UT-6630

Encrypted Ethernet Tunnel

User's Guide

Revised June 22, 2012

Firmware Version 1.x

Certifications

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.

RoHS

Some models of this product is available in RoHS versions.

This product is available in RoHS versions.

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 two ethernet interfaces, one WLAN interface, and one USB-based wireless broadband interface.

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

The bridge transports all valid Ethernet protocols. It provides a virtual private network by bridging the two LANs with a UDP/IP tunnel that may be encrypted using the AES algorithm. 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 to "extend" a flat subnet across other IP address range networks such as the Internet.

Note that configuration screen examples shown in this manual are for the UT family products. Some display screen options may differ slightly from what your unit displays.

EtherSeries UT-Family Applications

The UT-Family connects multiple LAN segments by using standard UDP/IP protocols between the bridges. It is commonly used to connect a remote LAN to a central LAN. The bridges connect using UDP/IP, negotiate an encrypted link, and then bridge all traffic between the two LANs.

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.

The bridge may be configured to auto-connect upon power-up.. In this mode, it will connect to a remote bridge through any valid IP path, and may be configured to use DHCP. It may also be configured to disconnect upon inactivity timers.

When using the broadband (Ethernet) connection (either wireless or wired), 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

Other Protocols

The bridge uses the UCP/IP protocol to connect to its remote peer. It does pass IP, IPX, AppleTalk, and other non-routable protocols through the encrypted IP tunnel. It handles Multi-cast IP including IGMP Report Proxy features.

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 avilable.

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.

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 UT to UT negotiation. The encryption methodology is industry-standard AES. Only workstations on the “secure” side of a unit may be used to configure or control it.

On-board Tools

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

Simple Web Proxy

A simple web proxy is included. This operation allows web traffic from the trusted interface to be passed to the untrusted 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 UT-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 UT Bridge
- Power Adapter
- This User’s Guide CDROM
- Short cable with RJ-45 connectors
- 9-pin PC-direct adapter (Units with serial ports only)
- 9-pin Remote-PC 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, 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, or the default may be used if appropriate for your network..

Any standard web browser may be used for configuration once the bridge is configured with a valid IP address.

The UT-Family of bridges will link only with other UT-Family bridges, however it will connect to the other bridge through any valid ethernet UDP/IP link.

UT-6630 Hardware

Introduction

The UT-6630 model bridge contains two Ethernet ports and two USB ports. It is designed for operation with a direct wired ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, or Cable modem. It supports up to 100 simultaneous remote UT units.

Configuration

This model contains a serial interface to be used in initial setup (if needed) and two USB interfaces (used only if browser certificates are enabled). 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. The setup port is always active on this model**.** Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are much easier to use.

UT-6630 Front

LED Indicators

The front panel LED indicators include an over-temperature warning, LAN Activity, LAN status (two per interface), and power indicator.

USB Connectors

There are two USB connectors. They are interchangeable, and only the first one that senses a USB device connection is activated. The USB interface is used to transfer security certificates (if used).

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 .

Ethernet Connectors

The two 10/100/1000BaseT connectors are auto-sensing

Chapter 2
Installation

This Chapter details the installation process for the UT 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 (using https 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 UT 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.

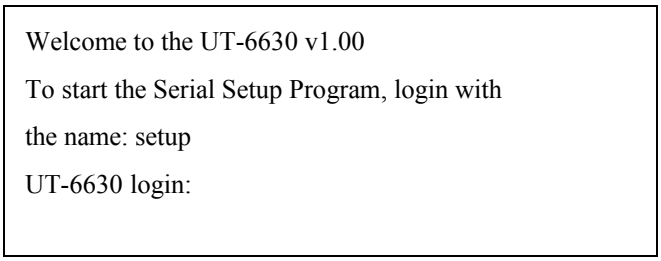
Entries are always tested for valid values. However, there are many "valid" values that are not appropriate for any given configuration. So, "appropriateness" isn't tested. For example, an IP address of 300.400.500.256 will not be accepted, but the field will accept an IP address that is not appropriate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

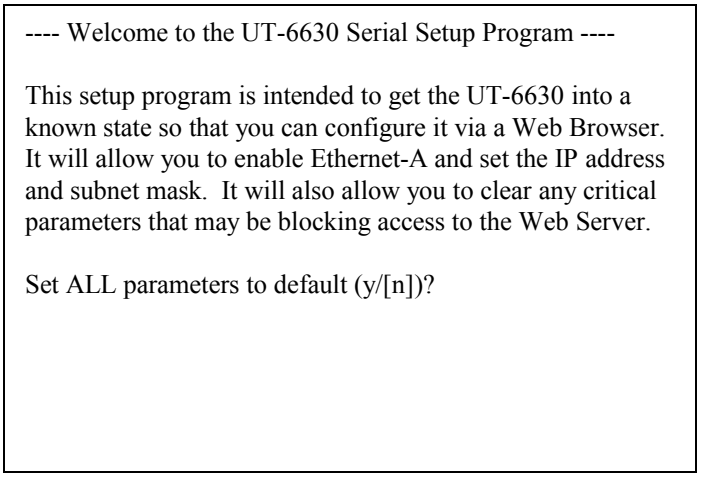
1. Connect a terminal or PC running terminal emulation program (Hyperterm, Procomm, etc) to the serial port of the bridge.
2. Start the terminal emulation program using 9600 bps, 8-bits, No parity, No flow control.
3. Power up the bridge.



Login Screen

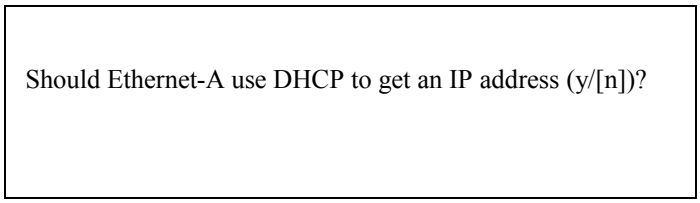
4. The Bridge will start up pausing at a login screen. **For initial setup, enter the login name "setup" in lower case letters. No password is required.**

