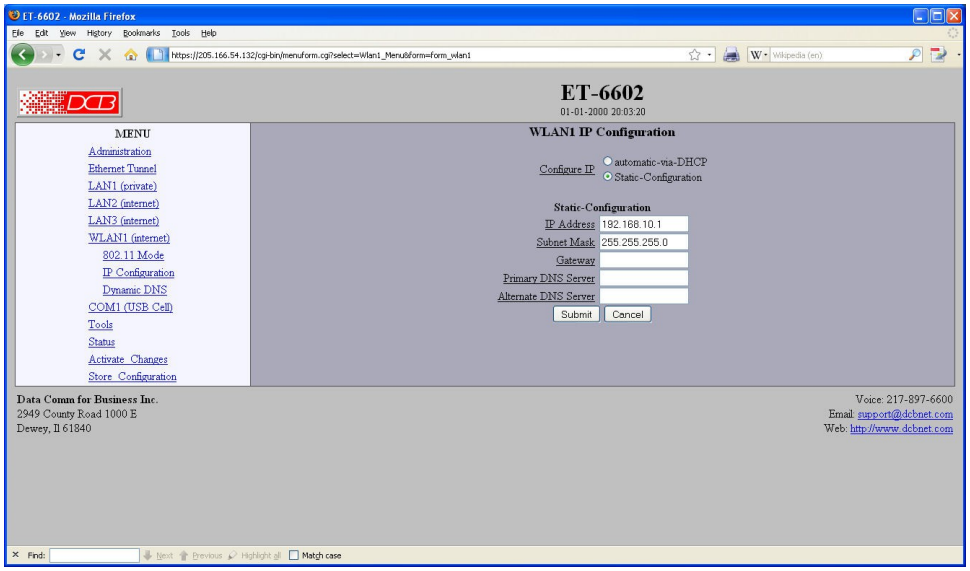
- Network Key
  This field sets the network key. The format of the key is dependent upon the security mechanism.

  WEP Security: The key is usually entered as a series of hexadecimal numbers (0-9, A-F) with an optional '-' character separating each group of 4 characters. For example, a key may be entered as 1234-5678-9A or 123456789A. Optionally the key may be entered as an ASCII character string. To do so, the key must be preceeded with "s:". The key is then generated from the ASCII string by converting each character to its ASCII value. For example, the key s:12345 would be converted to the hexadecimal key 3132-3334-35.

  WPA Security: The key is entered as a passphrase consisting of 8 to 63 characters.

Notes:

WLAN 1 IP Configuration



WLAN 1 IP Configuration Screen

The ET contains multiple Ethernet interfaces. WLAN 1 is normally used for the WAN untrusted connection. This screen is used to configure IP parameters for WLAN 1.

Fields

- Configure IP
  Select DHCP or a static configuration. If DHCP is selected, the static-configuration is ignored.

- IP Address
  An IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. If you are directly connected to the Internet, it must

globally unique.
This field is not used if DHCP Client has been enabled. The DHCP server will assign the IP address.

- Subnet Mask
  A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, many subnets have a mask of 255.255.255.0. This means the first 24 bits of the address is the subnet identifier and the last 8 bits is the host identifier.

  This field is not used if DHCP Client has been enabled. The subnet mask will be assigned by the DHCP server.

- Gateway

  The Gateway specifies the address of the gateway router on the local subnet. Packets destined for a host not on the local subnet are forwarded to the gateway router.

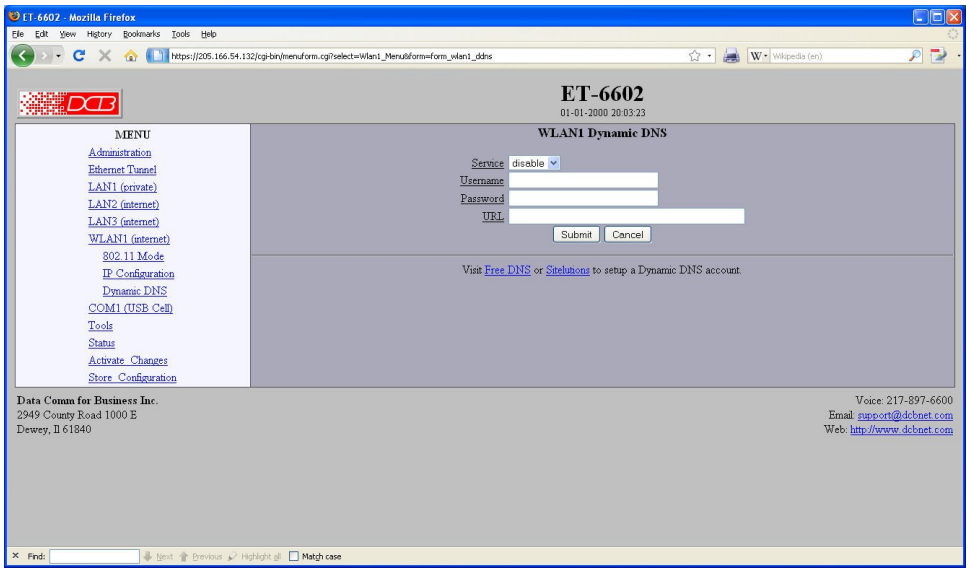
  The tunnel uses policy-based routing rules which allow each interface to have a gateway router defined. Routing decisions take into account the source IP address when selecting a gateway. Instances where a source address has not been established, such as when initiating a connection, ping, etc, the tunnel will give priority to Ethernet-B's gateway.

- Primary DNS
  The IP address of the primary DNS server. This server will be used to resolve host names into ip addresses.

  Note: The DNS servers are common for all interfaces. If any of the interfaces are configured to use DHCP, the DNS servers assigned by the DHCP server will take precedence.

- Secondary DNS
  The IP address of the secondary DNS server. This server will be used to resolve host names into ip addresses in the event that the primary name server does not respond or is unable to resolve an name.

WLAN 1 Dynamic DNS Configuration



WLAN 1 Dynamic DNS Configuration Screen

A Dynamic DNS service allows you to associate a dynamically assigned IP address to a hostname and domain. This is achieved by having the device contact the Dynamic DNS service after it has been assigned an IP address. By contacting the Dynamic DNS service, the service is able to detect the device's IP address and will create DNS record for that device.

In order to use Dynamic DNS, you must first setup an account with a Dynamic DNS service provider. We have tested with the service provided by FreeDNS and Sitelutions. However, any URL based service using HTTP Get should work.

The unit will perform a HTTP Get each time a interface is enabled and/or each time the IP address changes.

Fields

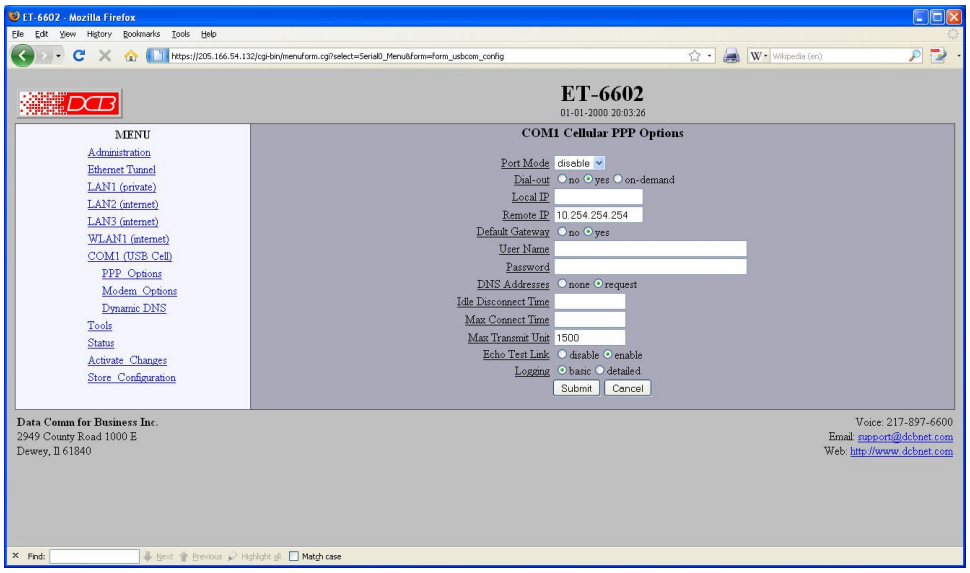
- **Service**
  Enable/Disable Dynamic DNS support for the associated interface.
- **Username**
  Optional username for Dynamic DNS servers that require HTTP basic authentication.
- **Passsword**
  Optional password for Dynamic DNS servers that require HTTP basic authentication.
- **URL**
  HTTP url to access when the associated interface is enabled. The url must be in the form of:
  http://www.somewebsite.com/subdirectory?optionalparms
  If the service uses a port number other than 80, you may append the port number following the hostname. For example:
  http://www.somewebsite.com:8000/subdirectory?optionalparms.
  If your service requires you to send your IP address in the URL, insert the string **{IP}**, in the position that the IP address is required. For example:
  http://www.somewebsite.com/subdirectory?IP={IP}
  Https (SSL) is not supported.

Notes

FreeDNS Configuration Notes:
After creating an account and hostname with FreeDNS simply cut and paste the **Direct_URL** assigned by FreeDNS into the URL field. You do not need to set the username or password fields. The URL should look similar to this:
http://freedns.afraid.org/dynamic/update.php?ABCDEFGabcdefg1234567hijkHIJLlmnopU2

Sitelutions Configuration Notes:
You must first setup an account with Sitelutions then create a DNS record for your host. When you do this, Sitelutions will assign a Dynamic DNS record ID to this entry. The Sitelutions URL to update your DNS record has your email account, password, DNS record ID, and IP address appended as paramters. The URL should look similar to this:
http://www.sitelutions.com/dnsup?user=me@email.com&pass=password&id=1234567&ip={IP}

COM1 Cellular PPP Configuration



COM1 USB(Cellular) PPP Configuration Screen

There may be one USB cellular modem connected to the ET. These screens configure that modem connection.

Fields

- Port Mode
  Sets the operating mode of the port. PPP mode enables the port for PPP operation. The port should be disabled if it is not being used. This will free up system resources.

- Dial-Out
  When set to yes, the tunnel will immediately try to establish a PPP session by dialing the phone.

  When set to on-demand, the tunnel will create a pseudo PPP session and wait for outbound traffic. When traffic is detected, it will attempt to dial-out and establish a real PPP session.

  Note: When *on-demand* is selected, you usually will need to set *default gw* to yes.

- Local IP
  Each side of a PPP connection must have an IP address. This is the IP address to use for the local PPP device. You can leave this field blank, but the remote PPP device must be configured to assign an address.

  If you leave this field blank when *Dial-out on-demand* is enabled, the tunnel will temporarily assign a local address to the interface. When the actual PPP connection is brought up, the tunnel will request a new address from the peer.

- Remote IP
  Each side of a PPP connection must have an IP address. This is the IP address to assign to the remote PPP device. You can leave this field blank, but the remote PPP device must be configured with a Local IP address.

- Default Gateway
  Each side of a PPP connection must have an IP address. This is the IP address to assign to the remote

PPP device. You can leave this field blank, but the remote PPP device must be configured with a Local IP address.

- User Name
  This is the user-name sent to the remote system for authentication. This field is optional. If the remote system does not require authentication, you may leave this field blank. The user-name may be a string of 1 to 15 printable characters. No space or control characters.

  Note: The username field is not typically used for wireless broadband (cellular) service. The authentication credentials are usually pre-programmed into the modem.

- Password
  This is the password sent to the remote system for authentication. This field is optional. If the remote system does not require authentication, you may leave this field blank. The password may be a string of 1 to 15 printable characters. No space or control characters.

  The password field is not typically used for wireless broadband (cellular) service. The authentication credentials are usually pre-programmed into the modem.

- DNS Address
  When set to *request*, DNS server addresses will be requested during PPP option negotiation.
  Note: Typically you would select *request* if you are dialing into an ISP.

- Idle Disconnect
  If there is no IP traffic across the PPP link for this amount of time (in minutes), the link will be terminated.

- Max Connect Time
  This is the maximum amount of time (in minutes) to allow a PPP connection to exist. The link will be taken down regardless of activity.