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...
```

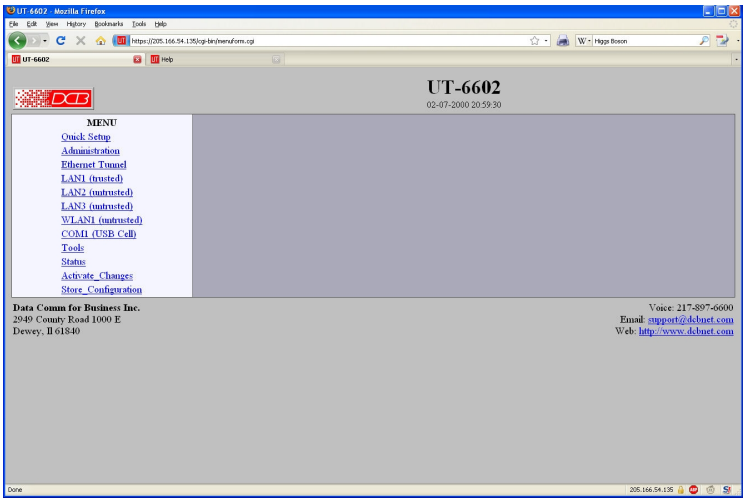
9. The bridge will now reboot.

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 and are using https instead of http for a secure connection. 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

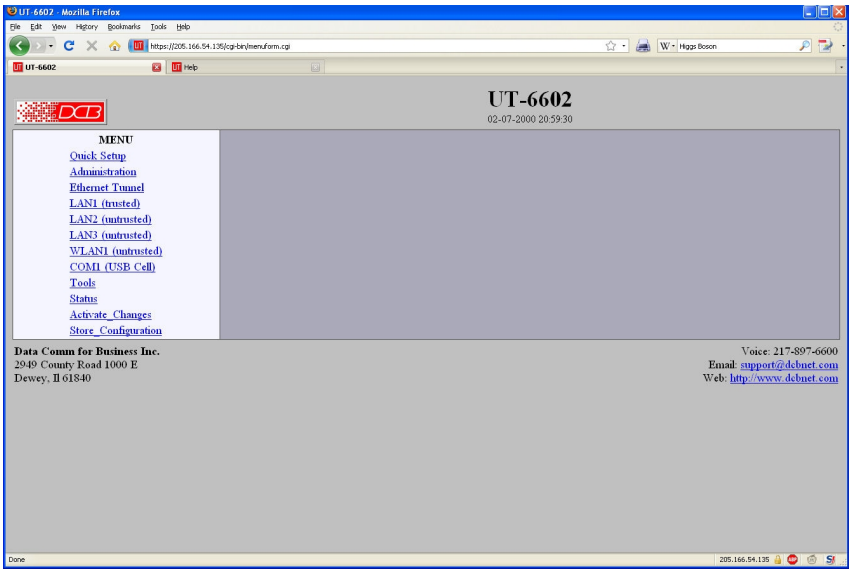
Enter the URL from step 1 (or http://192.168.0.1 if using the default address) into your web browser. The login screen below should be displayed.



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 Configuration Values



Initial Main Menu

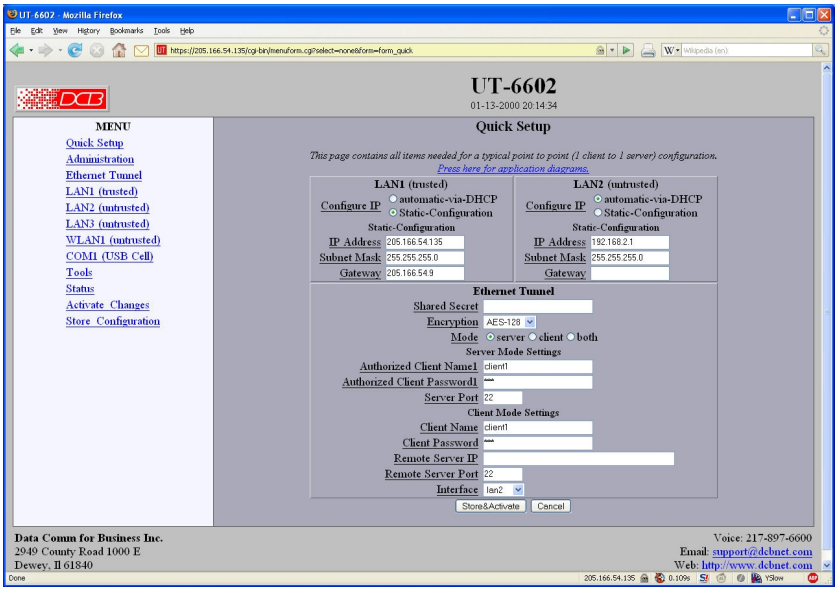
From this index screen, you can select a section on the left and will be taken to configuration screens for each bridge subsystem. You must enter configuration values specific to your installation.

5. Minimum Configuration

The minimum configuration items required for basic LAN-to-LAN bridging connection may all be entered using the Quick Setup screen.

1. Secure side ethernet configuration. Configure ethernet port A to match your LAN.
2. Insecure side ethernet port configuration. The default is to use DHCP on Ethernet port B.
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.

These are all configurable from the initial "Quick Setup" screen (see Chapter 4).



Quick Setup Screen

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 UT-Family bridge using a Web Browser.

Overview

The UT-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

Example 1:

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.

Example 2:.

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.

Example 3:

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.

Saved Configuration Files

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

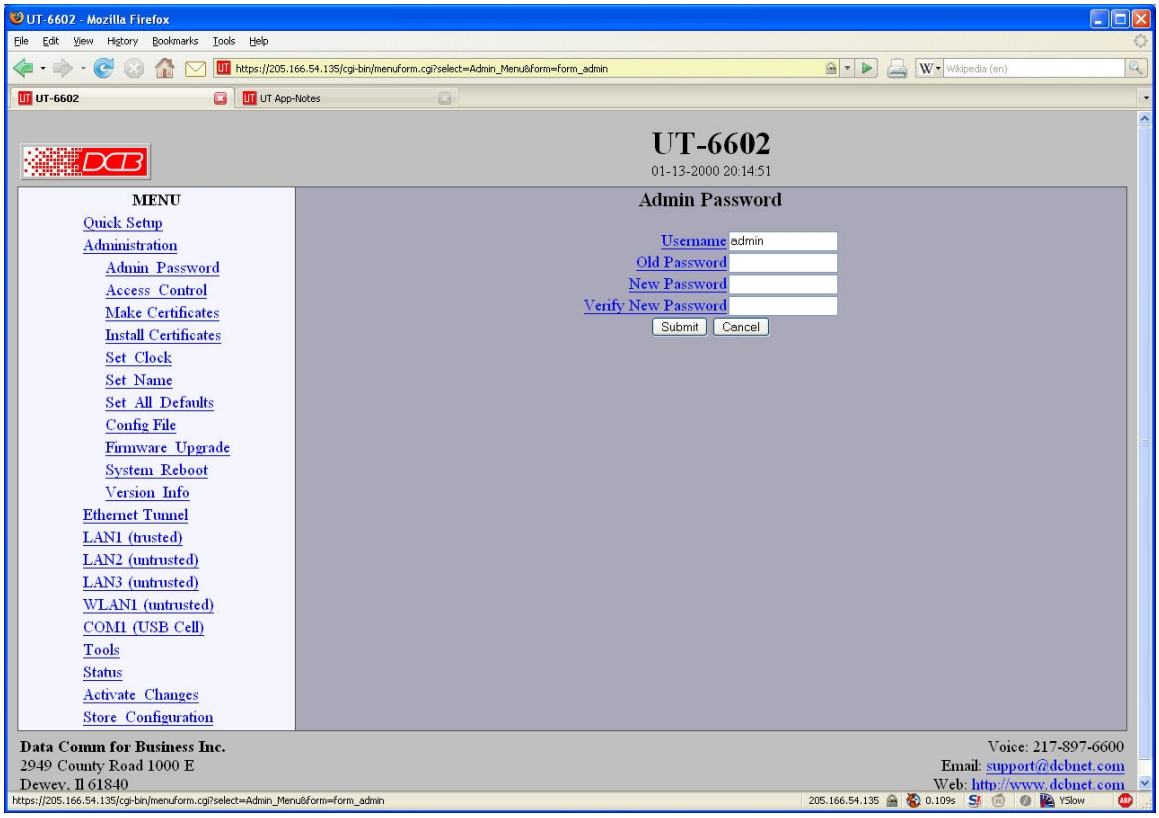
This Chapter describes configuration screens and some configuration hints for the EtherSeries UT-Family Bridge

Overview

The UT-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 UT-6630) requires a secure web browser connection for configuration (https://)

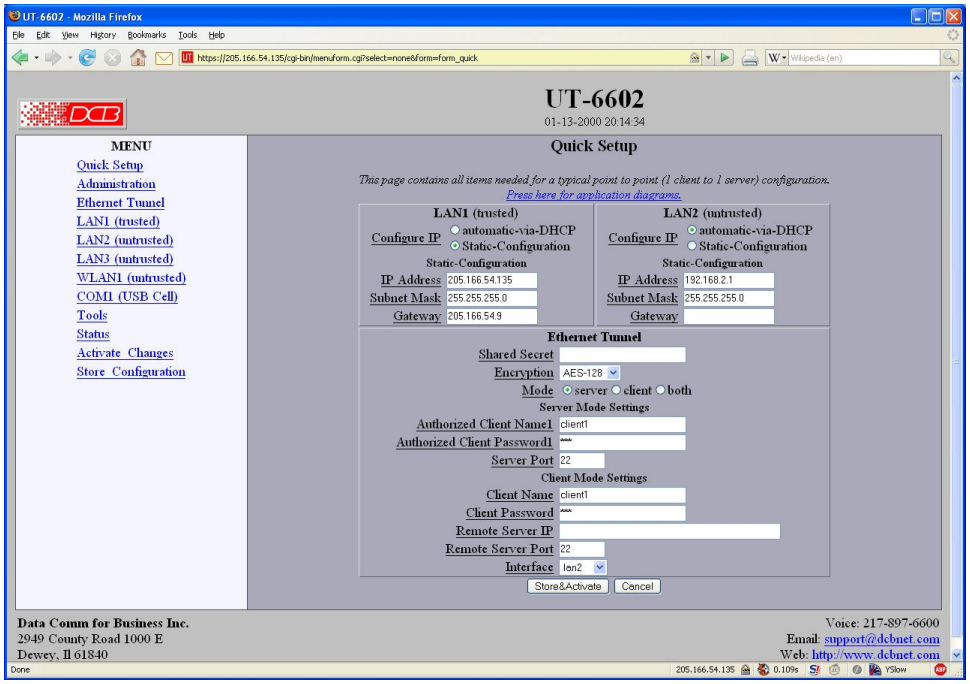


UT-6630 Main Screen

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.

Quick Setup Configuration Screen



Quick Setup Configuration Screen

For a simple point-to-point bridge setup using two hard-wired ethernet interfaces, all needed values may be entered on this single screen. However, if single-port configuration is required, the untrusted ports must be disabled on their Mode configuration screens. If other interfaces are used, their values need to be configured separately.

There is also a link from this page that shows the most commonly used application diagrams

Fields

Ethernet A (Trusted)

- 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.

Ethernet B (Untrusted or public side)

- 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.

Ethernet Tunnel

Shared Secret
The shared secret provides the initial level of privacy. All tunnels participating in the private network must have the same shared secret. This secret phrase is used to generate the 128-bit AES key used to cypher the initial communications. The secret phrase may be up to 52 characters in length. Do not use a quote or backslash character in the phrase. Best security requires a long, random shared secret.

Encryption
This options selects the encryption method for data passed between the tunnels. Encryption is available in 128 but, 192 bit, or 256 Bit AES. AES, also known as Rijndael, is a NIST approved encryption method. “None” disables encryption and is used for greatest throughput when encryption security isn't required.

Mode

Server, Client, or Both. Select the mode for this unit. It is permissible for a tunnel to be both a server and client simultaneously.

Server Mode Settings:

Authorized Client Name1
The name 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.

Authorized Client Password1

The password 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.

Server Port

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

Client Mode Settings:

Client Name

This is the client name sent to the server tunnel when authenticating. The client must use a matching name. The client name may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

Client Password

This is the client password used to authenticate the client to the server. The server must have a matching password in its table of Authorized Remote Clients. The password may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

Remote Server IP

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

Remote Server Port

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

Notes

In simple applications, the Quick Setup screen may be the only screen requiring configuration.

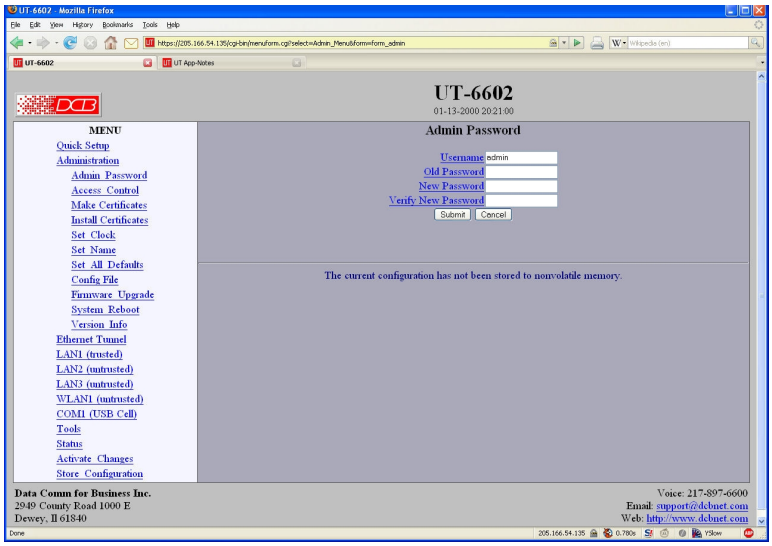
The UT should never be used in actual applications without changing all passwords. When used as a non-encrypting bridge, there is no security on the link between the UTs, and all traffic may be monitored by any node in the link, just as with any other bridge or router.

If the UT is to be used in a single-port application, Ethernet B must be disabled on the Ethernet B Mode screen.

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

Access to the UT'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 UT-6630), use https: (instead of http:) when addressing UT 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.

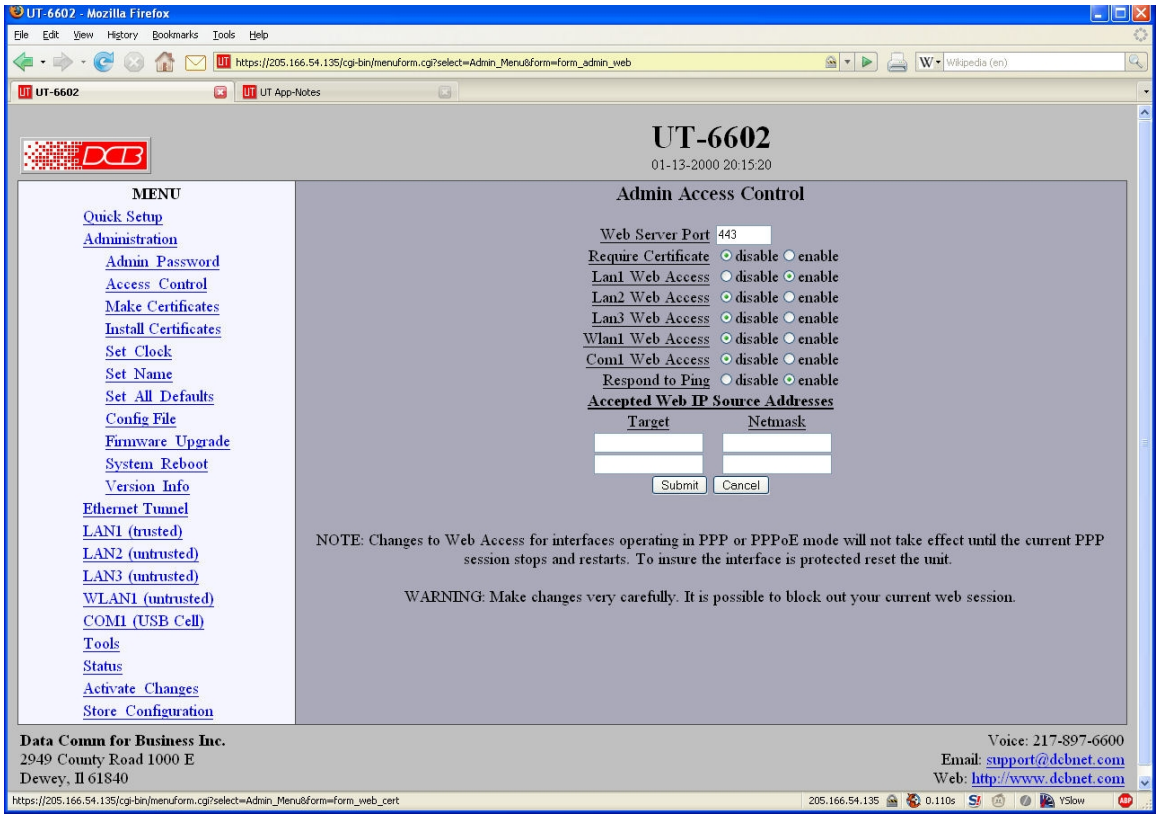
Fields

- 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 should be used. Otherwise, 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 UT's internal web server.

Fields

- Web Server Port
  This is the TCP Port to use for the 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 UT'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 .

- Require Certificates
  This option enables certificate based authentication of web browsers attempting to connect to the tunnel's internal web server. The browser must present the appropriate certificate, otherwise access will be denied. See the help section on making and installing certificates.

  Certificate based authentication is strongly recommended if access to the tunnel's web server is allowed via a public interface.

- Respond to Ping
  This item allows you to block ping requests to the UT. Ping is a valuable tool for diagnosing network problems, but can also become a security problem. Disabling ping causes the UT to not respond to ping requests for one of its IP addresses. It has no effect on the UT's passing of ping request and responses from other network nodes.

- Interface 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 UT'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

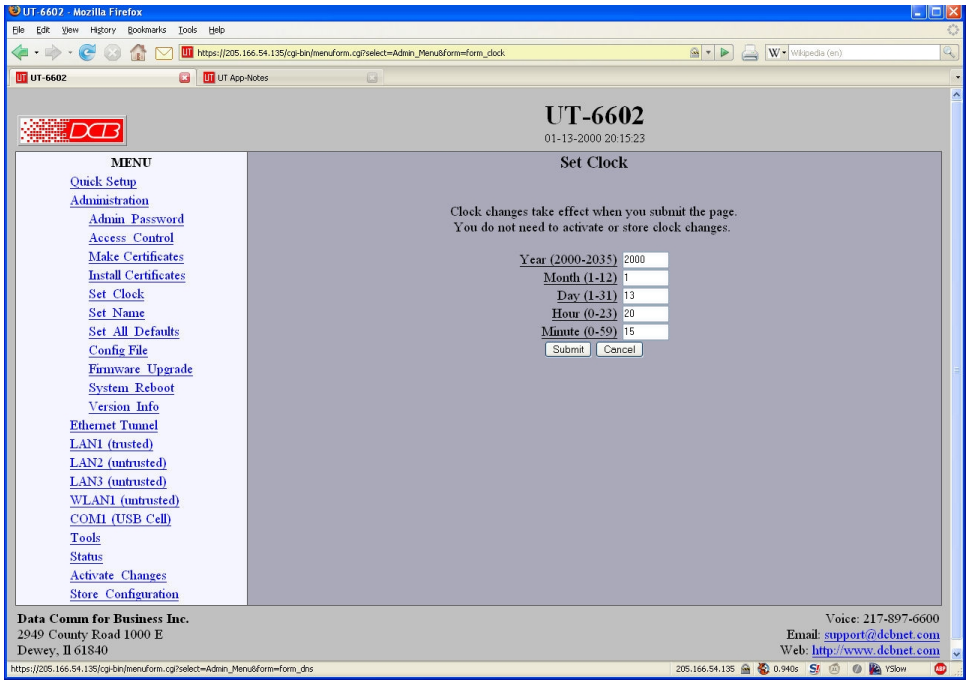
- Target
  Host or Network address.

- 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.

Set Clock



Set Clock Screen

This form allows you to set the UT'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.

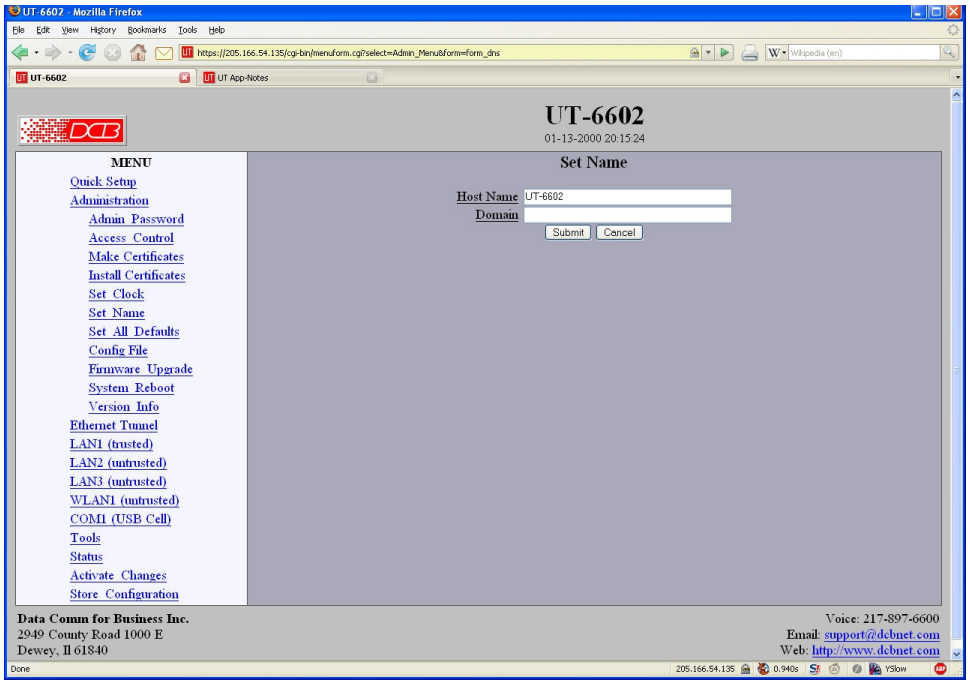
Hour Hour of the day in the range 0 to 23.

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 UT 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 Name



Set Name Screen

This form allows you to set the UT's host name and domain.. The setting will take effect when you "Activate Changes".

Fields

Host Name

The name given to the tunnel. If you enter a name, it will be displayed as the title of the web pages.

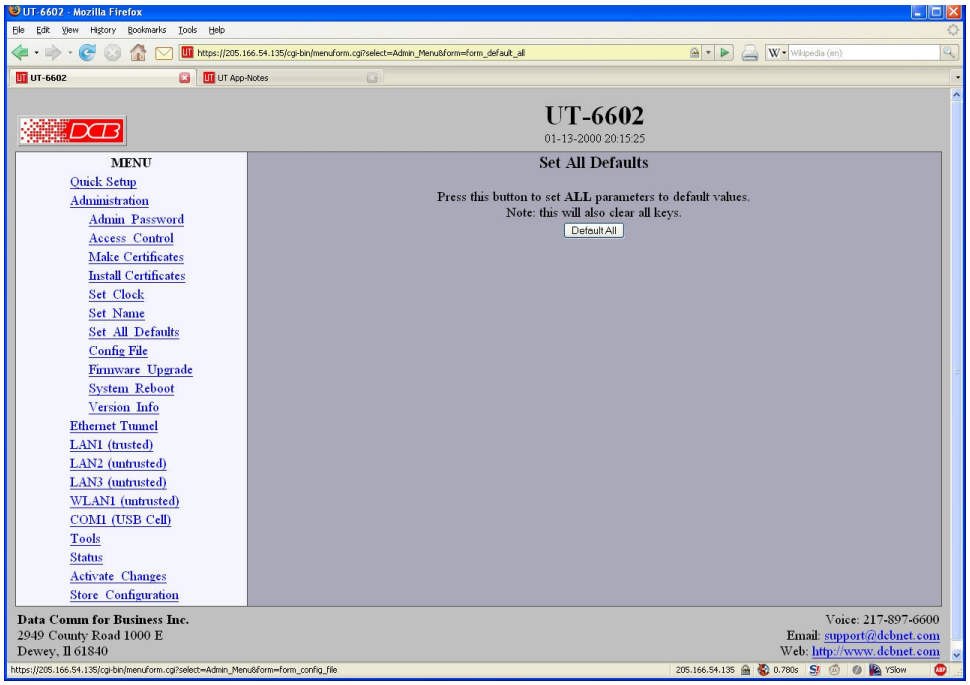
Domain

The name of the local domain. For example: widgets.com

Notes

- If used, these names must be appropriate for your DNS system.

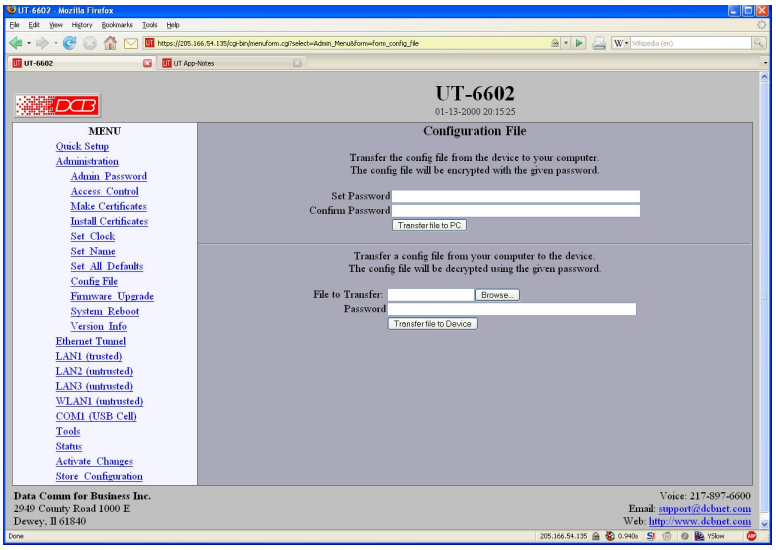
Set All Defaults



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.

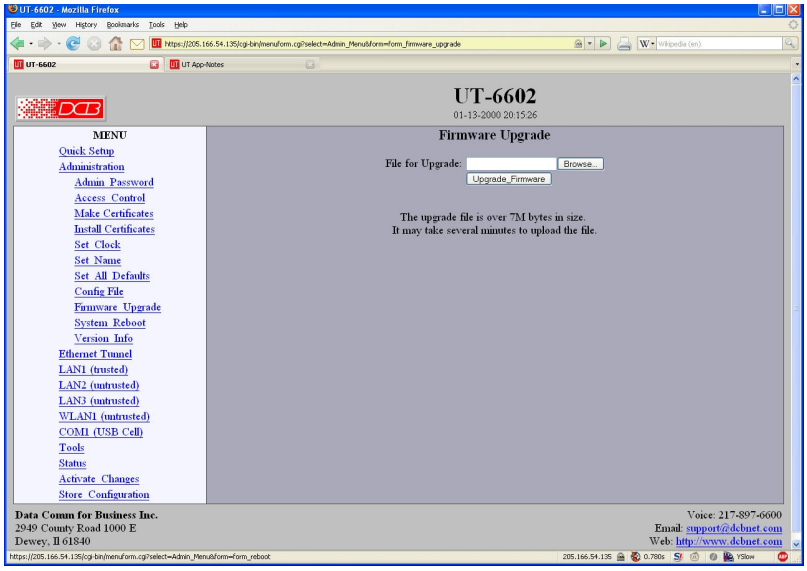