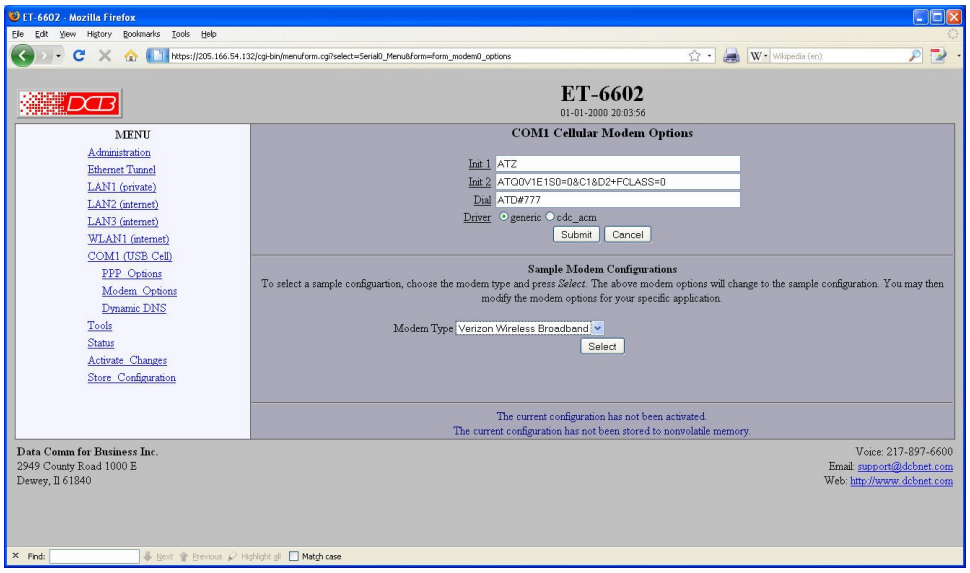
- Max Transmit Unit
  This selects the maximum transmit unit and maximum receive unit for the interface. Outgoing network packets will be limited to the specified size. The peer will be asked to limit its MTU to this size. The peer may negotiate a smaller size. The value may be between 128 to 1500.

- Echo Test Link
  When enabled, an LCP level echo request will be sent periodically (30 seconds) to the peer. If the peer fails to respond to 4 consecutive requests (2 minutes), the link will be taken down and reestablished.

- Logging
  This selects the level of information placed in the serial log files.

Notes:

COM 1 Cellular Modem Configuration



COM1 Cellular Modem Options Configuration Screen

When configuring the modem, there are several items you should consider in order for the tunnel to correctly inter-operate with it.

- The tunnel monitors Data Carrier Detect (DCD) to bring up and take down PPP sessions The modem should assert (DCD) when a connection is established and drop DCD when a connection is lost.
- The tunnel will assert DTR when it is ready to establish a PPP session and will drop DTR when a PPP session is terminating. The modem should hang up the phone if DTR is inactive. Likewise it should not answer an incoming call if DTR is inactive.
- Do not suppress the "OK" message. The tunnel looks for this message to determine when commands have been accepted.
- Suppress echo.
- The tunnel will look for the messages "BUSY", "NO CARRIER", "CARRIER", "NO DIALTONE", and "NO ANSWER" when dialing a connection. You should not suppress result messages

Fields

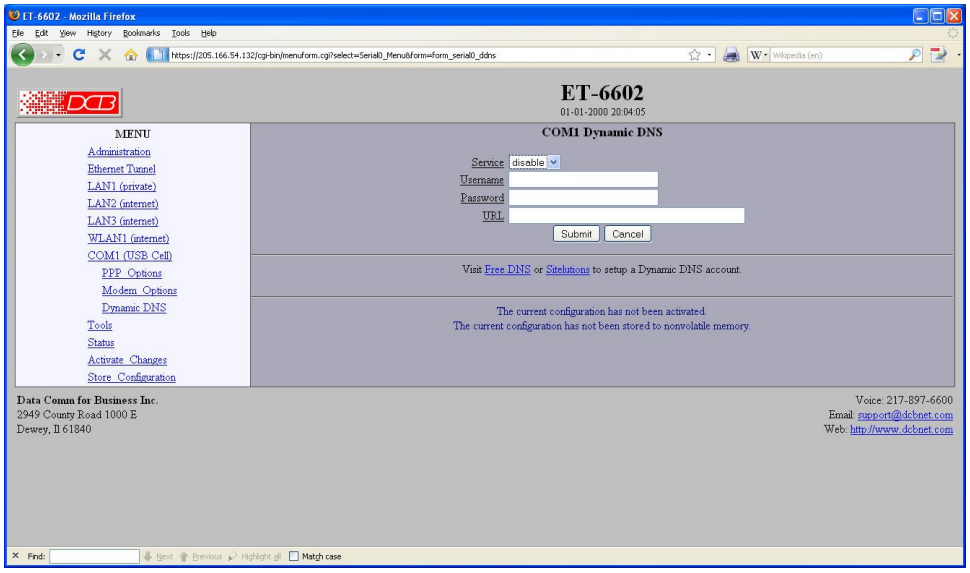
- Init 1
  The tunnel will send this command prior to starting each PPP connection. You should use it to put the modem into a known state. For DCB's D-Series modem, you should use the string: "AT&FE0V1&C1&D2&K3N1X4"
- Init 2
  The tunnel will send this command after sending the first initialization command and receiving an "OK" response. This is to allow for additional configuration or to allow for modems that can not be reset and configured with a single command string.
- Dial
  This command will be used when the tunnel needs to dial-out. It will be concatenated with the phone

number specified in the PPP options. For most modems, the command is "ATDT" to do touch-tone dialing and "ATDP" to do pulse-code dialing.

- Driver
  This option is a work-around for USB modems that require the Communication Device Class - Abstract Control Model (CDC_ACM) driver. Probing for a CDC_ACM modem, when it is not present, will indefinitely hang the driver, requiring a system restart to recover. If you are using a modem that requires this driver, please make sure to install the modem before powering up the system, and do not attempt to remove and reinstall it hot.

  If you are unsure which driver to use, always try the generic driver option first. It covers the most common USB wireless modems.

COM 1 Dynamic DNS Configuration



Com 1 Dynamic DNS Configuration Screen

A Dynamic DNS service allows you to associate a dynamically assigned IP address to a host name and domain. This is achieved by having the device contact the Dynamic DNS service after it has been assigned an IP address. By contacting the Dynamic DNS service, the service is able to detect the device's IP address and will create DNS record for that device.

In order to use Dynamic DNS, you must first setup an account with a Dynamic DNS service provider. We have tested with the service provided by FreeDNS and Sitelutions. However, any URL based service using HTTP Get should work.

The unit will perform a HTTP Get each time a interface is enabled and/or each time the IP address changes.

Fields

- **Service**
  Enable/Disable Dynamic DNS support for the associated interface.
- **Username**
  Optional username for Dynamic DNS servers that require HTTP basic authentication.

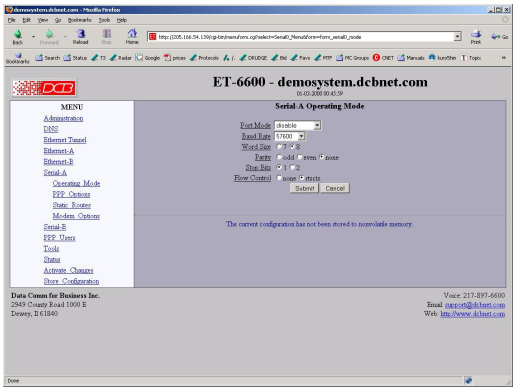
- **Passsword**
  Optional password for Dynamic DNS servers that require HTTP basic authentication.
- **URL**
  HTTP url to access when the associated interface is enabled. The url must be in the form of:
  http://www.somewebsite.com/subdirectory?optionalparms
  If the service uses a port number other than 80, you may append the port number following the hostname. For example:
  http://www.somewebsite.com:8000/subdirectory?optionalparms.
  If your service requires you to send your IP address in the URL, insert the string **{IP}**, in the position that the IP address is required. For example:
  http://www.somewebsite.com/subdirectory?IP={IP}
  Https (SSL) is not supported.

Notes

FreeDNS Configuration Notes:
After creating an account and hostname with FreeDNS simply cut and paste the **Direct_URL** assigned by FreeDNS into the URL field. You do not need to set the username or password fields. The URL should look similar to this:
http://freedns.afraid.org/dynamic/update.php?ABCDEFGabcdefg1234567hijkHIJLlmnopU2

Sitelutions Configuration Notes:
You must first setup an account with Sitelutions then create a DNS record for your host. When you do this, Sitelutions will assign a Dynamic DNS record ID to this entry. The Sitelutions URL to update your DNS record has your email account, password, DNS record ID, and IP address appended as paramters. The URL should look similar to this:
http://www.sitelutions.com/dnsup?user=me@email.com&pass=password&id=1234567&ip={IP}

Serial A/B Operating Mode Screen



Serial Port Operating Mode Screen

This form sets the operating mode and parameters for the serial ports on the ET-6600.

Fields

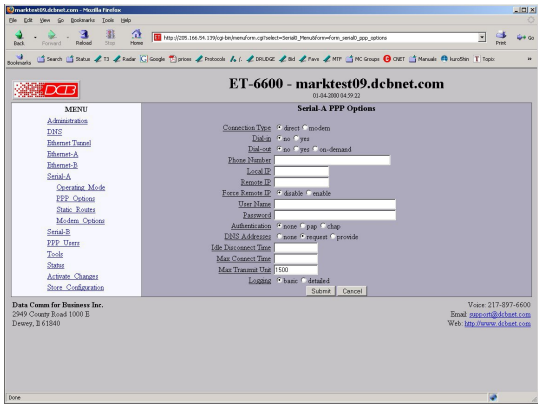
Mode
Sets the operating mode of the port. Currently PPP is the only mode supported. The port should be disabled if it is not being used. This will free up system resources.

- Baud Rate
  Serial port Baud rate.
- Word Size
  Number of data bits in each character. For PPP, this field is ignored and the number of bits is set to 8.
- Parity
  Enable parity generation and testing.
- Stop Bits
  Select 1 or 2. The ET serial interfaces do not support 1.5 stop bits.
- Flow Control
  Hardware flow control enable. The ET-6600 and ET-6690 use the RTS and CTS signals for hardware flow control. RTS is an output from the ET. It will be asserted when the ET is ready to receive data and de-asserted when the ET is not ready to receive data. CTS is an input to the ET. The ET will monitor CTS and will only transmit data when CTS is asserted.

Notes

- Serial ports should be disabled if not being used to free up system resources.
- If configuring PPP parameters while using the PPP link, the link will be dropped when the parameters are activated.

Serial A/B PPP Options Screen



Serial Port PPP Options Screen

This form is used to configure the PPP options for the serial interface on the ET-6600.

Fields

- This option effectively enables and disables the modem dialing options
  When set to direct, the ET assumes a hard-wired connection and directly attempts to establish a PPP connection. Modem related options are ignored.
- Dial-IN
  When set to yes, the modem is configured to answer incoming calls. The PPP session will be

established when the serial ports DCD (data carrier detect) signal goes active.
This feature may be used in conjunction with dial-out on-demand. YES.

- Dial-OUT
  When set to yes, the ET will immediately try to establish a PPP session by dialing the phone.
  When set to on-demand, the ET will create a pseudo PPP session and wait for outbound traffic. When traffic is detected, it will attempt to dial-out and establish a real PPP session.

  Note: When on-demand is selected, you must set Local IP and Remote IP addresses. You also need to set at least one entry in Static Routes for the remote network. This is the information needed by the ET to determine outbound traffic.

- Phone Number
  This is the phone number to use when making a dial-out call. This field is not only limited to phone numbers. If necessary, you may embed modem commands. This field is simply appended to the Modem Options - Dial field when making an outgoing call.

- Local IP
  Each side of a PPP connection must have an IP address. This is the IP address to use for the local PPP device. You can leave this field blank, but the remote PPP device must be configured to assign an address.

  With the ET serial ports, it is possible to borrow the IP address of one of the Ethernet interfaces for the Local IP address. However, this is a questionable practice as it might expose the web configuration screens to the public interface.

- When Dial-out on-demand is enabled, you must specify a Local IP. This may pose a problem when dialing an ISP that dynamically assigns the local address. To get around it, set the Local IP address to the address of one of the Ethernet interfaces. The ET-6600 will switch to the server assigned PPP address when the connection is established.

- Remote IP
  Each side of a PPP connection must have an IP address. This is the IP address to assign to the remote PPP device. You can leave this field blank, but the remote PPP device must be configured with a Local IP address.

  When Dial-out on-demand is enabled, you must specify a Remote IP. This may pose a problem when dialing an ISP where you don't know what the address of the remote device will be. In reality, you don't have to know the exact address. Something close will do. Choose the address of a device on the remote network such as a next-hop bridge, DNS server, or mail server. When the real PPP connection is established, the ET will switch to the server's real IP address.

- Force Remote IP
  When this option is enabled, the peer will be forced to use the Remote IP address, overriding the peer's configuration. If it refuses, the connection will be terminated. When this option is disabled, the peer's IP address will be used, if it has been configured with one. You would typically enable this if the tunnel is being used as a dial-in server.

- UserName
  This is the user-name to use when authenticating to a remote system. In other words, this is the user-name sent to the remote system. This field is optional. If the remote system does not require authentication, you may leave this field blank. The user-name may be a string of 1 to 15 printable characters. No space or control characters.

- Password
  This is the password to use when authenticating to the remote system. In other words, this is the password sent to the remote system. This field is optional. If the remote system does not require

authentication, you may leave this field blank. The password may be a string of 1 to 15 printable characters. No space or control characters.

- Authentication
  When set to pap or chap the remote system must provide a user-name and password in order to connect to the local system. The list of valid user-names and passwords are entered in the PPP Users table. When pap is selected, the remote system must use the Password Authentication Protocol (PAP).

  When chap is selected, the remote system must use the Challenge Handshake Authentication Protocol (CHAP). This includes MSCHAP V1 and V2

  Note: CHAP is considered the better of the two authentication methods.

- DNS Addresses

  When set to request, the local tunnel will request DNS addresses from the remote tunnel during PPP option negotiation. When set to provide, the local tunnel will provide DNS addresses to the remote tunnel during PPP option negotiation.

  Note: Typically you would select request if you are dialing into an ISP. You would select provide if you are using the tunnel as a dial-in server.

Idle Disconnect Time
: If there is no IP traffic across the PPP link for this amount of time (in minutes), the link will be terminated.

Max Connect Time
: This is the maximum amount of time (in minutes) to allow a PPP connection to exist. The link will be taken down regardless of activity.

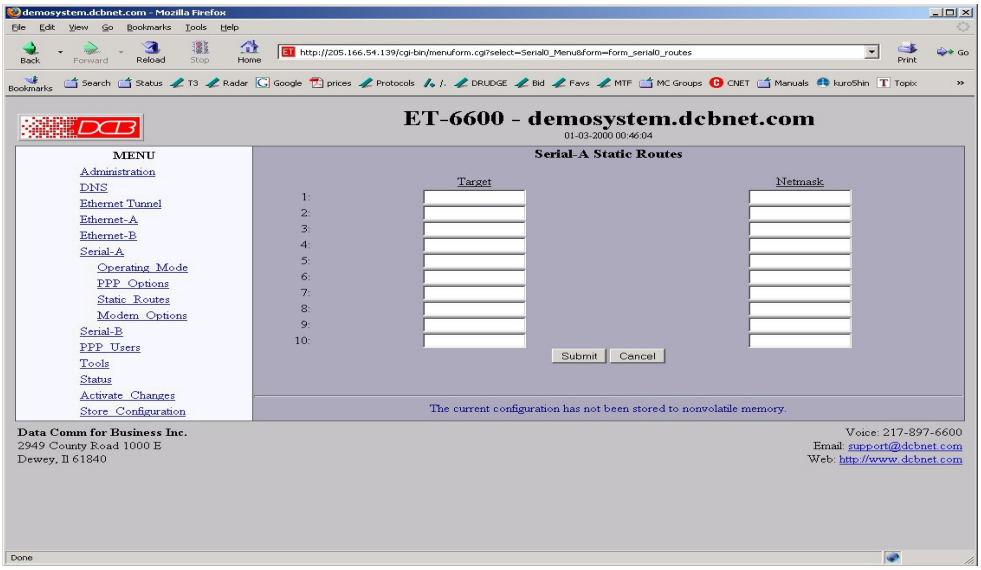
MTU
: This selects the maximum transmit unit and maximum receive unit for the interface. Outgoing network packets will be limited to the specified size. The peer will be asked to limit its MTU to this size. The peer may negotiate a smaller size. The value may be between 128 and 1500.

Logging
: This selects the level of information placed in the serial log file. Options are BASIC and DETAILED.

Notes

- Serial ports should be disabled if not being used to free up system resources.
- If configuring PPP parameters while using the PPP link, the link will be dropped when the parameters are activated.

Serial A/B Static Routes Screen



Serial Port Static Routes Screen

The tunnel maintains four tables of Static Routes. There is one for each possible interface, namely Ethernet-A, Ethernet-B, Serial-A, and Serial-B. The routes defined in the associated table are applied when an interface comes up and are removed when an interface goes down. It is important that routes be placed in the correct table. The rule-of-thumb is to apply a route to the interface that the routed packet should go out. For example, if you want your default route to go out the PPP link on Serial-A, you would add the default routing entry to Serial-A's static routing table. If you want packets to address 192.168.10.54 to go out Ethernet-A, you would add a routing entry to Ethernet-A's table.

The tunnel will automatically create a route for each interface. For Ethernet, this will be a network entry based on the IP address and netmask of the interface. For PPP links, this will be a host entry for the IP address of the remote PPP device.

You can view that Active Routing Table from the Status Menu/Routing Table. This use of the serial ports is specific to the ET-6600 model.

Fields

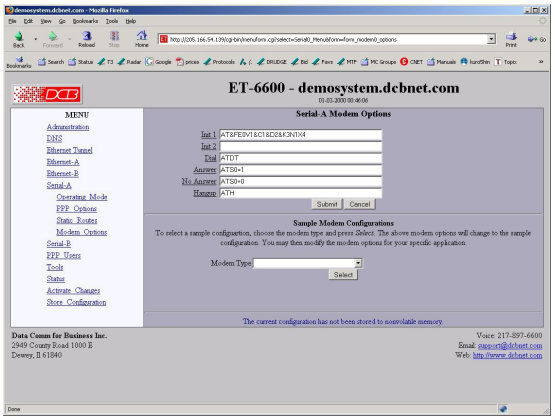
- Target
  Destination Host or Network address. Use a target address of 0.0.0.0 to specify a default route.
- Netmask
  If left blank or set to 255.255.255.255, the target is assumed to be a host address. Otherwise, the target is assumed to be a network address and the netmask specifies which address bits are significant. Use a netmask of 0.0.0.0 to specify a default route.

Notes

- The ET will automatically create a route for each interface. For Ethernet, this will be a network entry based on the IP address and netmask of the interface. For PPP links, this will be a host entry for the IP address of the remote PPP device.
- You can view that Active Routing Table from the Status Menu/Routing Table.

- There is no gateway field as all routes terminate at the other end of the serial link.
- The Port Forwarding screen is identical to the Ethernet Port Forwarding screen. See that section for details.
- This use of the serial ports is specific to the ET-6600 model.

Serial A/B Modem Options Screen



Serial Port Modem Options Screen

The Modem Options are used when the PPP Connect Type has been set to modem. They specify the various commands to send to the modem, depending on the selected PPP options.

When configuring your modem, there are several items you should consider in order for the tunnel to correctly inter-operate with it.

* The tunnel monitors Data Carrier Detect (DCD) to bring up and take down PPP sessions The modem should assert (DCD) when a connection is established and drop DCD when a connection is lost.

* The tunnel will assert DTR when it is ready to establish a PPP session and will drop DTR when a PPP session is terminating. The modem should hang up the phone if DTR is inactive. Likewise it should not answer an incoming call if DTR is inactive.

* Do not suppress the "OK" message. The tunnel looks for this message to determine when commands have been accepted.

* Suppress echo.

* The tunnel will look for the messages "BUSY", "NO CARRIER", "CARRIER", "NO DIALTONE", and "NO ANSWER" when dialing a connection. You should not suppress result messages.

Fields

Init 1
The ET-6600 will send this command prior to starting each PPP connection. You should use it to put the modem into a known state. For DCB's D-Series modem, you should use the string: "AT&FE0V1&C1&D2&K3N1X4"

Init 2
The ET will send this command after sending the first initialization command and receiving an "OK" response. This is to allow for additional configuration or to allow for modems that can not be reset and configured with a single command string.

Dial
This command will be used when the ET needs to dial-out. It will be concatenated with the phone number

specified in the PPP options. For most modems, the command is "ATDT" to do touch-tone dialing and "ATDP" to do pulse-code dialing.

Answer
This command will be used when the ET needs to enable auto-answer mode. For most modems, the command is "ATS0=1", where the 1 specifies how many rings to wait for before answering.

No Answer
This command will be used when the ET needs to disable auto-answer mode. For most modems, the command is "ATS0=0".

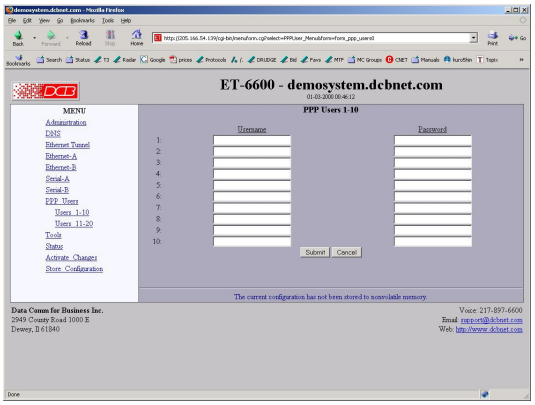
Hangup
This is the command used to hang-up the connection. For most modem, the command is "ATH". The ET will initially use the DTR signal to hang-up a connection. However, if the modem does not drop the DCD signal, the ET-6600 will issue "+++" wait for an "OK" response, then send this command.

Sample Modem Configurations
There are several sample configurations for DCB and other brand modems. When one of these is selected, the default values above are set correctly for the modem type selected.

Notes

The ET will look for the messages "BUSY", "NO CARRIER", "CARRIER", "NO DIALTONE", and "NO ANSWER" when dialing a connection. You should not suppress result messages

PPP Users Screen



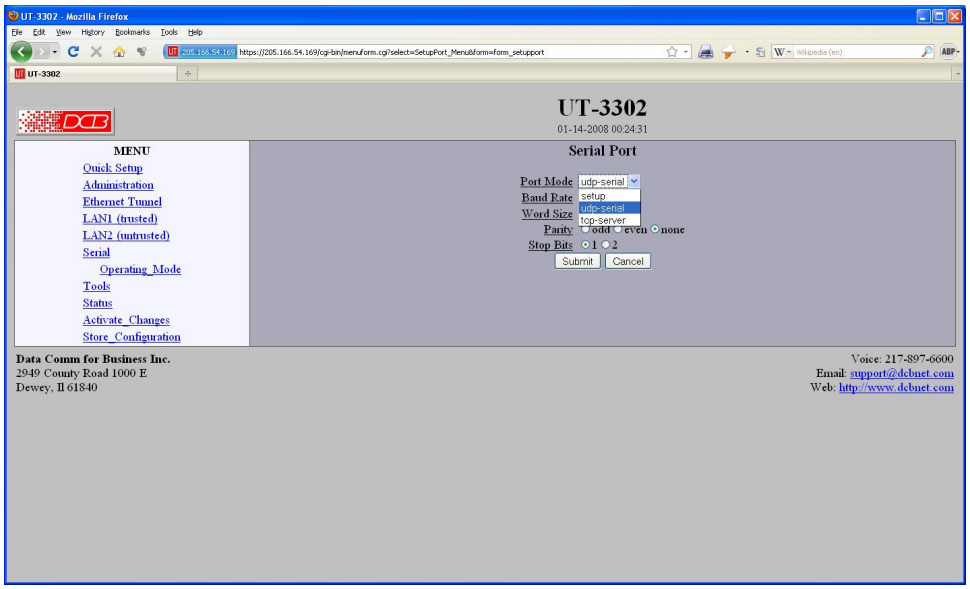
PPP Users Screen

This table specifies the usernames and password for remote PPP users. It will be used when either PAP or CHAP authentication is enabled.

Fields

- Username
  A string of 0 to 15 printable characters. Do not use space or control characters. Ignored if blank..
- Password
  A string of 0 to 15 printable characters. Do not use space or control characters. Ignored if blank.

Serial Port functionality Screen



Serial Functionality Screen

This form sets the operating mode for the DE-9 serial port. The port is labeled setup and is typically used for initial configuration in setup mode. However, it may be configured in UDP Serial Mode or TCP Server Mode. In UDP Serial Mode the unit will listen for UDP datagrams on the specified UDP port. When received, the payload of the datagram will be sent out the serial port. Likewise, data received on the serial port will be placed in a UDP datagram and send to all of the specified remote destinations. In TCP Server mode, a TCP client can connect to the server and stream data to/from the serial port. This functionality is only available on the ET-3302 model.

Note: Hardware and Software flow control are not implemented.