Fields

- 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 UT

Firmware Upgrade



Firmware Upgrade Screen

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

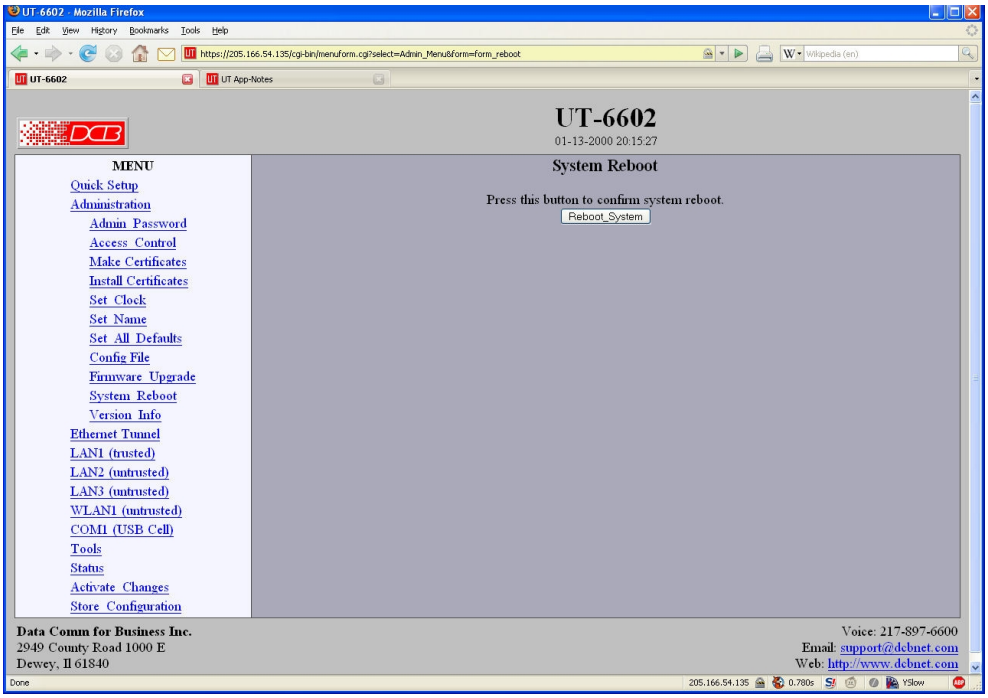
Fields

- 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 UT. 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.

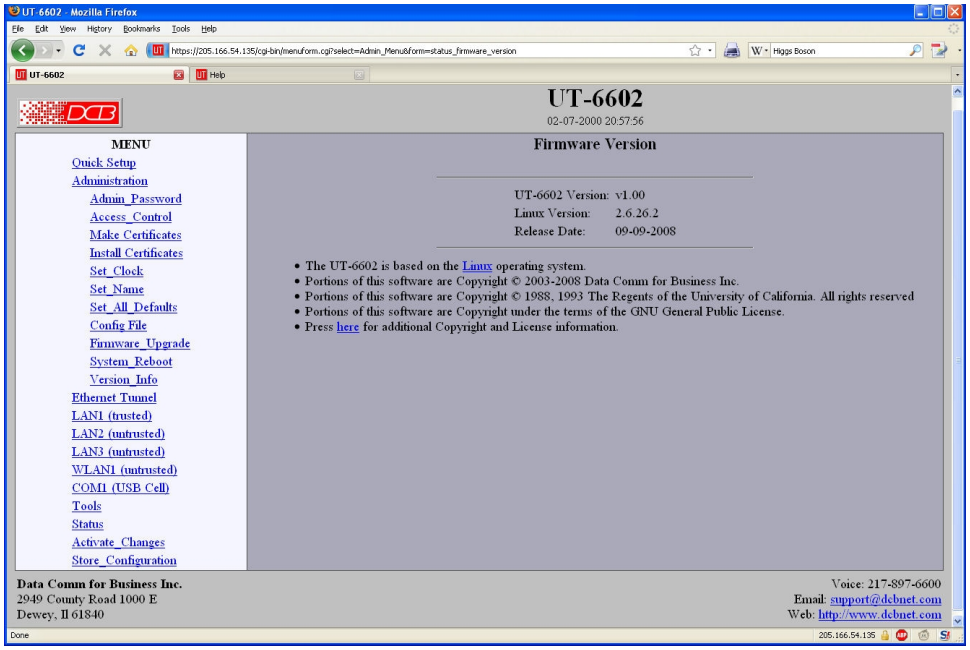
Fields

- 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.

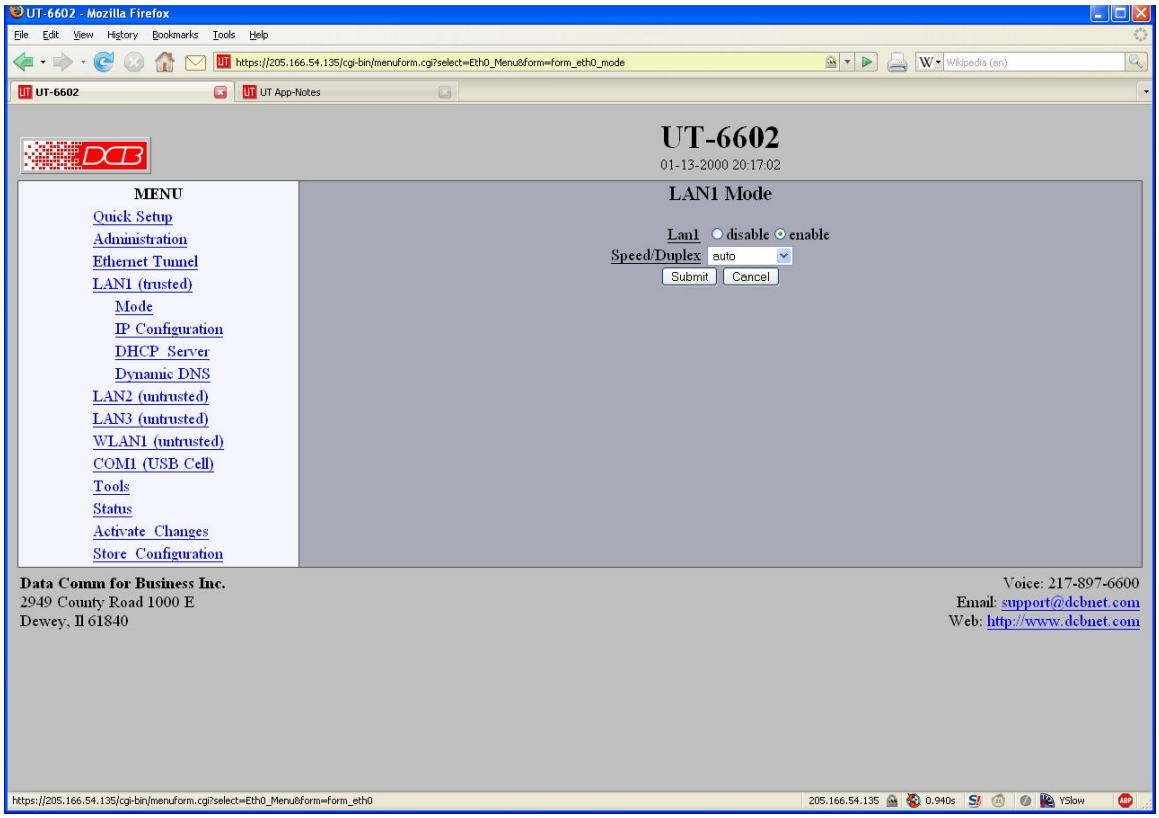
Version Information Screen



Version Information Screen

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

LAN Interface Mode



LAN Interface Mode Screen

The UT contains multiple Ethernet interfaces.

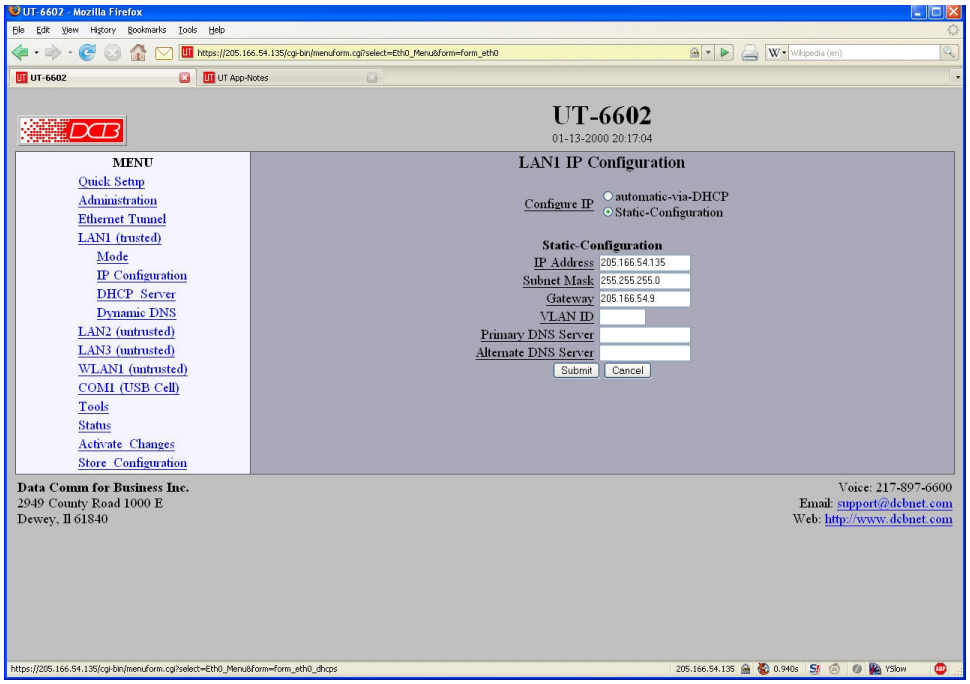
There is an Ethernet Mode screen, used to select the mode for each ethernet port The Mode screen for Ethernet A is limited to enabling the port, and selecting the port speed. Other interfaces are capable of PPPoE, and their mode screen contains additional information. See the Ethernet PPPoE configuration screen section for information pertaining to PPPoE.

Fields

- Enable / Disable
  This should always be set to enable if the interface is to be used.
- Mode
  Select AUTO, 10 Mbps half duplex, or 100 Mbps half duplex.. Select the appropriate one for this interface.

Notes:

LAN 1 IP Configuration



Lan 1 IP Configuration Screen

The UT contains multiple Ethernet interfaces. LAN 1 is normally used for the "local" trusted LAN. Ethernet-B is 10BaseT only. LAN 1 is always a local, secure side of the tunnel. Other interfaces may be configured as either secure or the insecure side, and are usually used with a broadband WAN or public Internet connection. This screen is used to configure IP parameters for LAN 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.

- 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.

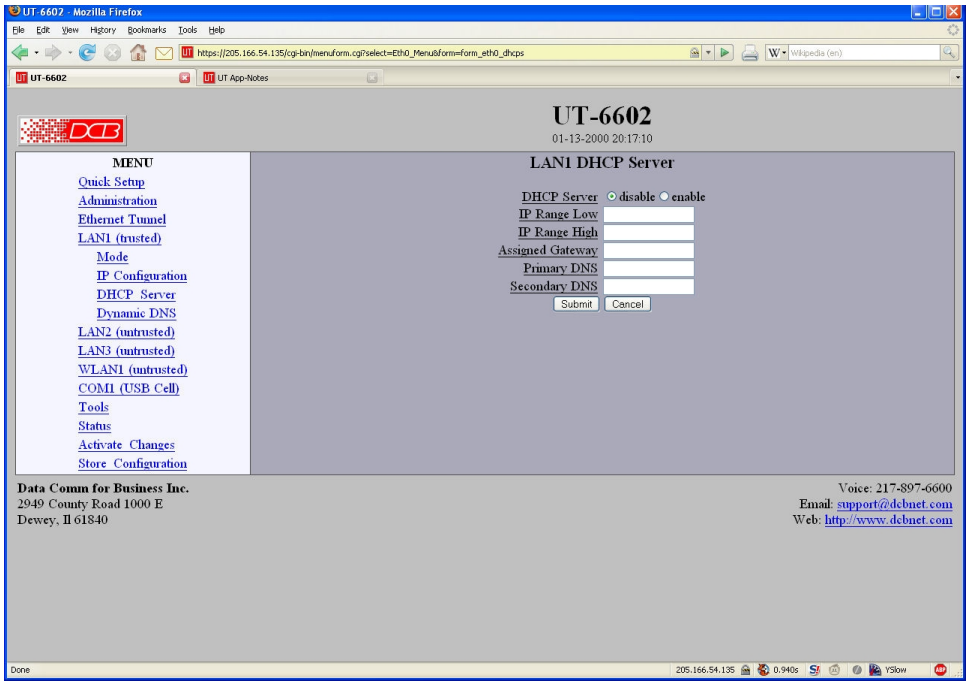
  Note: *Static-configuration* must be used on Ethernet-A if it is configured for an 802.1Q VLAN.

- 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.

LAN 1 DHCP Server Configuration



LAN 1 DHCP Configuration Screen

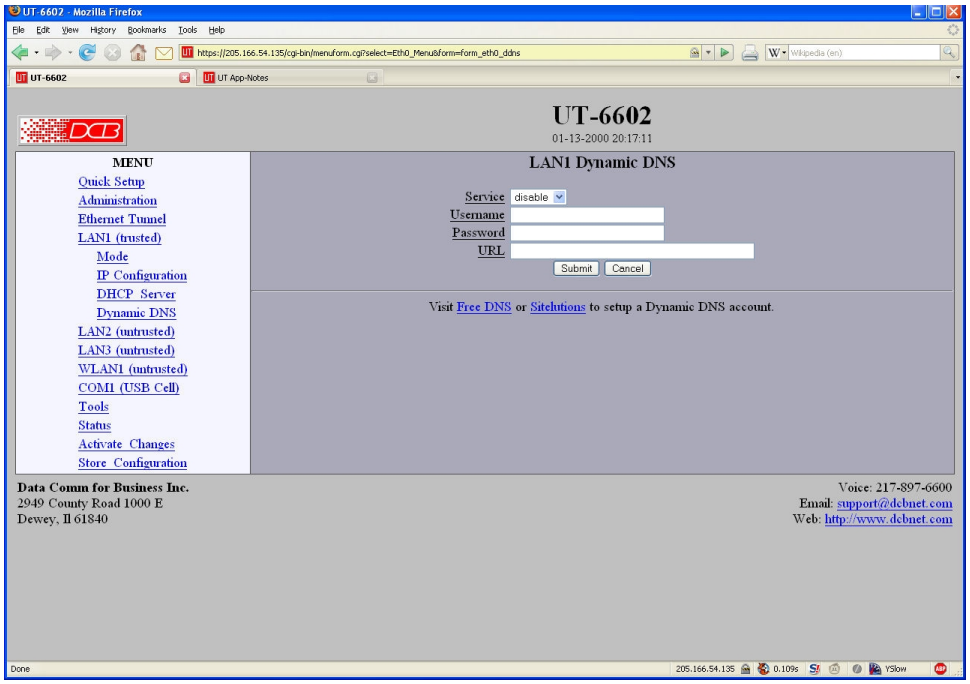
The UT may be configured as a DHCP server to provide Ip addresses, Gateway, and DNS server addressing for clients on the local LAN. This screen is used to enable and configure that service.

Fields

- **DHCP Server**
  Enable/Disable a DHCP Server on the interface. Addresses will be dynamically assigned from the following pool in response to DHCP Client requests.
- **IP Address Range Low Value**
  IP Range Low and IP Range High define an inclusive range of IP addresses to administer. The tunnel will dynamically assign these addresses to DHCP clients as requests are received. These addresses must be valid for the interface's subnet. For example, if the interface has an IP address of 192.168.0.1 and a netmask of 255.255.255.0, then the range of IP addresses must be on the 192.168.0 subnet.
- **IP Address Range High Value**
  IP Range Low and IP Range High define an inclusive range of IP addresses to administer. The tunnel will dynamically assign these addresses to DHCP clients as requests are received. These addresses must be valid for the interface's subnet. For example, if the interface has an IP address of 192.168.0.1 and a netmask of 255.255.255.0, then the range of IP addresses must be on the 192.168.0 subnet.
- **Default Gateway**
  This is the default gateway address to be given to the DHCP client. Typically, it would be the IP address of the gateway router on the subnet.

- **Primary DNS**
  This is the primary DNS server address assigned to the DHCP client.
- **Secondary DNS**
  This is the secondary DNS server address assigned to the DHCP client.

LAN 1 Dynamic DNS Configuration



LAN 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.

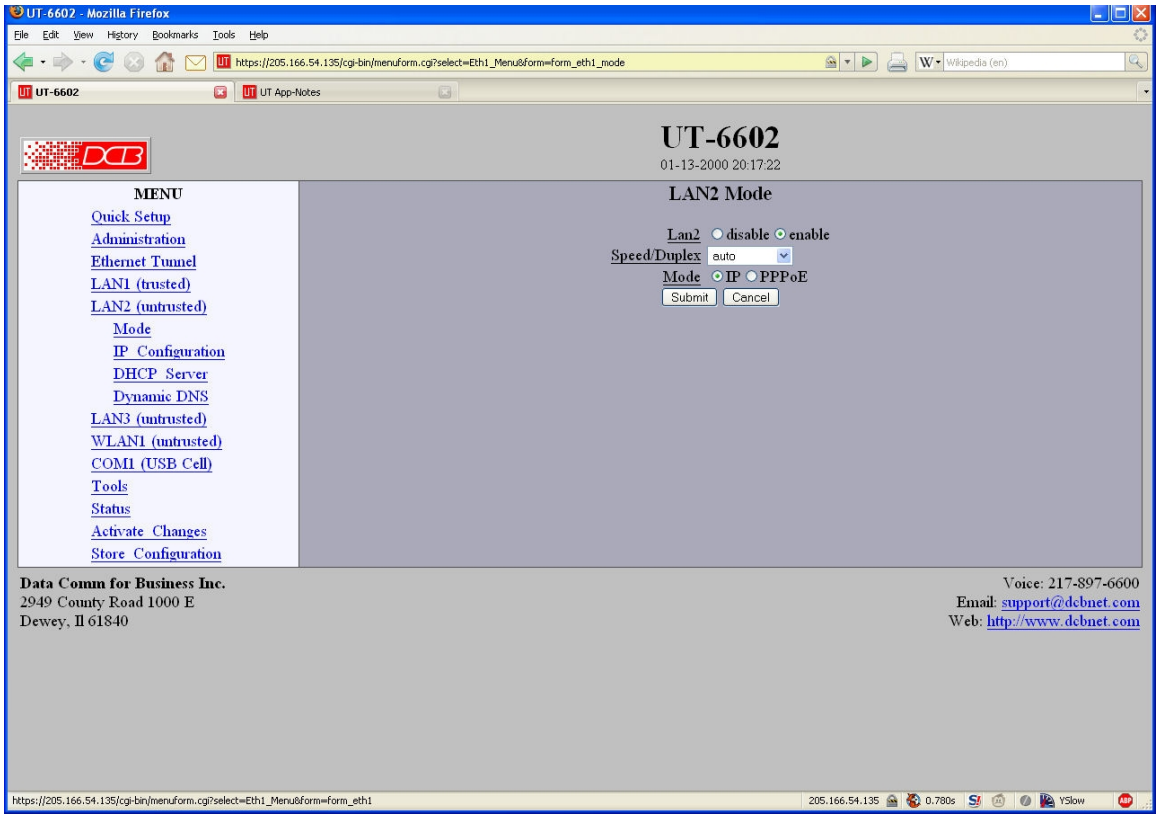
- **URL**