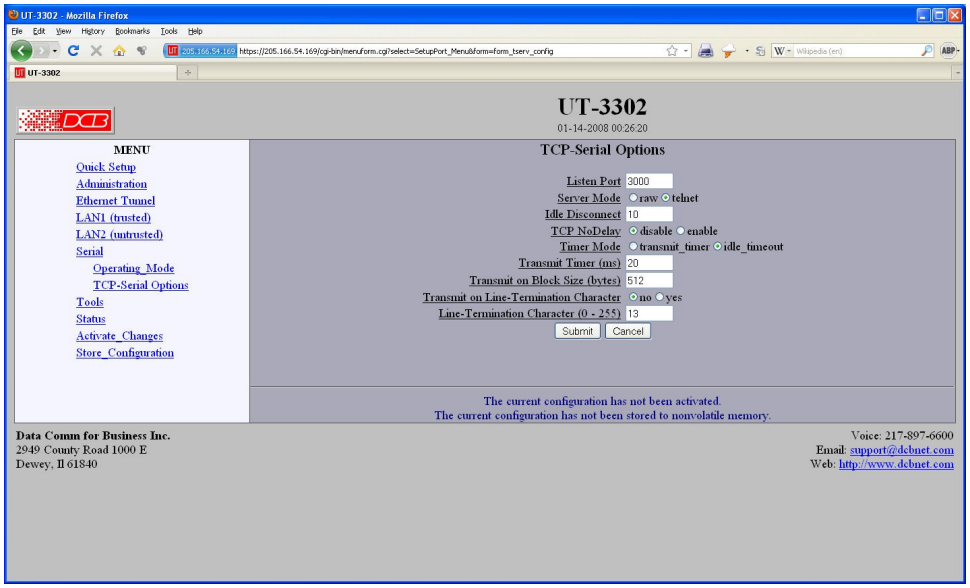
Fields

- Port Mode
  Sets the operating mode of the port as a setup port, UDP serial server, or TCP serial server.
- Baud Rate
  Serial port Baud rate.
- Size
  Number of data bits in each character. Ignored in setup mode.
- Parity
  Enable parity generation and testing. Ignored in setup mode.
- Stop Bits
  Select between 1 or 2 stop bits. Ignored in setup mode.

Notes

- See the EtherPath or EtherPoll product manuals for more details on the serial port functionality and compatibility with those products.

TCP Serial Options Screen



TCP Serial Options Screen

This form sconfigures the TCP serial mode options for the DE-9 serial port. The port is labeled setup and is typically used for initial configuration. However, it may be configured in UDP Serial Mode or TCP Server Mode. In TCP Server mode, a TCP client can connect to the server and stream data to/from the serial port. This functionality is only available on the ET-3302 model.

Fields

- Listen Port
  TCP Port number transmitted from and listening to. Default is port 3000

- Server Mode
  The TCP server can operate in either raw or telnet mode. In raw mode, all data is passed transparently between the serial port and the TCP connection. In telnet mode, telnet command processing will occur and telnet escaping rules will be followed.

- Transmit Timer [1ms to 10,000ms]
  When in Timer Mode: The time period for which data will be
  stored in the buffer before being sent. Allowable values range from 1ms to 10,000ms (10 seconds). A commonly used value is 20 msec.
  When in Idle Timeout Mode: The time period this unit's port must be idle (after receiving a character) before sending a block of data via the Ethenet. This is used to keep incoming blocks of data intact. It is useful for some protocols such as Modbus RTU. Its setting depends upon the port speed, and should be several character times. Allowable values range from 1ms to 10,000msec (10 seconds). A typical value for a 9.6 Kbps port is about 3 msec.

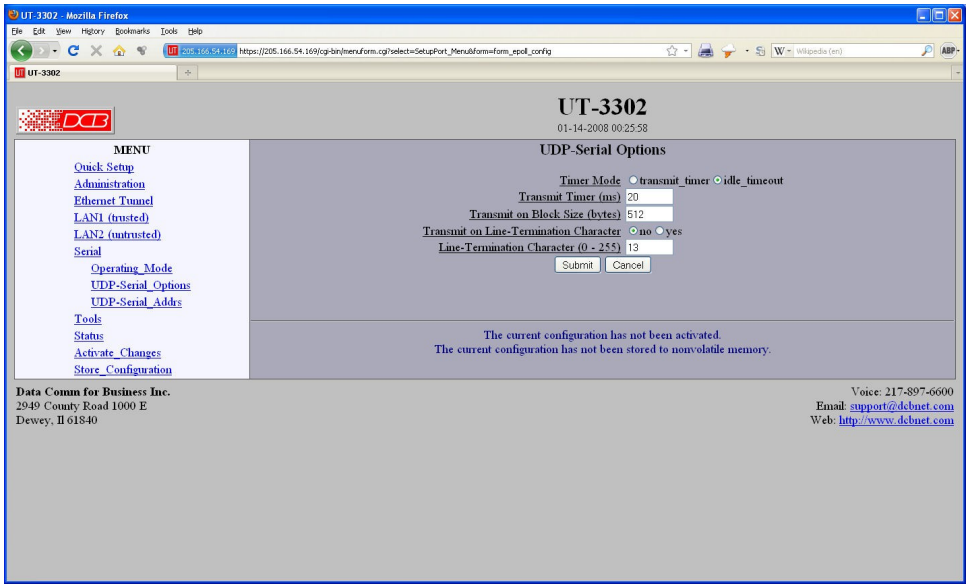
- Timer Mode
  When set to Timer, the timer is a free-running clock and if there is data in the buffer, an IP packet is transmitted every TIMER msec.
  When set to Idle Timeout, the timer is a serial port idle time value. If there is data in the buffer and the serial port has been idle for TIMER msec, then an IP packet is transmitted.

- Idle Disconnect
  This field sets the time, in minutes, where the TCP connection will be terminated if no data is exchanged with the client. A value of 0 disables the timer.
- TCP No Delay
  his option controls Nagle's algorithm. When TCP No-Delay is enabled, Nagle's algorithm is disabled, allowing small packets to be streamed without waiting for the ACK. Enabling TCP No-Delay can have a negative effect on network congestion, but will improve delivery of real-time data.
- Transmit on Block Size
  This field sets the serial input buffer threshold level. If the number of bytes in the serial input buffer reaches this level, it will push the data to the network, even if the Transmit Timer has not expired.
- Transmit on Line Termination Character
  Enable/disable Transmit on Line-Termination character. As serial data is received, it is scanned for a Line-Termination character. If one is detected, it will push the serial data to the network even if the Transmit Timer has not expired.
- Line Termination Character
  This field sets the Line-Termination Character. It is entered as the decimal value of the character (0 - 255).

Notes

- See the EtherPath or EtherPoll product manuals for more details on the serial port functionality.
- Hardware and Software flow control are not implemented.

UDP Serial Options Screen



UDP Serial Options Screen

This screen is used to configure details when using the UDP Server serial mode. This functionality is only available on the ET-3302 model.

Note: Hardware and Software flow control are not implemented.

Fields

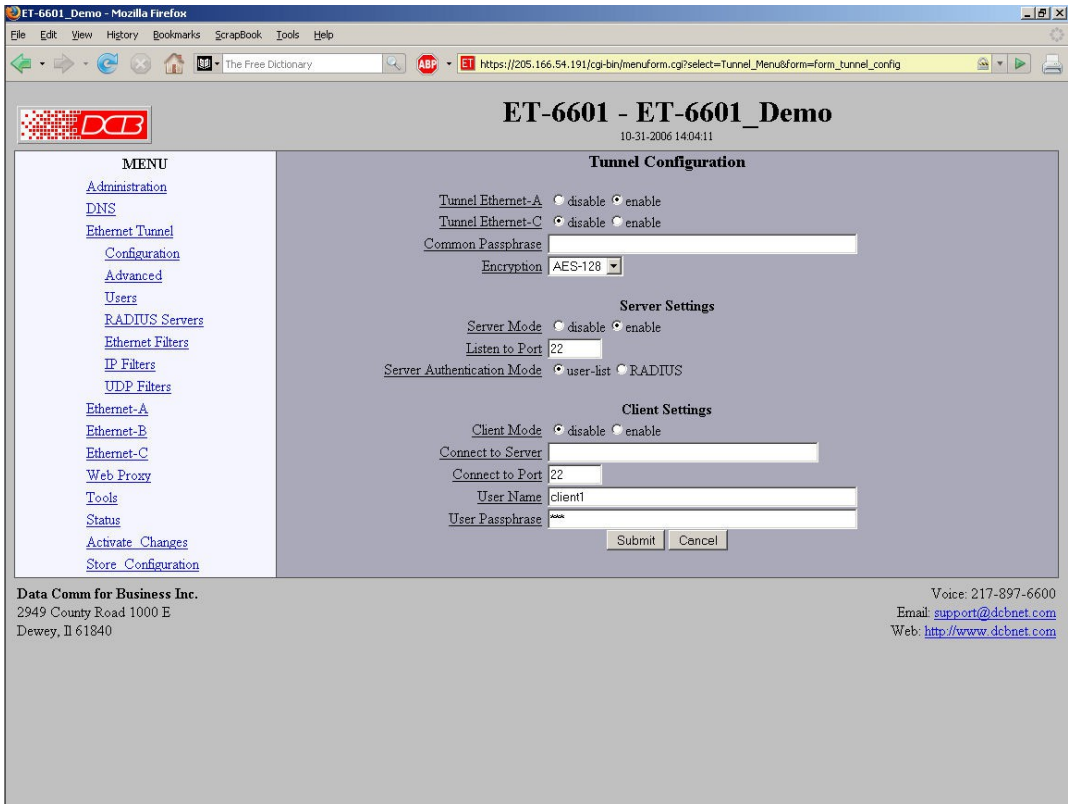
- Timer Mode
  When set to Timer, the timer is a free-running clock and if there is data in the buffer, an IP packet is transmitted every TIMER msec.
- Transmit Timer Allowable values range from 1ms to 10,000msec (10 seconds). A typical value for a 9.6 Kbps port is about 3 msec for Idle Timeout and 20 msec for Timer Mode.
  When set to Idle Timeout, the timer is a serial port idle time value. If there is data in the buffer and the serial port has been idle for TIMER msec, then an IP packet is transmitted. Transmit Timer [1ms to 10,000ms]
  When in Timer Mode: The time period for which data will be
  stored in the buffer before being sent. Allowable values range from 1ms to 10,000ms (10 seconds). A commonly used value is 20 msec.
- Transmit on Block Size
  This field sets the serial input buffer threshold level. If the number of bytes in the serial input buffer reaches this level, it will push the data to the network, even if the Transmit Timer has not expired.
- Transmit on Line Termination Character
  Enable/disable Transmit on Line-Termination character. As serial data is received, it is scanned for a Line-Termination character. If one is detected, it will push the serial data to the network even if the Transmit Timer has not expired.

- Line Termination Character
  This field sets the Line-Termination Character. It is entered as the decimal value of the character (0 - 255).

Notes

- See the EtherPath or EtherPoll product manuals for more details on the serial port functionality.

Encrypted Tunnel Configuration



Tunnel Configuration Screen

Fields

Tunnel Ethernet A

This enables tunneling of the Ethernet-A interface. All packets on Ethernet-A will be analyzed and transmitted to remote units based on MAC addresses. Much like an Ethernet switch, the tunnel will learn the location of hosts and will only transmit packets to a remote unit when needed.

It is permissible to use the tunnel with this option disabled. You would do so when you need a central server to act as a relay between multiple clients but don't wish to tunnel the Ethernet at the central server.

Tunnel Ethernet C/D

Enable tunneling of the optional Ethernet interfaces. This only applies to ET devices that have more than 2 ethernet interfaces. This effectively causes the additional interfaces to function as switch ports on the Ethernet-A network segment. If used in this way, you should not enable the IP configuration for these interfaces.

Common Passphrase

The common passphrase provides the initial level of privacy. All tunnels participating in the private network must have the same common passphrase. This passphrase is used to generate the 128-bit AES key used to cypher the initial communications. The passphrase may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

Encryption
This options selects the encryption method for data passed between the tunnels. AES-128 selects AES with a 128-bit key. AES, also known as Rijndael, is a NIST approved encryption method. ISAAC selects a stream cipher based on the ISAAC pseudorandom number generator using a 1024-byte seed. ISAAC runs faster than AES. In theory ISAAC is a strong cipher, but it has not received the scrutiny that AES has received. Some products also use AES-192 and AES-256 bit or ISAAC encryption. None disables encryption.

Server Mode

This option enables the tunnel to act as a server listening to the specified port. It is permissible for a tunnel to be both a server and client.

Listen-to Port

The TCP/IP port to listen to when server mode is enabled.

Server Authorization Mode

This option enables the tunnel to either use it's own built in list of authorized users (and passwords), or to select RADIUS servers to authenticate remote tunnel users. (This feature is only available on high performance ET products.)

Client Mode

This option enables the tunnel to act as a client, connecting to the specified host and port. It is permissible for a tunnel to be both a client and server.

Connect-to Server

The hostname or IP address of the server tunnel. That is the address this client will connect to.

Connect-to Port

The TCP/IP port to connect to when client mode is enabled. The server must be listening on this port

User Name

The username may be up to 52 characters in length. Do not use a quote or backslash character in the phrase. If blank, this entry is ignored.