  HTTP url to access when the associated interface is enabled. The url must be in the form of:
  http://www.somewebsite.com/subdirectory?optionalparms
  If the service uses a port number other than 80, you may append the port number following the hostname. For example:
  http://www.somewebsite.com:8000/subdirectory?optionalparms.
  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}

LAN 2 Mode



LAN 2 Mode Screen

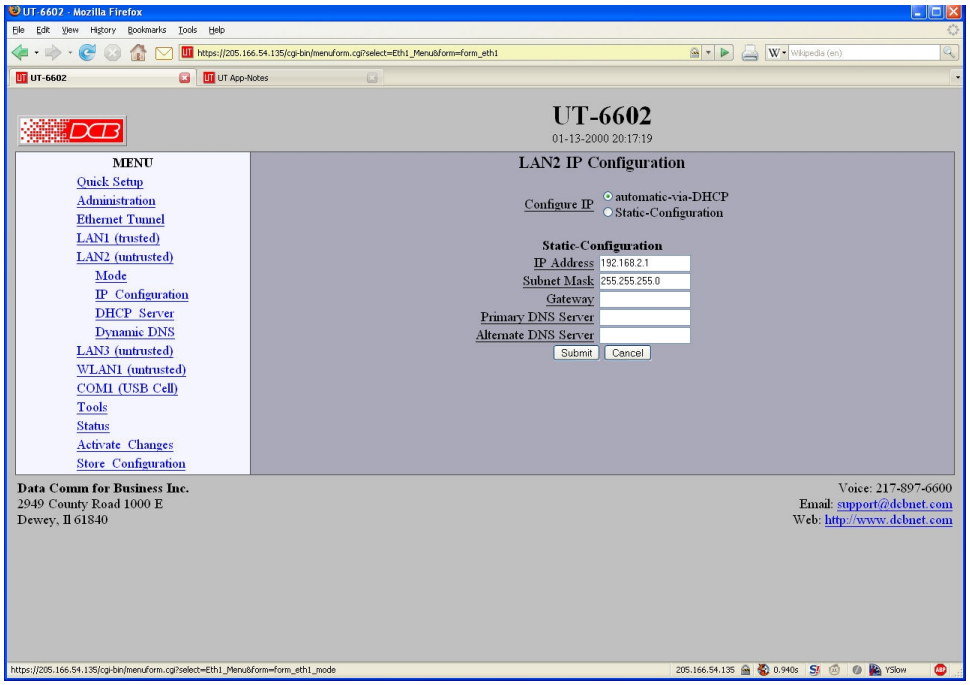
The UT contains multiple Ethernet interfaces.

There is an Ethernet Mode screen, used to select the mode for each ethernet port The Mode screen for Ethernet A is limited to enabling the port, and selecting the port speed. Other interfaces are capable of PPPoE, and theirs mode screen contains additional information. See the Ethernet PPPoE configuration screen section for information pertaining to PPPoE.

Fields

- Enable / Disable
  This should always be set to enable.
- Mode
  Select AUTO, 10 Mbps half duplex, or 100 Mbps half duplex.. Select the appropriate one for this interface.
- Maximum Transmit Unit
  This selects the maximum transmit unit for the ethernet interface. Outgoing network packets will be limited to the specified size. The value may be between 128 to 1500. If blank, the interface default will be used which is 1500.

LAN 2 IP Configuration



LAN 2 Configuration Screen

The UT contains multiple Ethernet interfaces. The LAN2 interface is used for the “WAN” untrusted connection. LAN 1 is always a local, secure side of the tunnel. The other interface is always the insecure side, and is usually used with a broadband WAN or public Internet connection. This screen is used to configure IP parameters for LAN 2 .

Some installations may use PPPOE on this interfaces. On those installations, there is Ethernet Mode screen, used to select the mode for PPPOE . See the Ethernet PPPOE configuration screen section for information pertaining to PPPOE.

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.

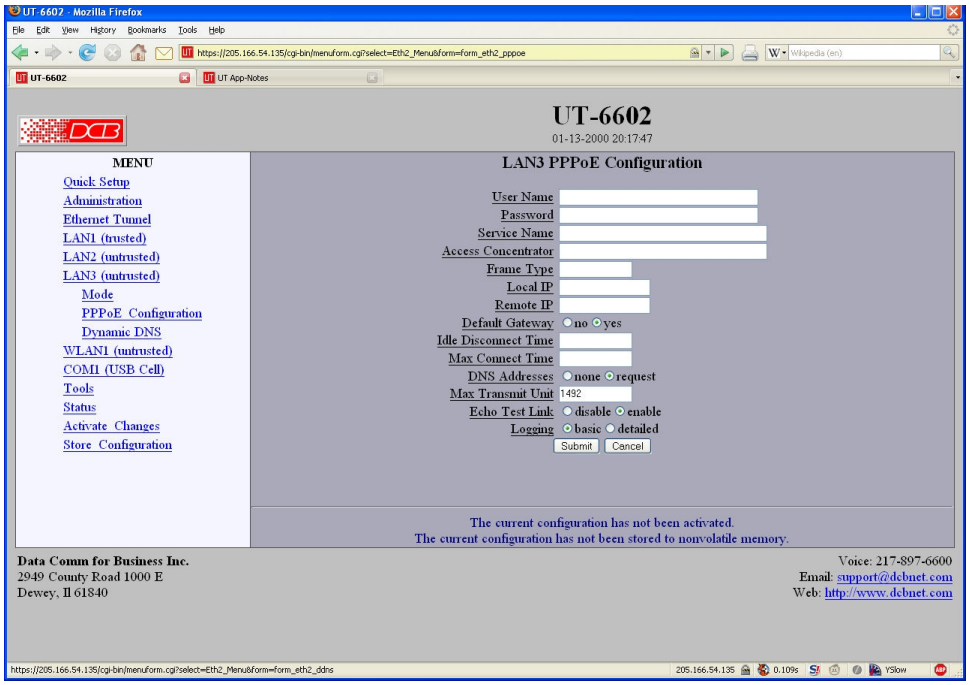
- DHCP Server Settings
  If this unit is to be a DHCP server, the low and high limits for assigned addresses and default gateway must be entered in this section.

- 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.

LAN 2 PPPoE Configuration



PPPoE Configuration Screen

PPPoE is available on the LAN 2 interface. This screen is only available for those interfaces that have the mode configured to PPPoE.

Fields

- 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.
- Frame 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 UT 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 UT will request DNS addresses from the PPPoE Server during PPP option negotiation. When set to *none*, the local UT will not request DNS addresses, and will use the static DNS configuration.

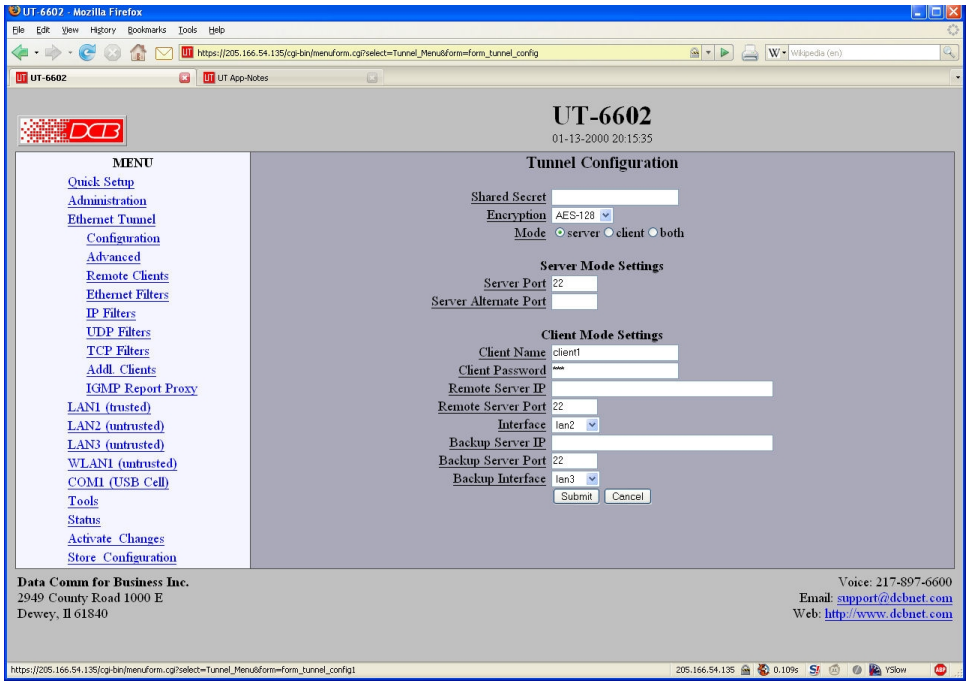
- MTU
  This selects the maximum transmit unit and maximum receive unit for the PPPoE interface. Outgoing network packets will be limited to the specified size. The peer will be asked to limit its MTU to this size. The peer may negotiate a smaller size. The value may be between 128 to 1500. For PPPoE,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



Ethernet Tunnel Configuration Screen

Fields

Shared Secret
The shared secret provides the initial level of privacy. All tunnels participating in the private network must have the same shared secret. This secret phrase is used to generate the 128-bit AES key used to cypher the initial communications. The secret phrase may be up to 52 characters in length. Do not use a quote or backslash character in the phrase. Best security requires a long, random shared secret.

Encryption
This options selects the encryption method for data passed between the tunnels. Encryption is available in 128 but, 192 bit, or 256 Bit AES. AES, also known as Rijndael, is a NIST approved encryption method. "None" disables encryption and is used for greatest throughput when encryption security isn't required.