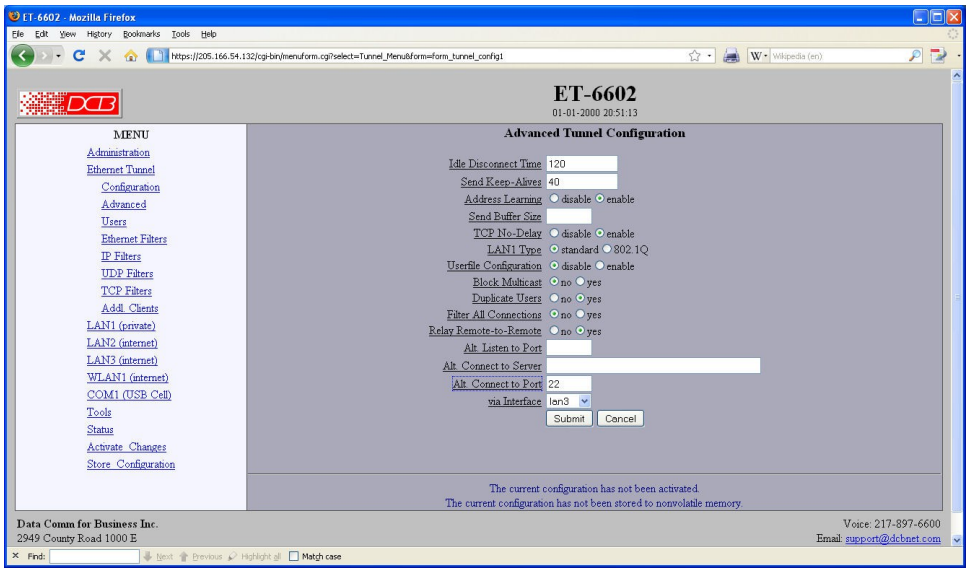
User Passphrase

The passphrase may be up to 52 characters in length. Do not use a quote or backslash character in the phrase. If blank, this entry is ignored.

Notes

The ET should never be used in actual applications without changing all passphrases. When used as a non-encrypting bridge, there is no security on the link between the ETs, and all traffic may be monitored by any node in the link, just as with any other bridge or router.

Advanced Tunnel Configuration



Advanced Tunnel Configuration Screen

Fields

Idle Disconnect Time
Setting a time enables an idle disconnect timer. If no packets are received from a remote tunnel for the specified amount of time, the TCP/IP connection with that remote tunnel is closed. Time is in seconds. If blank or set to zero, idle disconnect is disabled**.**

Send Keep-Alives
Setting a time enables a keep-alive feature. If the tunnel has not sent anything to the remote tunnel for the specified amount of time, a keep-alive message is sent. This feature is used to prevent an Idle Disconnect. Time is in seconds. If blank or set to zero, keep-alive is disabled.

Address Learning
Enable/disable Ethernet address learning. When enabled, the tunnel will learn the location of ethernet devices and only bridge packets when needed. When disabled, the tunnel will bridge all packets regardless of their location. For normal use, you should have learning enabled. However, for debugging purposes, you may wish to disable it. When disabled, you can use a packet sniffer, such as Ethereal, to view the Ethernet traffic at a remote location. To do so, you will have to disable learning at both the client and server units.

Send Buffer Size
This options allow you to control the amount of TCP buffering for outbound data to a remote tunnel. Valid range is 2048 to 16384 bytes. If blank, the system default of 16k is used. If you have a high speed connection, you should not need to set this. However, for a low speed connections you may need to reduce the buffer size to prevent a deep backlog of data which may cause some polling protocols to fail.

TCP No-Delay

his option controls Nagle's algorithm. When TCP No-Delay is enabled, Nagle's algorithm is disabled, allowing small packets to be streamed without waiting for the ACK. Enabling TCP No-Delay can have a negative effect on network congestion, but will improve delivery of real-time data. Default is enabled.

Ethernet-A Type

This option selects the Ethernet traffic type. The choice is standard Ethernet or 802.1Q VLAN tagged Ethernet. This essentially controls the MTU which is different between the two types of Ethernet.

Userfile Configuration

Userfile Configuration is an alternate method of configuring remote tunnel users. Instead of using the Users web pages, a comma delineated file is uploaded into the tunnel. Each line in the file represents one user. The first field is the username. The second field is the passphrase. Following the passphrase, you may specify 0 or more multicast channels. Because the file is comma delineated, you may not have a comma in the username or passphrase. Also, you may not use the quote or backslash character. The username and passphrase are case sensitive. Multicast channels are specified as an IP_address:port_number. An example userfile is shown below:

joe, joe's secret

bill, bill's passphrase, 224.0.55.1:5010

sally, only sally knows., 224.0.55.1:5010, 224.0.55.2:5000

Block Multicast

Setting this option to yes will cause the tunnel to block multicast traffic from being sent to the remote tunnels. Multicast traffic received from remote tunnels will still be output on the local LAN.

Note: With the use of the Userfile Configuration, you can override the blocking of multicast traffic on a user-by-user basis and direct one or more multicast channels to a remote tunnel.

Duplicate Users

This option only applies to the server tunnel. When set to no, the server will only allow one instance of a client, based on the client's username, to be connected.

Filter All Connections

Bridge filters (Ethernet, IP, UDP, and TCP) are normally applied only to the packets traveling in from the local Ethernet toward a remote tunnel. If this field is set to *yes*, filters will be also be applied to packets incoming on all tunnel connections.

Important note, setting this feature to yes will eliminate the ability to have a service enabled at one endpoint while blocking that service in the opposite direction. The service is effectively disabled in all directions.

Relay Remote-to-Remote

When set to *yes*, the local tunnel will relay packets between remote tunnels. When set to *no* the local tunnel will only bridge packets to/from the local LAN. If the bridges are configured as a mesh network, this should be set to no.

Alternate Listen-to Port

A secondary TCP/IP port to listen to when server mode is enabled. This is optional. When used, the client tunnels may be configured to use either server port.

Alternate Connect-to Server

The host name or IP address of an alternate server tunnel to connect to in the event that the client is unable to connect to the primary server.

Alternate Connect-to Port

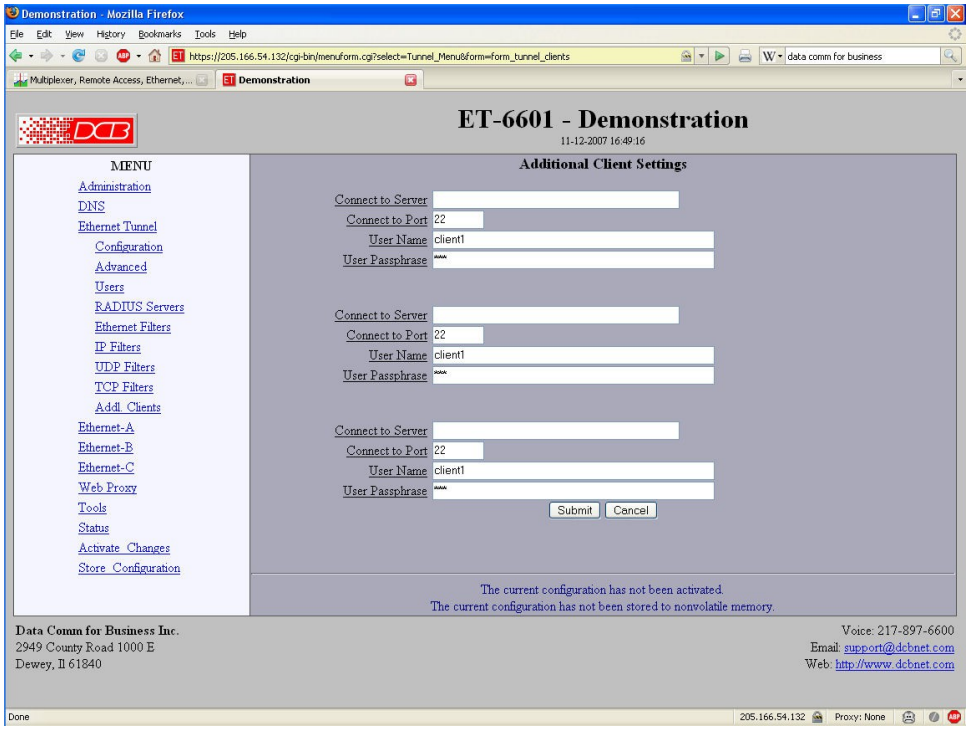
The TCP/IP port on the alternate server tunnel to connect to.

Via Interface

The ethernet interface the alternate server tunnel is to connected through.

Notes

Additional Clients



Additional Clients Configuration Screen

This screen allows you to enter up to three additional client configurations, making this unit a client for as many as four servers.

Fields

Connect-to Server
The hostname or IP address of the server tunnel.

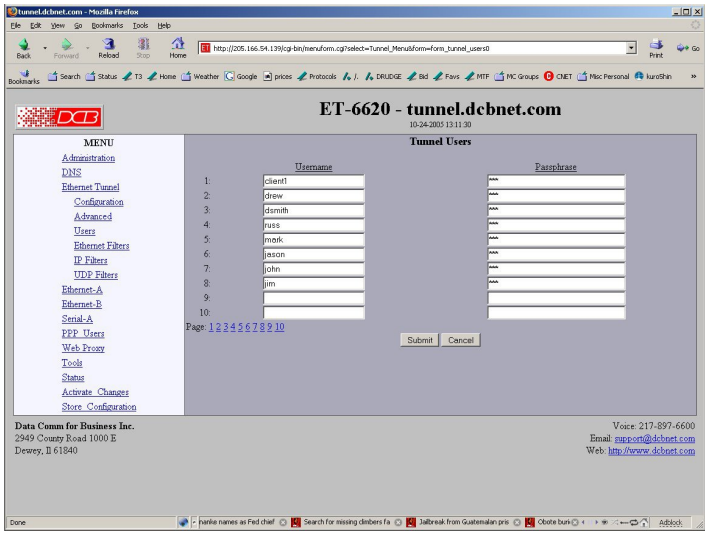
Connect-to Port
The TCP/IP port on the server tunnel to connect.

User name
This is the username to send to the server tunnel when authenticating. The server must have a matching username in it table of users. The username may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

User Passphrase
This is the user specific passphrase used to authenticate the client to the server. The server must have a matching passphrase in its table of users. This passphrase is also used to generate 128-bit AES session keys, used to cypher communications between the client and server. The passphrase may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

Notes

Tunnel Users Screen



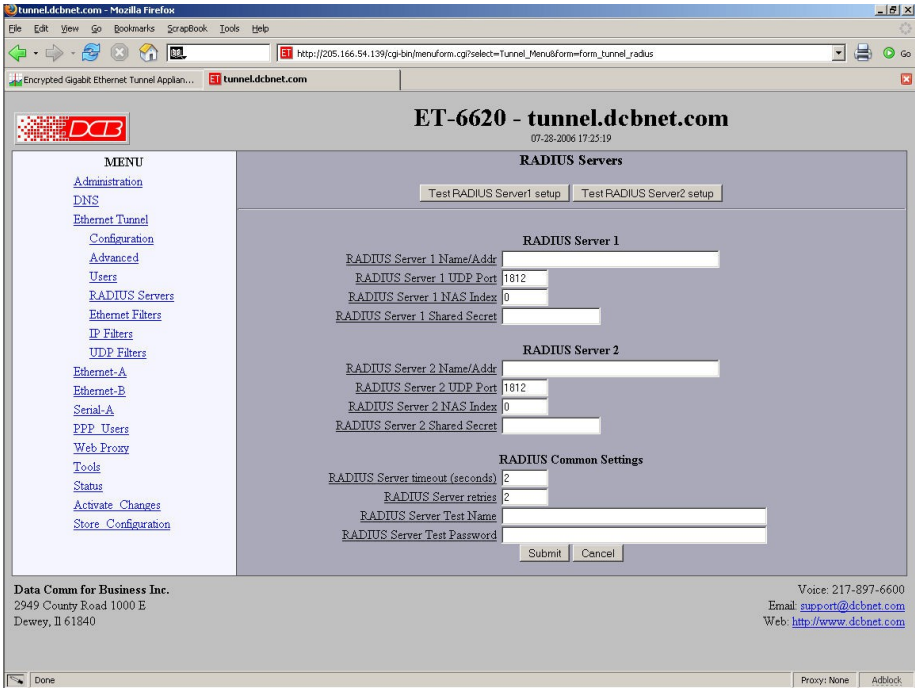
Tunnel Users Screen

This table specifies the usernames and password for remote ET users. It will be used to authenticate remote users on the system. There are multiple screens (up to 5 on the 6604 and up to 10 on the 6620) available.

Fields

- Username
  A string of 0 to 15 printable characters. Do not use space or control characters. Ignored if blank..
- Password
  A string of 0 to 15 printable characters. Do not use space or control characters. Ignored if blank.

Radius Servers Screen



Radius Servers Screen

This table specifies up to two RADIUS servers used to authenticate remote ET users. If configured, these will be used to authenticate remote users on the system instead of the internal database. There are multiple screens (up to 5 on the 6604 and up to 10 on the 6620) available.