Mode

Server, Client, or Both. Select the mode for this unit. It is permissible for a tunnel to be both a server and client simultaneously.

Server Mode Settings:

Server Port

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

Server Alternate Port

The server may be configured use a second UDP port. This is optional. When used, the client tunnels may be configured to use either server port. The purpose of this option is to allow an alternate connection path through a router with multiple network up-links. The port number may then be used to differentiate the path.

Client Mode Settings:

Client Name

This is the client name sent to the server tunnel when authenticating. The server must have a matching name in the table of Authorized Remote Clients. The client name may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

Client Password

This is the client password used to authenticate the client to the server. The server must have a matching password in its table of Authorized Remote Clients. The password may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

Remote Server IP

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

Remote Server Port

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

Interface

TSelects network interface to use when connecting to the server.

Backup Server IP

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

Backup Server Port

The UDP/IP port on the backup server tunnel to connect.

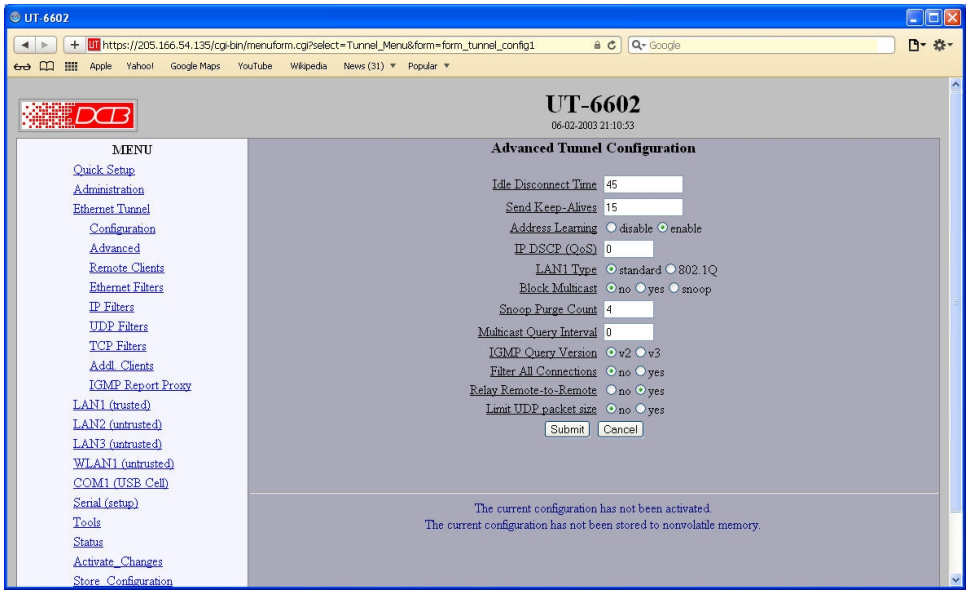
Interface

TSelects network interface to use when connecting to the server.

Notes

The UT 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 UTs, 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 UDP/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.

IPDSCP (Differentiated Services Codepoint)
This option allows you to set the Differentiated Services Codepoint (DSCP) Field in the IP header of the tunnel's UDP packets. A value of zero select the default behavior. Any value between 0 and 63 is allowed. Interpretation of DSCP and its effect on Quality of Service (QoS) is dependent upon the network infrastructure.

Limit UDP Packet Size

When set to *yes*, the local tunnel will limit the size of UDP packets sent out the untrusted interface to 1412 bytes, not including IP and Ethernet headers. Limiting the packet size will eliminate IP fragmentation on Ethernet networks with a MTU of 1500 bytes. This may be necessary when routing through a firewall that will not pass IP fragments.

If this feature is enabled, all UT devices must be running firmware version 1.04 or later.

LAN 1 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.

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.

Snoop Purge Count

This option only applies when IGMP snooping is enabled. Hosts that do not respond to an IGMP query will eventually be purged from the IGMP snooping table. This option sets the number of missed reports required before purging an entry. The snoop purge count should be 3 or larger.

IGMP Query Version

This option only applies when IGMP snooping is enabled and/or the Multicast Query Interval is non zero. This option sets the version of IGMP to use for query messages. However if a multicast router is detected on the network, the tunnel will mimic the multicast router's IGMP version.

Multicast Query Interval

A value of 0 disables the feature. A non-zero value enables periodic sending of IGMP query messages and sets the IGMP query interval, in seconds. 125 seconds is the typical IGMP query interval.