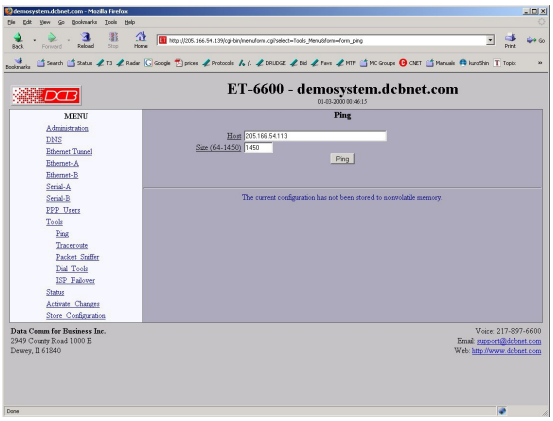
Fields

- RADIUS Server x Name/Addr
  The name or IP address of the RADIUS server that is to authenticate remote tunnel users. If blank, this entry is ignored.
- RADIUS Server x UDP Port
  Each RADIUS Server can use a different UDP port number. The default UDP RADIUS Authentication port is 1812.
- RADIUS Server x NIS Index
  When the ET server asks for authentication from a RADIUS server, it supplies a Name, a Password, and an Index. The index allows the RADIUS Server to distinguish one ET server from another. It can also be used by the Server for other purposes beyond the scope of this help file. Zero is the default index.
- RADIUS Server x Shared Secret
  A shared secret (e.g. passphrase) is used between the RADIUS Server and the ET server for security. The shared secret set in the ET server must match the expected shared secret for that ET server on the RADIUS Servers. (RADIUS servers can distinguish clients by their incoming IP address, so each RADIUS client can have a different shared secret.) If the ET tunnel is using RADIUS servers, but the shared secrets do not match, no remote Tunnel users will be able to establish a tunnel connection. This will be noted in the ET Server log, but not the remote ET Tunnel log. For compatibility, shared secrets

are limited to 16 characters, and cannot include the double quote character. Note that the shared secret is not the same as the ET passphrase.

- RADIUS Server Timeout (seconds)
  he length of time in seconds that a RADIUS server can take for a response. This must be at least one second. The default is 2 seconds. Long retries may impair the ability of the secondary RADIUS server from being effective.
- RADIUS Server Retries
  The number of times to attempt to contact a RADIUS server. Retries are taken only when a server does not respond. Too many retries may prevent the secondary RADIUS server from being used (because the remote ET device times out first.)
- RADIUS Server Test Name
  Only used when pressing the Test RADIUS Server buttons. Use this field to test a RADIUS Server to see if it accepts or rejects an authorization request. Normally, the name and password come from remote ET devices, but for the RADIUS Server test, you must supply a name, (as a substitute for the remote ET's "User Name",) and this field is where you enter it before you press the Test Button. For security, this field isn't stored in the config file.
- RADIUS Server Test Password
  Only used when pressing the Test RADIUS Server buttons. Use this field to test a RADIUS Server to see if it accepts or rejects an authorization request. Normally, the name and password come from remote ET devices, but for the RADIUS Server test, you must supply a password, (as a substitute for the remote ET's "User Passphrase",) and this field is where you enter it before you press the Test Button. For security, this field isn't stored in the config file.

Ping Screen



Ping Screen

Ping will send four ICMP echo requests to the specified host. It will wait approximately 16 seconds for a response.

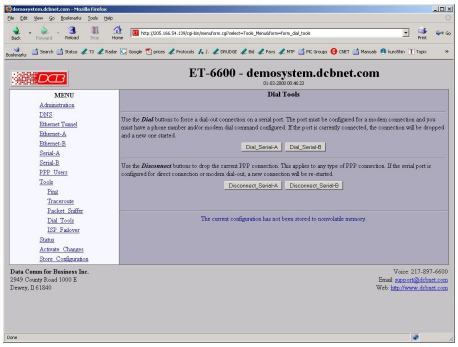
Fields

- Host
  IP address of the target host. If hostname DNS is enabled, you may use a hostname.
- Size
  Number of data bytes to send.

Notes

- Ping and traceroute are useful tools to determine if routing is correct.
- Ping may also be used to ”force” a dial-up connection to dial.

Dial Tools Screen



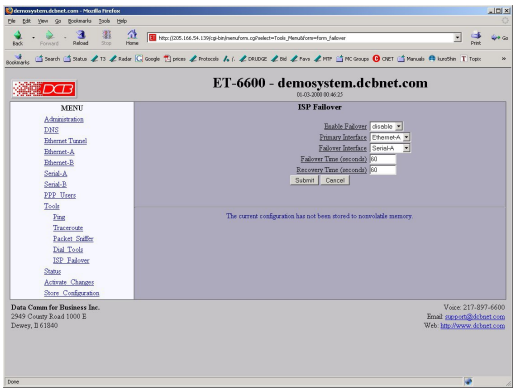
Dial Tools Screen

This screen is used to test and manage the serial lines. The action buttons allow a dial operation to be forced or a connection to be terminated on each interface.

Notes

- Check the port status screens to verify that the disconnect or dial operation was performed correctly.

ISP Fail-over Screen



ISP Fail-over Screen

ISP Failover is a tool that will detect routing failures through a primary interface to an Internet Service Provider (ISP). When a failure is detected, default routing will switch to a secondary (or failover) interface. When recovery is detected, default routing will switch back to the primary interface.

ISP Failover works by periodically testing access to an ISP's DNS server. As long as the server is responding, the tunnel will consider the primary interface to be UP. In the event that the DNS server stops responding, the tunnel will consider the primary interface to be DOWN.

While in failover mode, the tunnel will continue to test access to the ISP's DNS server. When the server starts responding again, recovery is initiated.

In order for the ISP Failover tool to work, the ISP must be dynamically assigning the DNS server to the tunnel. Also, the DNS server for the primary interface and the failover interface must not be the same. Also, both the primary interface and the failover interface must be configured with a default route. The ISP Failover tool will selectively apply the default route based on which interface is in use.

The best method for setting up failover is to first leave the ISP Failover tool disabled and set up the primary interface and the failover interface independently. With the failover interface disabled, configure the primary interface. Make sure it is correctly operating. Then disable the primary interface and enable the failover interface. Make sure it is operating correctly. Then enable both interfaces and the ISP Failover tool.

Fields

- Username
  A string of 0 to 15 printable characters. Do not use space or control characters. Ignored if blank..
- Enable
  Enable/Disable failure detection.
- Primary Interface
  This specifies which interface is to be used as the primary interface. When not in a failover condition, the default route will be applied to the primary interface and will not be applied to the failover interface.
- Failover Interface
  This specifies which interface is to be used as the failover interface. When in a failover condition the default route will be applied to the failover interface and will not be applied to the primary interface.
- Failover Time
  If the primary interface is down for this period of time the tunnel switches to failover mode. This time is set in seconds. The actual test interval will be 1/5 this time. Five consecutive failures will trigger the failover.

  Make sure you do not set this value too low for the primary interface. For example, if the primary interface is through a modem, make sure to allow for dial and connect time. This could be more than 30 seconds. If the primary interface is through an Ethernet port make sure to allow time for 10/100 negotiation and DHCP service.
- Recovery Time
  If the primary interface is up for this period of time the tunnel will switch out of failover mode. This time is set in seconds. The actual test interval will be 1/5 this time. Fibe consecutive responses will trigger recovery.

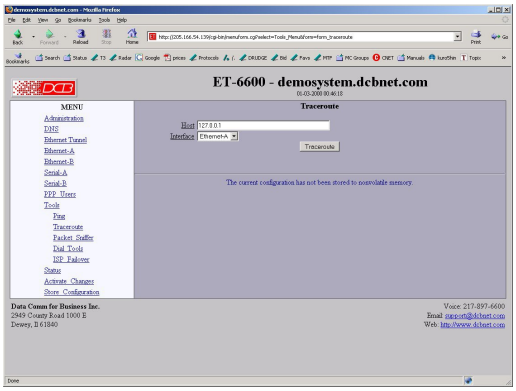
Notes

Make sure to add a static default route for both the primary and failover interface. The tunnel will selectively apply the default route depending whether or not there is a failover condition. For Ethernet interfaces, this is not necessary if DHCP client is enabled and the DHCP server supplies a default route.

Don't be to aggressive on your Failover Time setting. If the value is too low, the tunnel may get stuck in a situation where it never recovers.

Each time the tunnel switches interfaces, both primary and failover interfaces are taken down then brought back up. This is necessary to clear out any NAT associations and to clear out all old cached routes from the routing table. For dial-up connections, this means that the modem will be disconnect if currently connected.

Traceroute Screen



Traceroute Screen

Traceroute displays the route that a packet will take to reach another host. This is performed by sending UDP packets to port 33434 with progressively larger Time-to-Live values and listening for ICMP TIME-EXCEEDED responses from the bridges along the way.

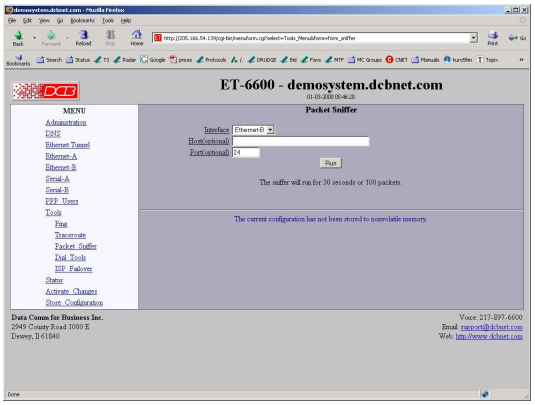
Fields

Host
IP address of the target host. If hostname DNS is enabled, you may use a hostname.

Interface
Which interface to use. The routing table is bypassed.

Notes

Packet Sniffer Screen



Packet Sniffer Screen

The Packet Sniffer allows you to take a snapshot of the network traffic passing through an interface.

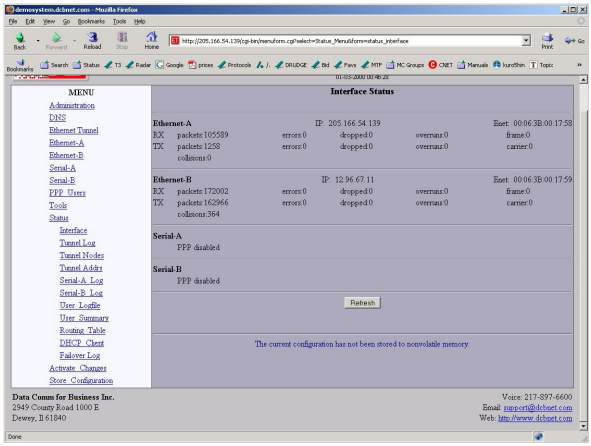
Fields

- Interface
  Which interface to use. If the interface is a serial port, you will only see the traffic that is passing through the IP layer of PPP. You will not see low-level PPP traffic.
- Host
  This applies a host filter. Only packets with a matching source or destination IP address will be included in the trace.
- Port
  This applies a port number filter. Only TCP or UDP packets with a matching source or destination port number will be included in the trace..

Notes

- Only packet headers are shown. You will not be able to see the data contents of the packets.

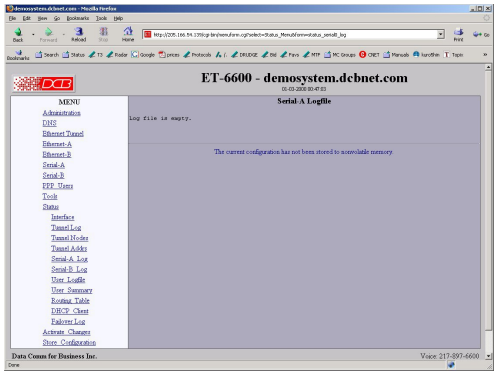
Interface Status Screen



Status Screen

The Interface Status screen shows port status and packet counters for each interface on the ET.

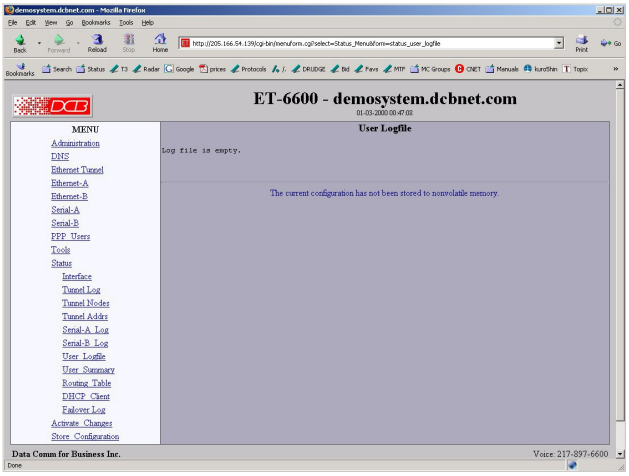
Serial A/B Log Screen



Interface Log Screen

The Interface Log screen shows important events logged for each interface on the ET.

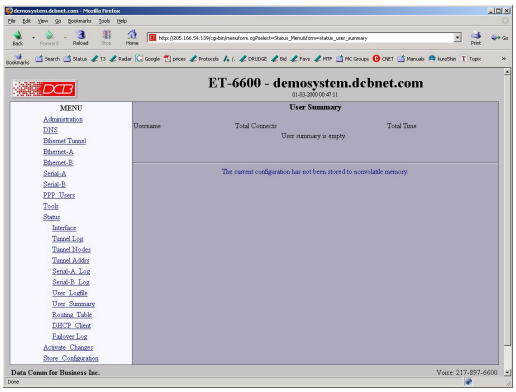
User Log Screen



User Log Screen

The User Log screen shows connect and disconnect events logged at the system level on the ET. No logging is performed if PPP authentication is disabled.

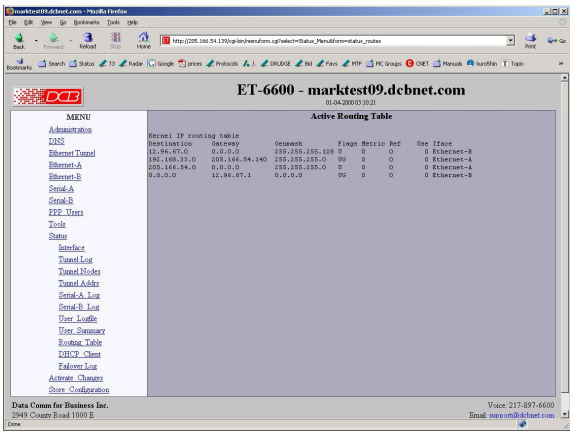
User Summary Screen



User Summary Screen

The User Summary screen shows connection detail by user on the ET.

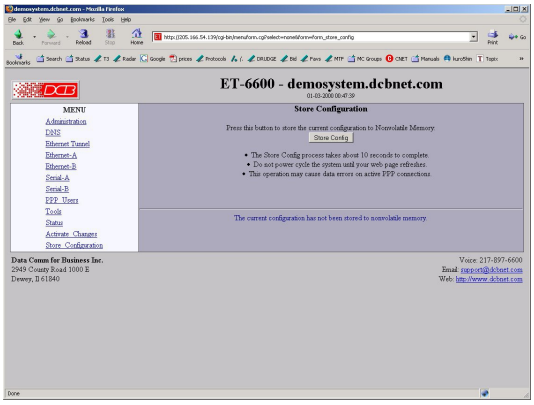
Routing Table Screen



Routing Table Screen

The Routing Table screen shows all routes configured in the ET.

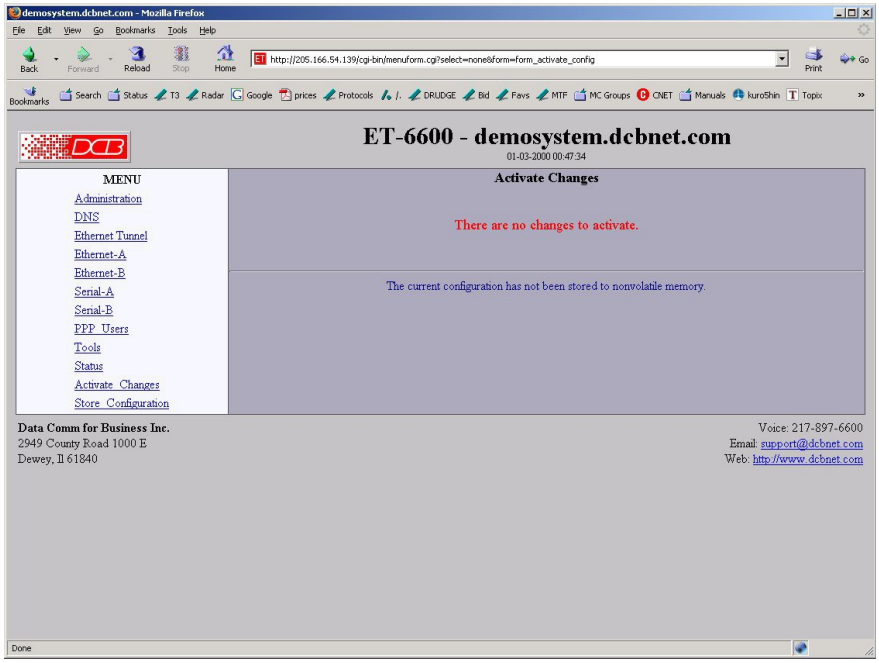
Store Configuration Screen



Store Configuration Screen

The Store configuration screen is used to store the current configuration to non-volatile memory. This does not activate configuration changes. Configuration changes are made to a temporary area. They may be "activated" using the Activate Changes screen, in which case they will become immediately active, overwriting the pre-existing configuration for the duration of this session; or they may be "stored" using this screen, in which case they will be written to non-volatile memory and used at the next reset or power-up.

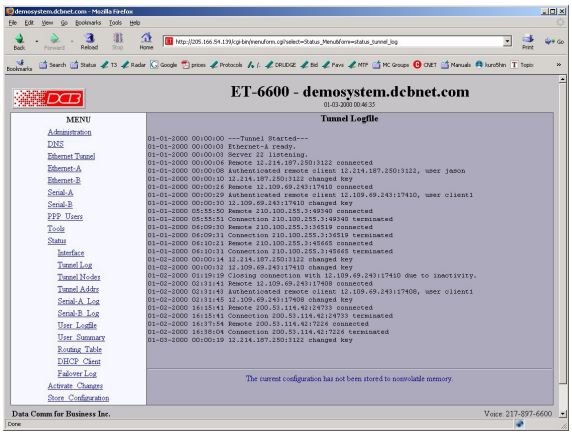
Activate Configuration Screen



Activate Configuration Screen

The Activate configuration screen is used to activate the current changes. Configuration changes are made to a temporary area. These changes will become immediately active, overwriting the pre-existing configuration for the duration of this session. Changes may be "stored" using the store configuration screen, in which case they will be written to non-volatile memory and used at the next reset or power-up.

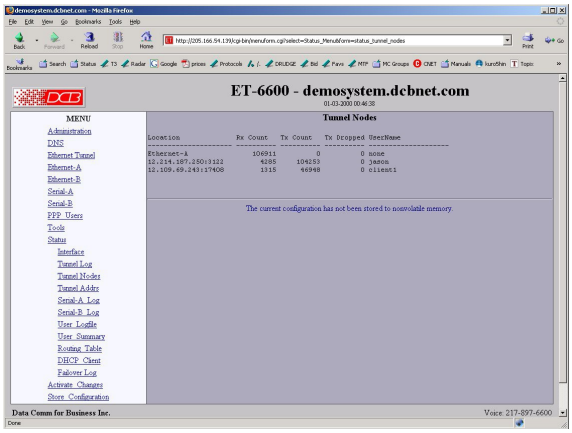
Tunnel Log Screen



Tunnel Log Screen

The Tunnel Log File Screen displays a record of all key changes, connections, authentications, and disconnects.

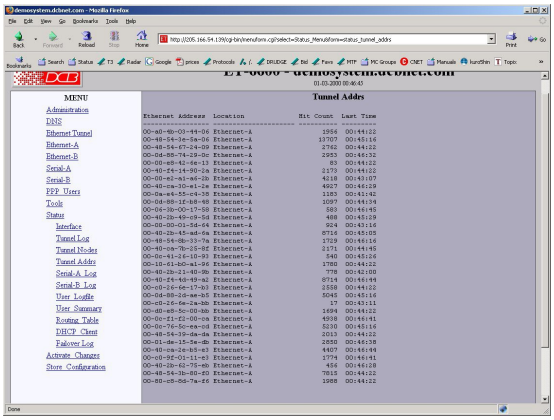
Tunnel Nodes Screen



Tunnel Nodes Screen

The Tunnel Nodes Screen displays currently connected remote nodes. These nodes are other ET units that have authenticated with this unit.

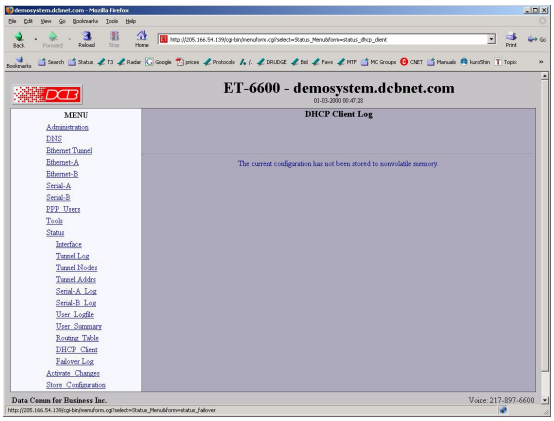
Tunnel Addresses Screen



Tunnel Addresses Screen

The Tunnel Addresses Screen displays the MAC address, interface location, number of packets passed, and time of the last packet received from tunneled nodes.

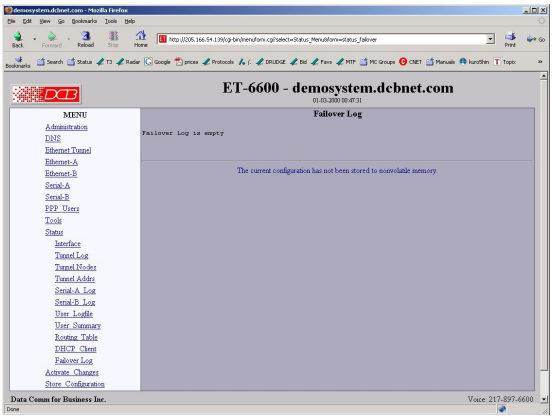
DHCP Client Log Screen



DHCP Client Log Screen

The DHCP Client Log Screen displays recent history of DHCP client activity.

ISP Fail-over Log Screen



ISP Failover Log Screen

The ISP Fail-over Log Screen displays recent history of ISP Fail-over operation.

Chapter 5
Operation

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

Common Uses – Overview

Some of the most commonly used configurations are for:

- Remote LAN connected to local LAN via dial-in PPP using a modem or wireless connection.
- Remote LAN connected to local LAN via broadband ISP Internet connection
- Remote LAN connected to local LAN via a dedicated communications link.
- LAN-to-LAN connection using dial on demand (DOD).

Any of these connection methods may have the data transverse the Internet, a private network, various firewalls, NAT servers, and other routes. Although any ethernet protocol may be bridged (including UDP, IP, Netbios, Appletalk, etc) the connection between two ET units is via TCP/IP, therefore a TCP connection is required between the two ET units. The ET serial ports support PPP.

These configurations are detailed in this chapter. Some sample configuration files may be downloaded from the DCB support web site and then transferred to your bridge.

The local or remote LAN may be a full-fledged network or a single PC using an ethernet cross-over cable.

The ET link requires one unit to be configured as a server, and one or more units configured as clients. A single ET may function as both a server and a client.

Remote LAN to Local LAN via PPP

A server ET is connected to the host remote LAN and configured for dial-in PPP on one serial port. The remote ET client is configured as a PPP dial-in client, and a PC is connected to its Ethernet A port via a cross-over cable.

Remote LAN to Local LAN via Broadband Internet

The server ET is connected to the host remote LAN and eventually connected to the Internet via some ISP. The remote client ET is connected to a broadband router via Ethernet B, and a local LAN is connected to Ethernet A. All PCs on the local LAN are bridged to the remote LAN.

Remote LAN to Local LAN via Dedicated Serial Link

A server ET is connected to the host remote LAN and configured for direct-connect PPP on one serial port. The remote ET client is configured as a PPP direct connect client, and a PC is connected to its Ethernet A port via a cross-over cable, or the remote LAN is connected to Ethernet A. A dedicated serial link connects the serial PPP ports on the two ET units.

Remote LAN to Local LAN via PPP with Dial on Demand

Similar to the PPP connection above, however the PPP is simply configured for Dial on Demand. Whenever the ET senses a packet to transfer to the other LAN, it dials up the remote site automatically.

Chapter 6
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 EtherSeries bridge 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.

***P*:** All the LEDs are off.
S: Check the power supply or power connection.

***P*:** When using 10/100/1000Base-T cabling, the unit does not work.
S: Check the switch or hub's link LED for the port to which the bridge is connected. If it is off, make sure the network cable between the bridge and hub is in good condition.

How To Set The Bridge To Factory Defaults ET-3302

If you know the IP address, you may browse to the Administration screen – Set All Defaults. If the IP address is unknown, use the serial connection setup method (Chapter 2), and answer Yes when asked if you wish to reset the unit to factory defaults. The factory default IP adderss for the trusted side ethernet port (Port A) is 192.168.0.1 . Another method uses the hardware setup switch for firmware versions 2.19 and newer :

The unit can be set to temporarily set to defaults by pressing and holding the setup switch during power-up. The sequence is:

1) apply power, blue (bottom) led will go on then the green (top) led will go on.
2) wait for the green led to go off
3) press and hold the setup switch
4) wait for the green led to blink on then off
5) the switch may be released.
6) the serial port will be in setup mode and the unit can be accesses from the default address

Note) The default settings are not written to NV memory. The user must store the settings from either the serial port or the web interface.