When the tunnel is performing IGMP snooping, it is reading IGMP reports to determine where multicast traffic should be forwarded. A host computer will send an IGMP report when it wishes to receive (join) or stop receiving (leave) a channel. However, IGMP is an unreliable protocol and it is possible for an IGMP report to be missed. To compensate for this, a multicast router will periodically send an IGMP Query message causing the hosts to report the channels they are receiving. If your network does not have a multicast router, then you should configure the tunnel to send IGMP Query messages.

There should only be one IGMP querier on a network. If your network has a multicast router, you should not enable the Multicast Query Interval in the tunnel. If you need the tunnel to provide backup, in the event the multicast router is down, set the Multicast Query Interval to a time larger than the Query Interval time configured in the router. Most routers default to 125 seconds.

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.

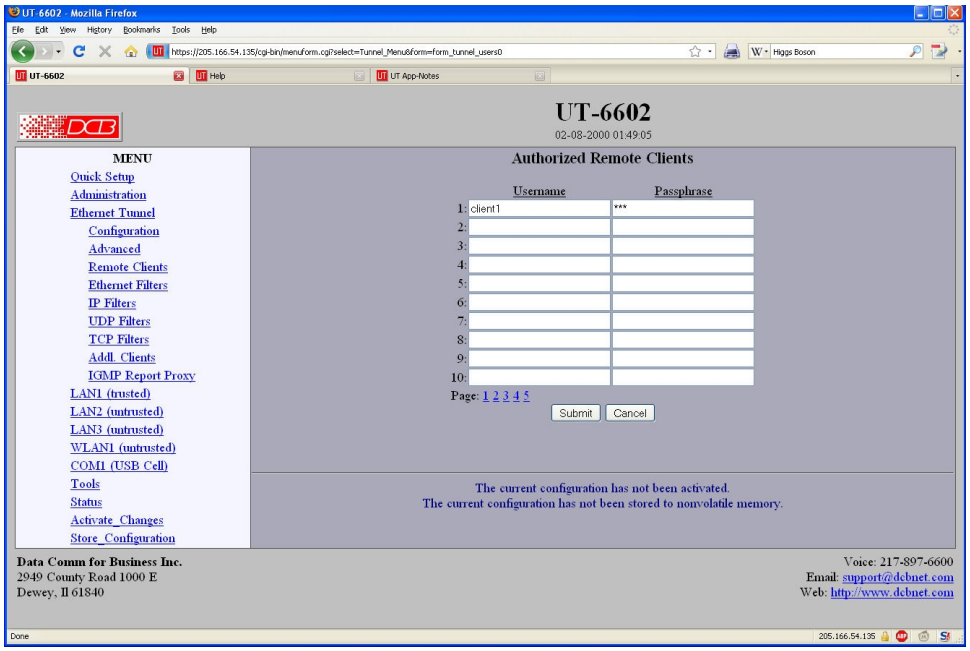
Important note, setting this feature to yes will eliminate the ability to have a service enabled at one endpoint while blocking that service in the opposite direction. The service is effectively disabled in all directions.

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.

Notes

Remote Clients Screen



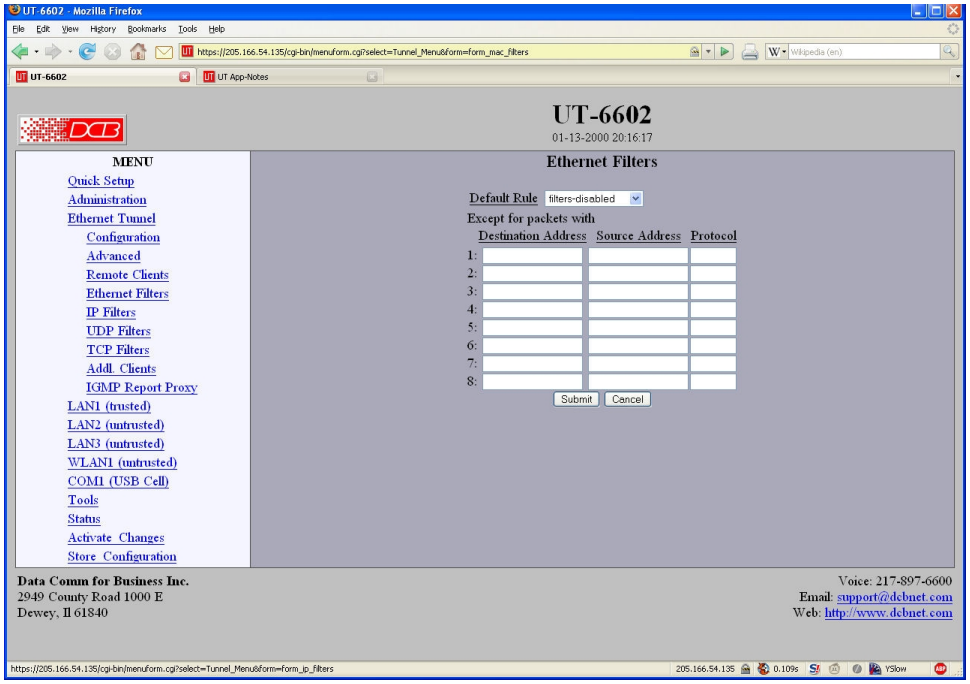
Remote Clients Screen

This table specifies the names and passwords for remote Tunnel clients. It is used by the Server Tunnel to authenticate Client Tunnels. There may be 100 remote clients configured.

Fields

- Client Name
  The name 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. .
- Client Password
  AThe password 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.

Ethernet (MAC) Address Filters Screen



Ethernet 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.

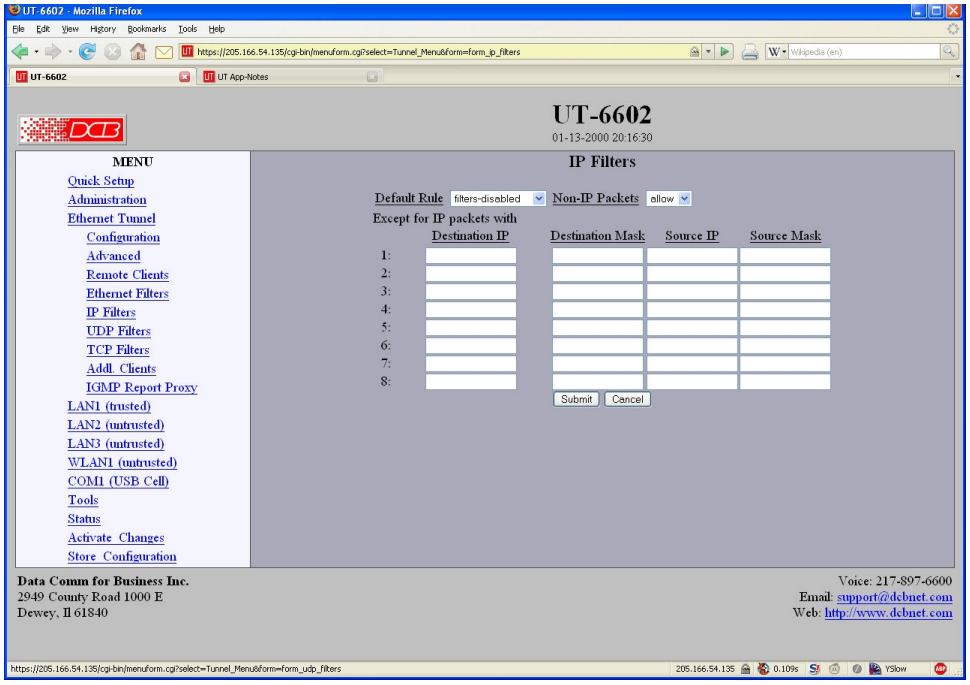
Fields

- 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 UT's internal web server through the associated interface filters.

IP Address Filters Screen



IP 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 of 0.0.0.0 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

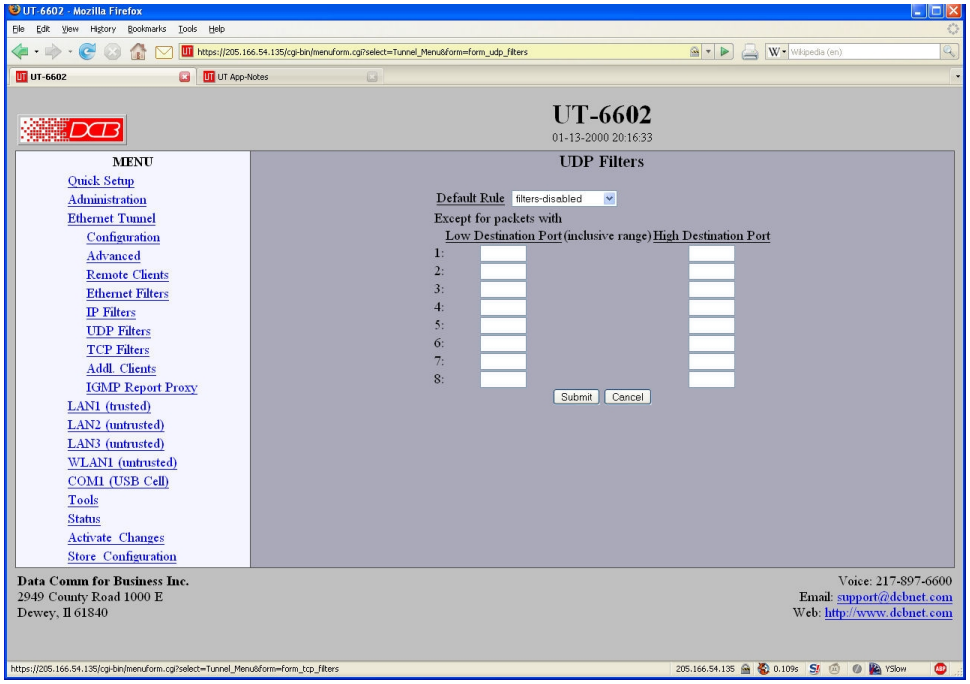
Please note that IP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

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 Port 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.

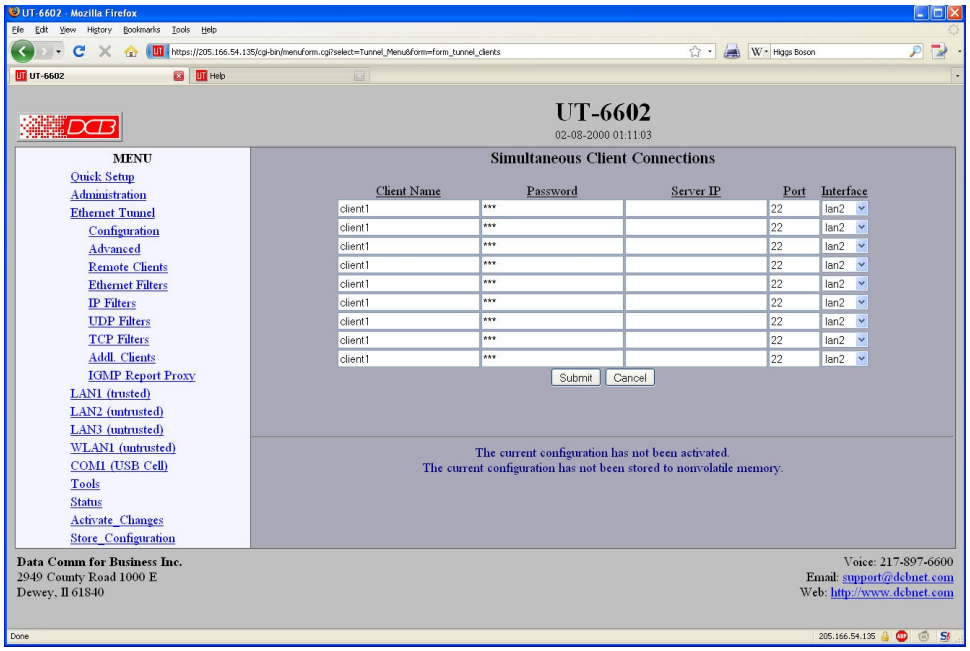
- High Destination Port
  This field specifies the High Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.

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.

Additional Clients



Additional Clients Configuration Screen

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

Fields

Client name
This is the client name sent to the server tunnel when authenticating. The server must have a matching name in the table of Authorized Remote Clients. The client name may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

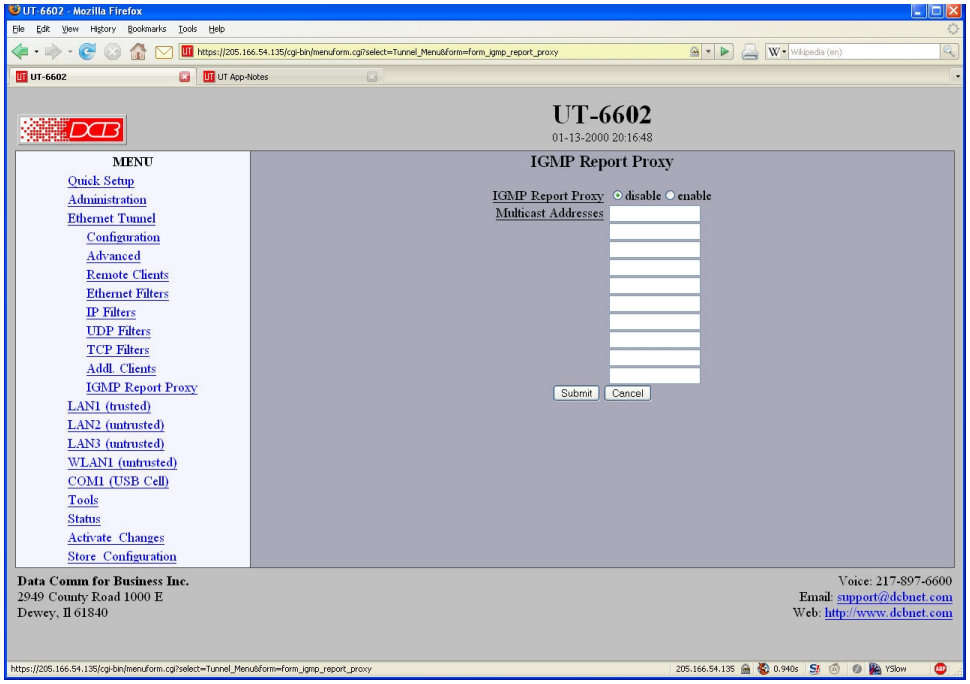
User Password
This is the client password used to authenticate the client to the server. The server must have a matching password in its table of Authorized Remote Clients. The password may be up to 52 characters in length. Do not use a quote or backslash character in the phrase.

Server IP
The hostname or IP address of the server tunnel.

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

Notes

IGMP Report Proxy



IGMP Report Proxy Configuration Screen

IGMP snooping and protocols such as PIM rely on IGMP reports to build their forwarding tables. However some multicast receivers do not fully implement IGMP, resulting in the multicast packets not reaching the physical network segment. To work around this problem the tunnel can be configured to "join" a set of multicast channels. It will then generate the proper IGMP reports.

IGMP Report Proxy should be enabled in the tunnel on the same physical LAN as the multicast receiver.

IGMP Report Proxy will not correct a situation where an IGMP snooping Ethernet switch is placed between the tunnel and the multicast receiver. IGMP snooping will need to be disabled in the Ethernet switch.