Can't Connect via the LAN

***P*:** Can't connect with a Web Browser.
S: Check the following:

- Insure that you are addressing the ET correctly ie. https:// instead of http:// for some models .
- Start troubleshooting from a known state. Power the bridge OFF and ON to reboot.
- Is a proper IP address configured in the bridge and PC?
- "Ping" the bridge 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 bridge (e.g. `ping 192.168.0.1`). 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 **The most common problem cause is incorrect IP address configurations. Make sure the workstation and bridge have compatible IP addresses.**
- It may be that your "ARP table" contains invalid entries. You can clear the "ARP table" by rebooting, or, on Windows 95 , by typing the following command at the command prompt or *Run* dialog box.: `ARP * -d`
- Check that you are using the proper Ethernet connection on the bridge. Only Ethernet Port A works at 100BaseT on some models, and the port in use must be enabled. Ethernet Port A is the local, secure side.
- The bridge is meant to be connected to a hub or ethernet switch. If connected directly to a PC, an ethernet crossover cable must be used.
- 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 initial configuration program using a serial cable connection.
S: Check that:

- The communication parameters are set properly.
- Disconnect and reconnect the power supply to the bridge with switch two UP.
- Power is available... an LED is on.
- The terminal program is operating properly. Try a loopback connector at the bridge 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.

Checking Bridge Operation

Once the bridge is installed on your Network, you verify proper operation by testing its functionality. Attempt to send packets through it, to verify its operation. The procedure is as follows.

From a PC on one side of the bridge, ping a PC on the other side of the bridge, or attempt a web connection to a web server on the other side of the bridge. If either method succeeds, then two-way operation is confirmed.

If any one PC on one side of the bridge can communicate with any single PC or server on the other side of the bridge, then the bridge configuration is likely correct and other problems should be investigated with a larger view of the network in mind.

Remember that this unit is a bridge, not a router. All IP addresses should be in the same IP subnet address range.

Appendix A

Specifications

EtherSeries ET-6600 Bridge Specifications

- Flash Memory: 4 Mbytes
- SRAM: 8 Mbytes
- LAN A Interface: 10/100BaseTx, Autosense
- LAN B Interface: 10BaseT
- 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
- Throughput: 700 Kbps
- Supports 8 simultaneous client ETs
- Power: 6 VDC 600mA or Optional power supplies
- Switch: Configuration, Reset
- LED:8 (Status, Serial Activity, LAN Activity, Power)
- Default IP address: 192.168.0.1
- Browser Management port: 80
- Operational Temperature -40C to +85C subject to power supply limitations

EtherSeries ET-6690 Bridge Specifications

- Flash Memory: 4 Mbytes
- SRAM: 8 Mbytes
- LAN A Interface: 10/100BaseTx, Autosense
- LAN B Interface: 10BaseT
- RS-232: One male DE-9 connector (PC –9 Pin)
- RS-232 speed: Up to 230.4.2 Kbps
- Modem Connection: Internal V.92 modem, RJ-11 telco connector
- CPU: Motorola Coldfire 5272 CPU 66 Mhz
- OS: uClinux
- Throughput: 700 Kbps
- Supports 8 simultaneous client ETs
- Power: 6 VDC 600mA or Optional power supplies
- Switch: Configuration, Reset

- LED:8 (Status, Serial Activity, LAN Activity, Power)
- Default IP address: 192.168.0.1
- Browser Management port: 80
- Operational Temperature -40C to +85C subject to power supply limitations

EtherSeries ET-3300 Bridge Specifications

- Flash Memory: 4 Mbytes
- SRAM: 8 Mbytes
- LAN A Interface: 10/100BaseTx, Autosense
- LAN B Interface: 10BaseT
- CPU: Motorola Coldfire 5272 CPU 66 Mhz
- OS: uClinux
- Throughput: 700 Kbps
- Supports 8 simultaneous client ETs
- Power: 6 VDC 600mA or Optional power supplies
- Switch: Configuration
- LED:8 (Status, Serial Activity, LAN Activity, Power)
- Default IP address: 192.168.0.1
- Browser Management port: 80
- Operational Temperature 0C to +50C

EtherSeries ET-3302 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- Trusted LAN 1 Interface: Four ports configured as 10/100BaseTx, Autosense switch
- Untrusted LAN 2 Interface : One10/100BaseT autosense port
- Support for PPPoE on Untrusted LAN interface
- Serial Port (1) RS-232 port for setup
- OS: uClinux
- CPU: 300 Mhz Atheros, 32 MB RAM, 64 MB NAND memory
- Throughput: 10 Mbps or greater
- Supports 8 simultaneous client ETs
- Bridge/Tunnel supports 4096 MAC address table entries
- Power: 10-28 VDC 6 watts supplied with 100-240 VAC external supply (optional power supplies available)
- LED: Power, LAN Activity(5), LAN speed(5)
- Default LAN 1 IP address: 192.168.0.1

- Default LAN 1 IP addresses: DHCP Client
- Browser Management port: 443 (HTTPS)
- Operational Temperature -50C to +85C
- Dimensions 5 ¼ x 4 x 1
- Browser Management port: 443 SSL
- Operational Temperature -20C to +70C

EtherSeries ET-6630 Bridge Specifications

- Flash Memory: 128 M bytes or more
- DRAM: 256 M bytes or more
- LAN A Interface: 10/100/1000BaseT, Autosense
- LAN B Interface: 10/100/1000BaseT, Autosense
- CPU: Pentium 4, 2.66Ghz or faster
- OS: Linux
- Power: 120 VAC or 240 VAC, 260 Watts Maximum
- Rack-mount: 1U high
- Throughput: greater than 300 Mbps
- Supports 100 simultaneous client ETs
- Switch: Configuration
- LED: (Over-temperature warning, LAN Activity, LAN Status (two per interface), Power)
- Default IP address: 192.168.0.1
- Authentication with built-in database or external Radius server
- Browser Management port: 443 SSL
- Operational Temperature 0C to +50C

EtherSeries ET-6602 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100BaseTx, Autosense
- WLAN Interface : Optional Internal 802.11 using Ubiquiti Atheros cards at 900 Mhz, 2.4 Ghz, 4.9 Ghz, and 5.8 Ghz
- Support for PPPoE on Ethernet B and Ethernet C
- USB Interface: (one optional) USB Cellular broadband modem
- Serial Port (1) RS-232 port for setup
- OS: uClinux
- Throughput: 10 Mbps with AES, greater with encryption disabled
- Supports 50 simultaneous client ETs
- Bridge/Tunnel supports 4096 MAC address table entries
- Power: 7-20 VDC 4 watts (Up to 2 amps required for 802.11 radio cards or Optional power supplies. Supplied with 100-240 VAC external supply
- Switch: Serial configuration press-button
- LED:7 (LAN Activity, Power)
- Default LAN 1 IP address: 192.168.0.1
- Default LAN 1/3 IP addresses: DHCP Client
- Browser Management port: 443 (HTTPS)
- Operational Temperature -50C to +85C
- Dimensions 6 ¼ x 6 x 1
- Browser Management port: 443 SSL
- Operational Temperature 0C to +50C

RS-232 PIN Assignments – ET-6600, ET-6690

The EtherSeries 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

RS-232 Port Pin Assignments

Control Signal Operation

DCD

Input. The ET monitors Data Carrier Detect (DCD) to bring up and take down PPP sessions The modem should assert (DCD) when a connection is established and drop DCD when a connection is lost.

Receive Data

Input, data into the bridge

Transmit Data

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

DTR

Output. The ET will assert DTR when it is ready to establish a PPP session and will drop DTR when a PPP session is terminating. The modem should hang up the phone if DTR is inactive. Likewise it should not answer an incoming call if DTR is inactive.

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. When pin 8 input is LOW, the serial interface turns OFF the pin 4 (DTR) and 7 (RTS) output signals.

CTS

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

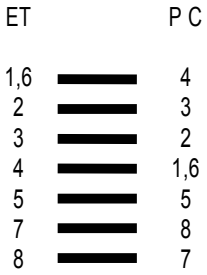
Ring Indicator

Not used

Cables

Commonly used cable connections:

To PC 9-pin COM: port



This null-modem crossover cable is easily constructed by combining a “PC-Direct” adapter hood and a “Remote-PC” adapter hood along with a straight through 10BaseT cable. This cable is used for configuration and is provided with the bridge. This cable is commonly available as a “cross-over” or “null-modem” PC 9-pin connection cable.

Bridge to Modem

Use any commercially available PC-to-modem cable. OR, use a “Remote-PC” adapter hood and an “Asynchronous Modem” adapter hood along with a straight through 10BaseT cable. This cable is provided with the bridge by replacing the above cable adapter hood with the “Asynchronous Modem” adapter hood.

Bridge to hub or ethernet switch

Use any commercially available 10/100BaseT cable. If using 100BaseT or 1000BaseT, an appropriately rated cable is required.

Bridge to PC crossover ethernet cable

A crossover cable may be constructed to allow the bridge **ethernet port** to directly connect to a PC without using a hub.

Use the following pinout to build an ethernet crossover cable:

ET		PC
RJ-45		RJ-45
PIN		PIN
1	-	3
2	-	6
3	-	1
6	-	2

Appendix B

Open Source Software Information

Some models of the ET bridge were designed in conjunction with Open Source Linux software.

Introduction

Some models of the ET bridge were 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

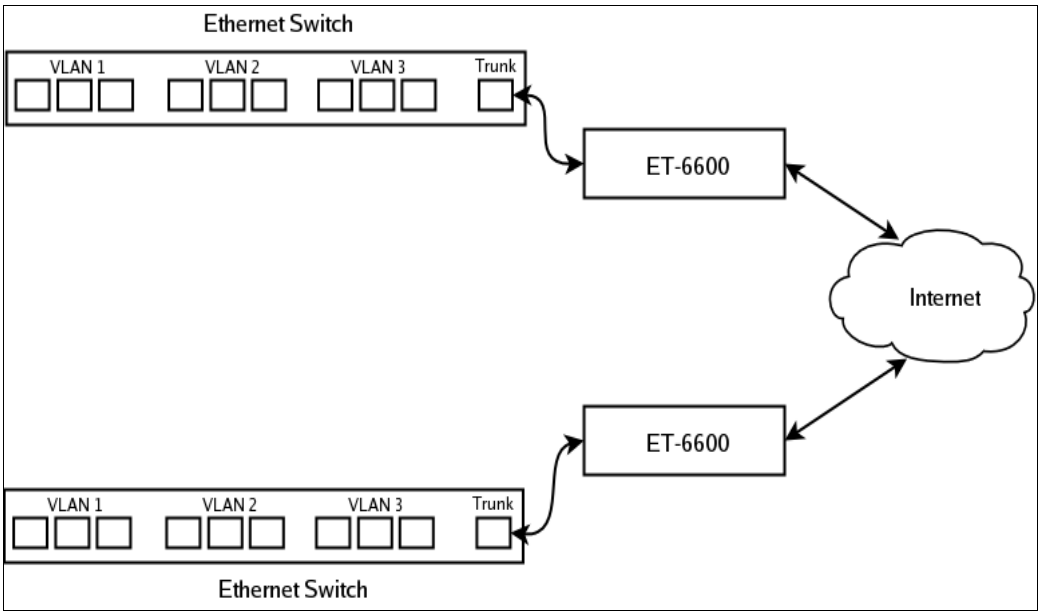
Appendix C

802.1Q VLAN Tagging

The ET family supports bridging of 802.1Q VLAN packets.

Introduction

Firmware versions 1.02 and later for the ET adds support for bridging 802.1Q Tagged Ethernet. An application for this is shown below where two 802.1Q VLAN switches are being tunneled across the Internet.



VLAN Configuration Differences

The default configuration for the ET is for Standard Ethernet. You cannot attach Ethernet-A to the VLAN trunk without first enabling it for operation on a VLAN. There are two way for you to do this. The first way is through the serial setup. The setup utility will ask if you will be attaching Ethernet-A to a VLAN trunk. If you answer "yes", it will then ask for a VLAN ID. When you complete serial setup, you can attach Ethernet-A to the VLAN trunk and will be able to access the ET from the VLAN that you specified. In other words, if you set the VLAN ID to 2, you will be able to access the ET from any Ethernet port on VLAN 2.

The second way to set the VLAN ID is through the web interface using the default IP configuration. If you choose to use this method, remember that you must first attach the ET to untagged or standard Ethernet port, set the VLAN ID, activate the changes, then move the Ethernet cable to the VLAN trunk.

In addition to setting the VLAN ID, you must also set the Tunnel Configuration for 802.1Q Ethernet. You will find this option in the *Tunnel Configuration – Advanced Configuration* web screen.

Note that when configured for a VLAN trunk, the operator interface is no longer available on the ET, as it's seeing the ethernet port as a trunk port.