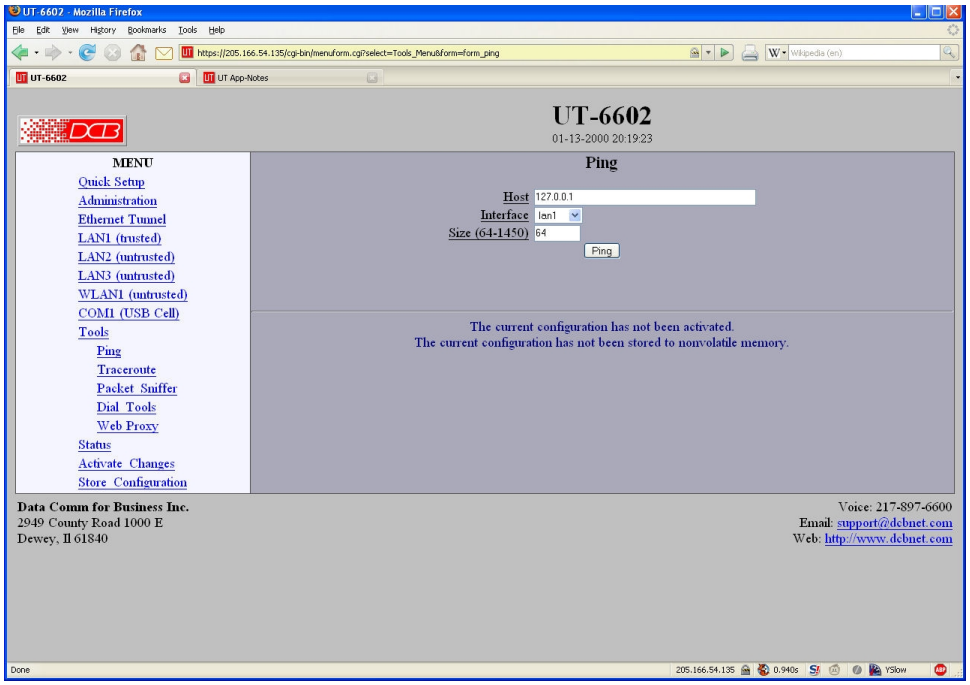
Fields

IGMP Report Proxy
This Enables or disables IGMP Report Proxy

Multicast Addresses
This is list of multicast addresses to join.

Notes

Ping Screen



Ping Screen

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

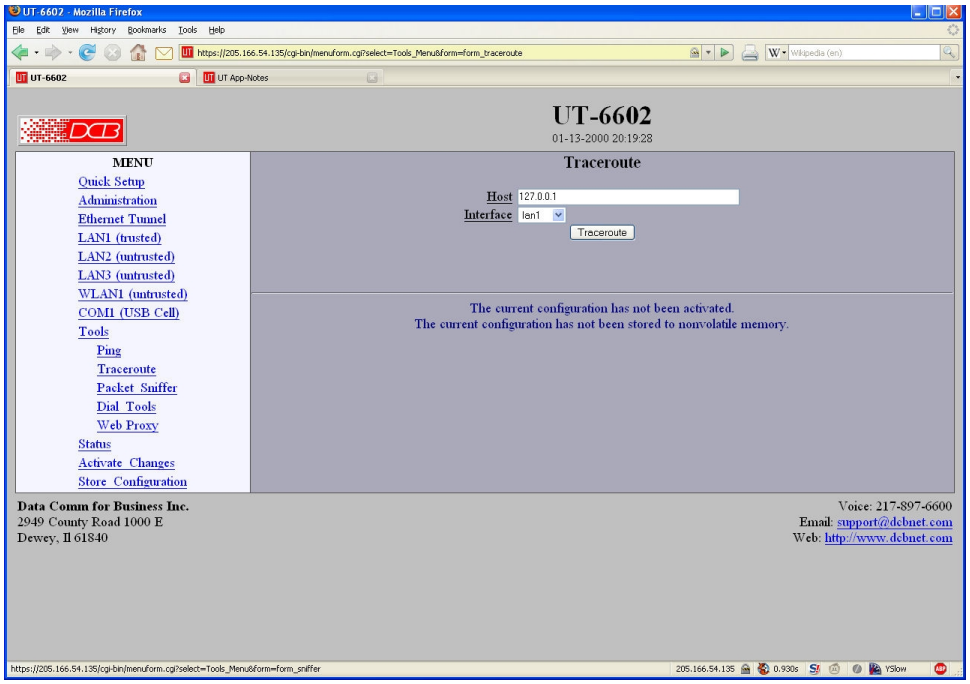
Fields

- Host
  IP address of the target host. If hostname DNS is enabled, you may use a host name.
- Interface
  Which interface to use. This controls the default gateway to be chosen in the event the target host is not on a local network segment.
- Size
  Number of data bytes to send.

Notes

- Ping and traceroute are useful tools to determine if routing is correct.

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

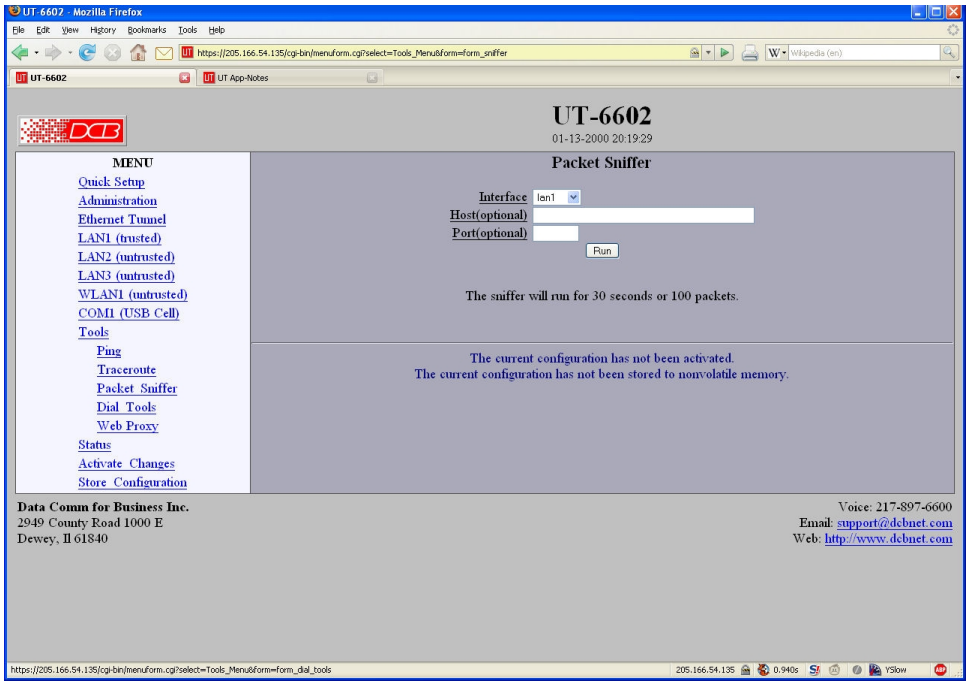
Host

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.

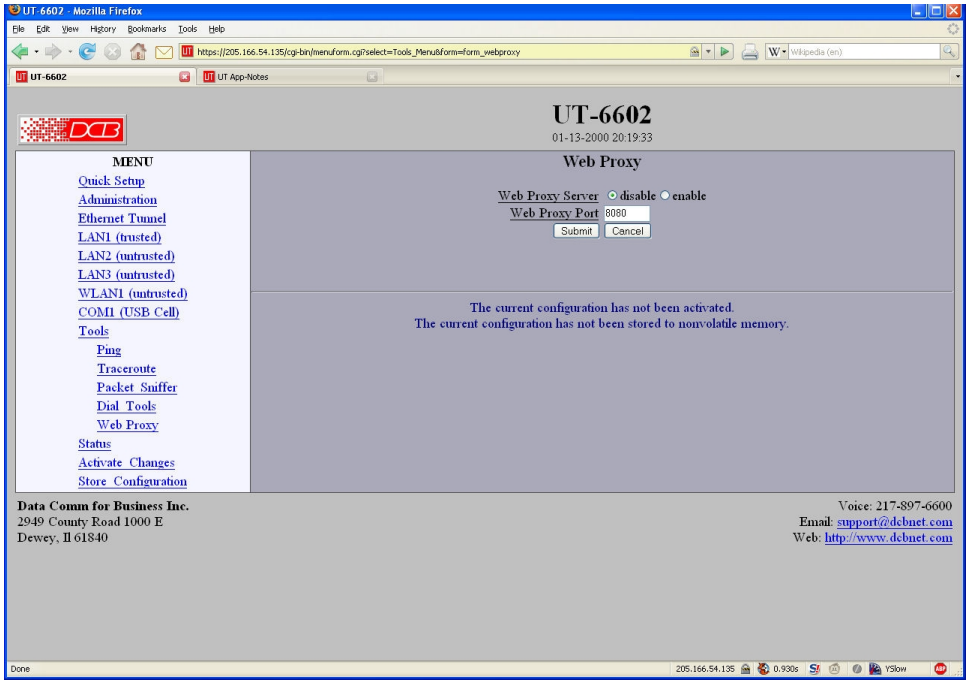
Fields

- 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.

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

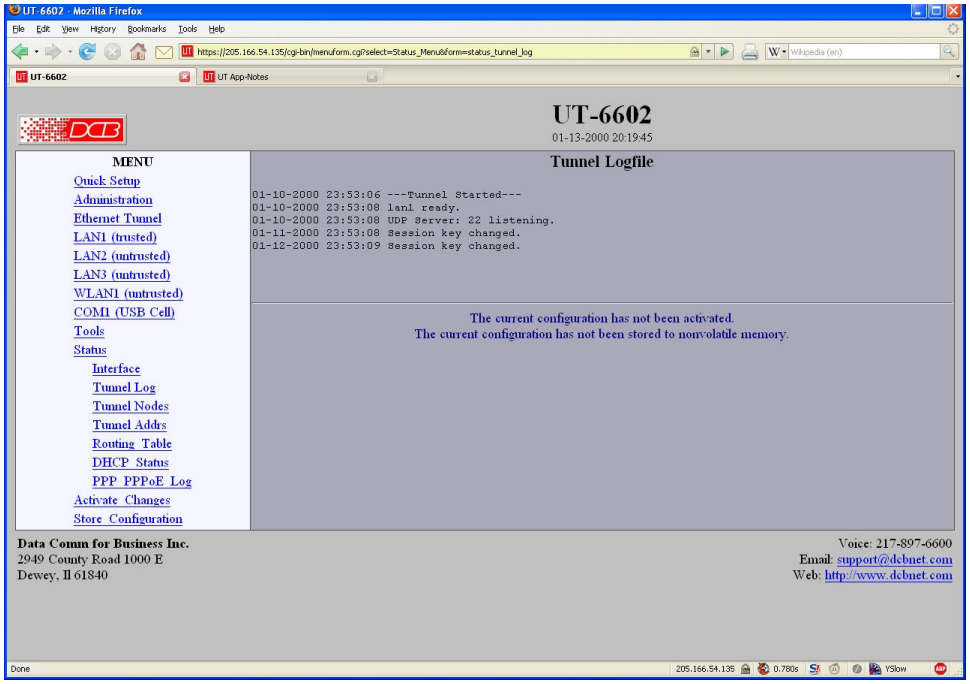
set the IP address and port number. Use the IP address of the Ethernet-A interface as the proxy server address.

Interface Status Screen

Status Screen

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

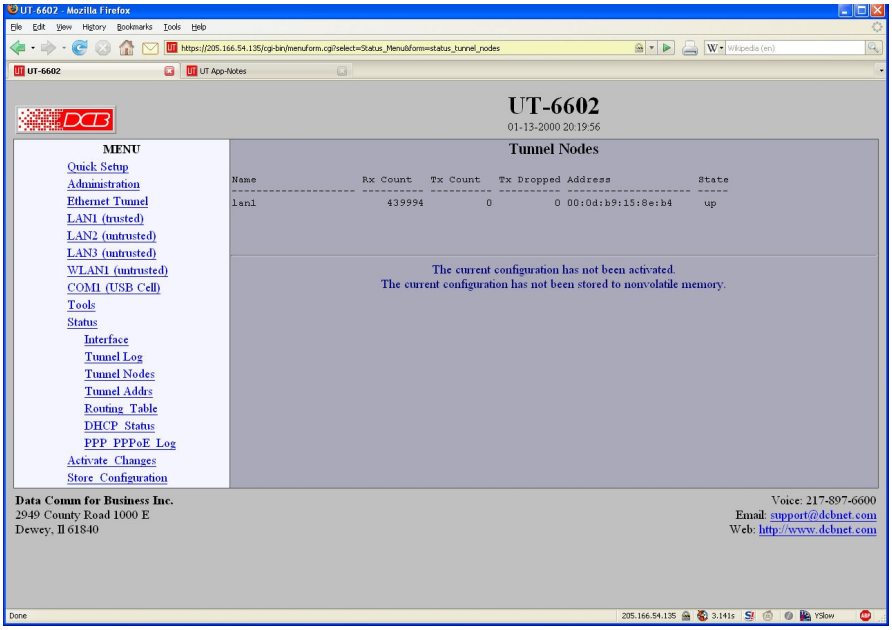
Tunnel Log Screen



Tunnel Log Screen

The Tunnel Log screen shows important events logged for each interface on the UT.

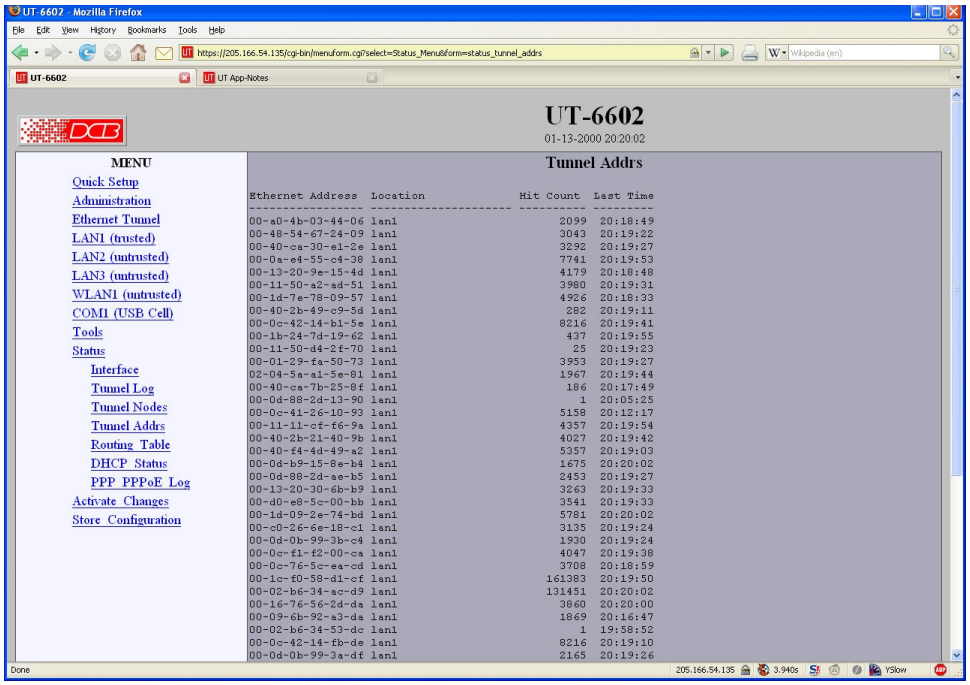
Tunnel Nodes Screen



Tunnel Nodes Screen

The Tunnel Nodes screen shows the status of known remote UT nodes. Status is indicated by the state being UP, connecting, or connected.

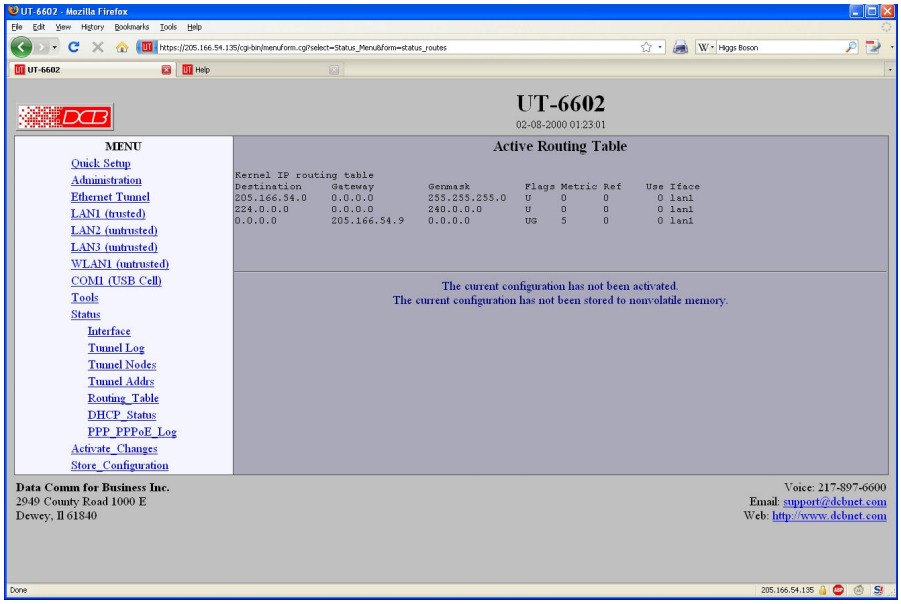
Tunnel Addresses Screen



Tunnel Addresses Screen

The Tunnel Addresses screen shows the ethernet (MAC) address of all ethernet nodes recognized along with their port location, hit count, and time of last contact.

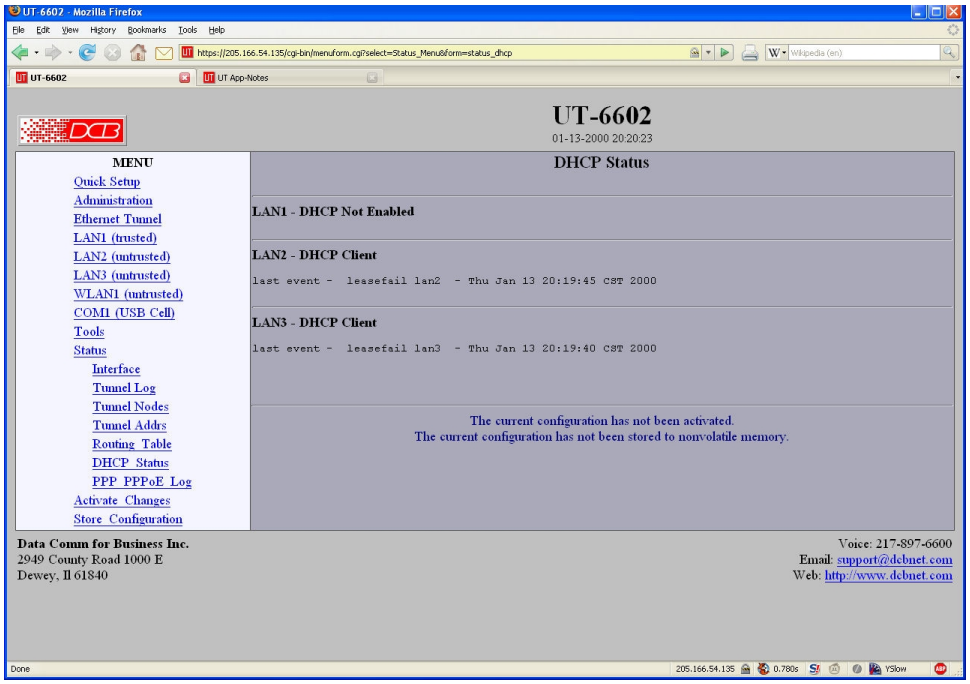
Routing Table Screen



Routing Table Screen

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

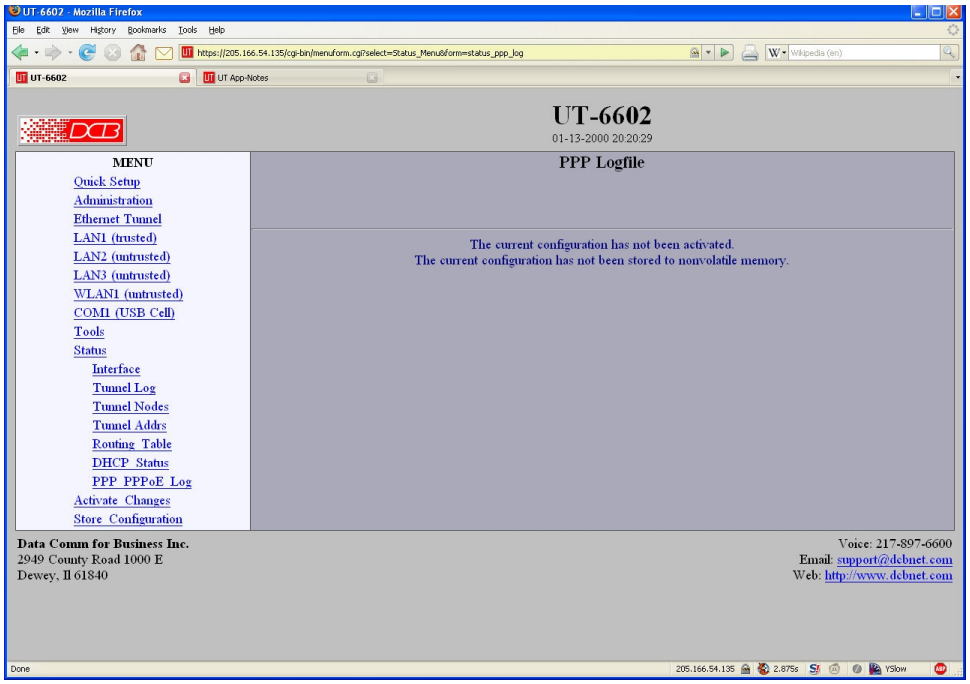
DHCP Status Screen



DHCP Status Screen

The DHCP Status Screen displays recent history of DHCP server activity.

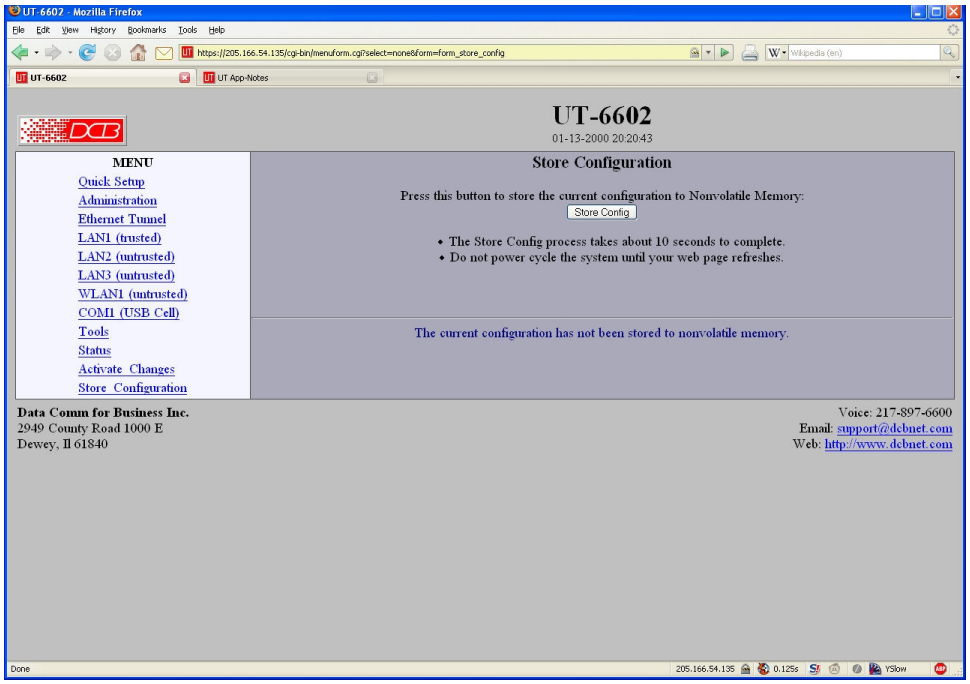
PPPOE Log Screen



PPPOE Log Screen

The PPP Log Screen displays recent history of PPPoE operation.

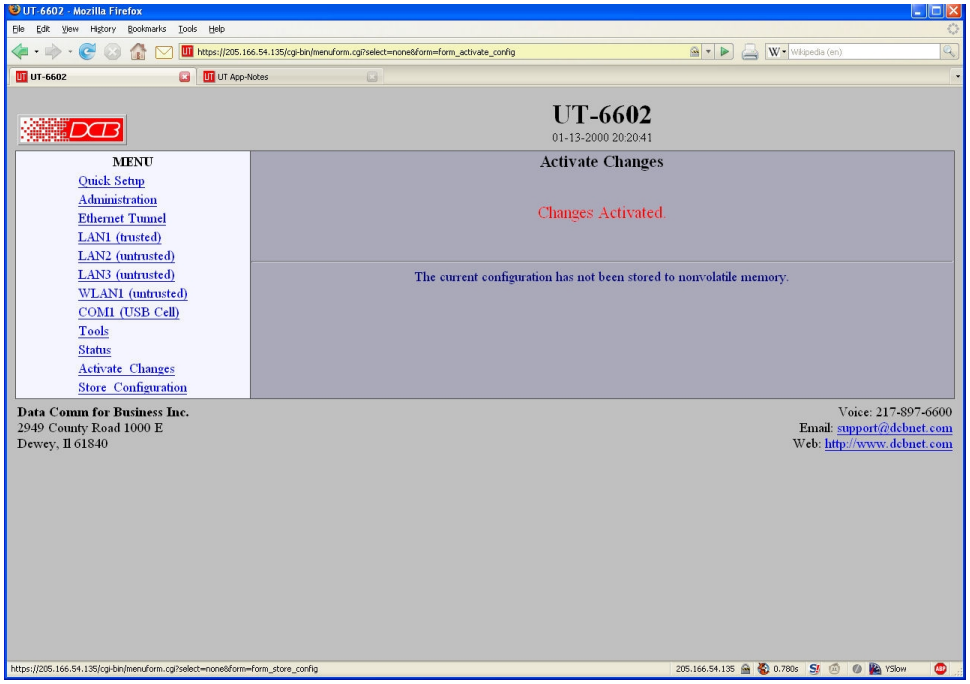
Store Configuration Screen



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. **Refer to the configuration process section for details about the configuration process.**

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.

Chapter 5
Operation

This Chapter explains how to use the UT, 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 broadband ISP Internet connection
- Remote LAN connected to local LAN via wireless Internet connection
- Multiple remote LANs connected together using various ad-hoc ethernet connections

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 UT units is via UDP/IP, therefore a TCP path is required between the UT units.

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 ethernet device using an ethernet cross-over cable.

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

Remote LAN to Local LAN via Broadband Internet

The server UT is connected to the host remote LAN and eventually connected to the Internet via some ISP. The remote client UT is connected to a broadband router via Ethernet B, and a local LAN is connected to Ethernet A. All ethernet devices on the local LAN are bridged to the remote LAN. Filtering may be used to limit connectivity to the desired ethernet devices.

Remote LAN to Local LAN via Wireless Internet

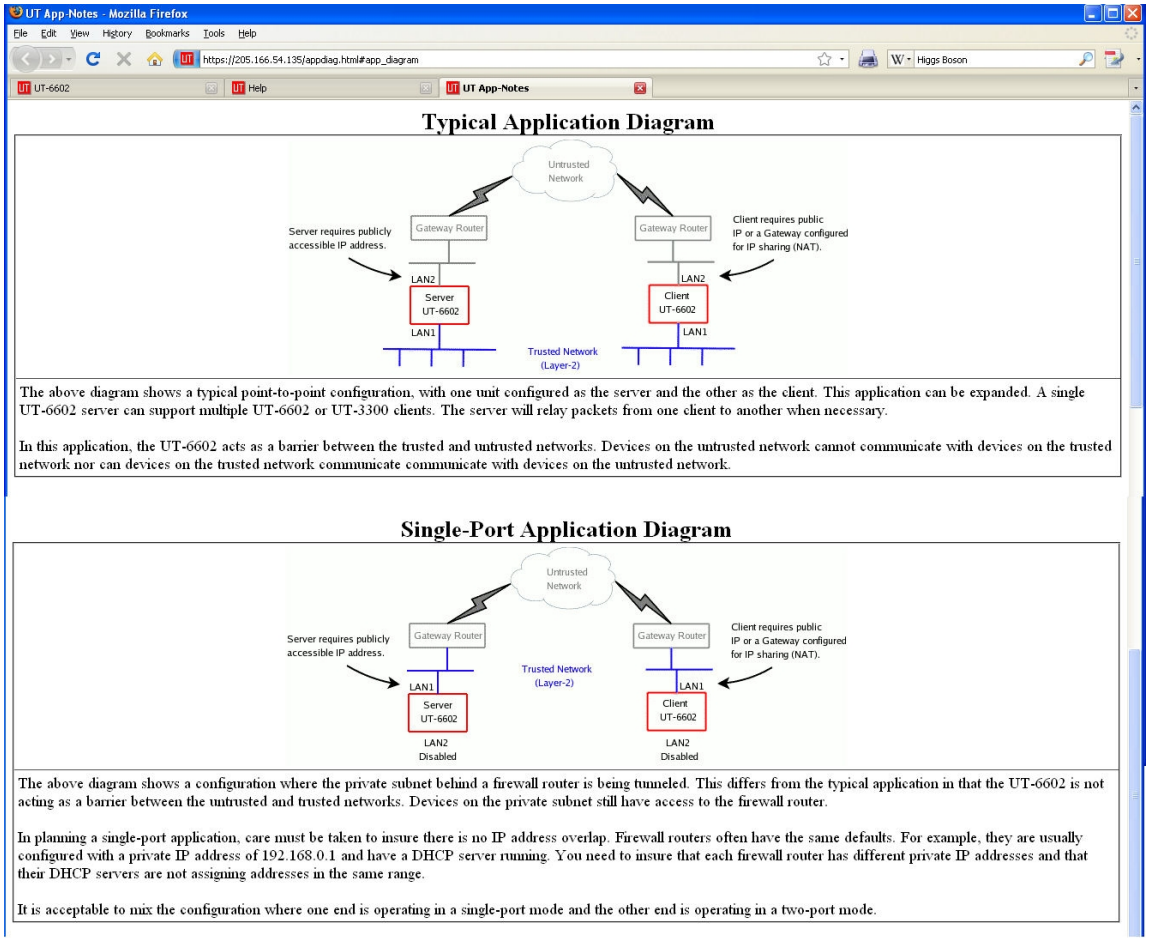
Similar to the above configuration, but a wireless ethernet device is used in the public Internet connection path.

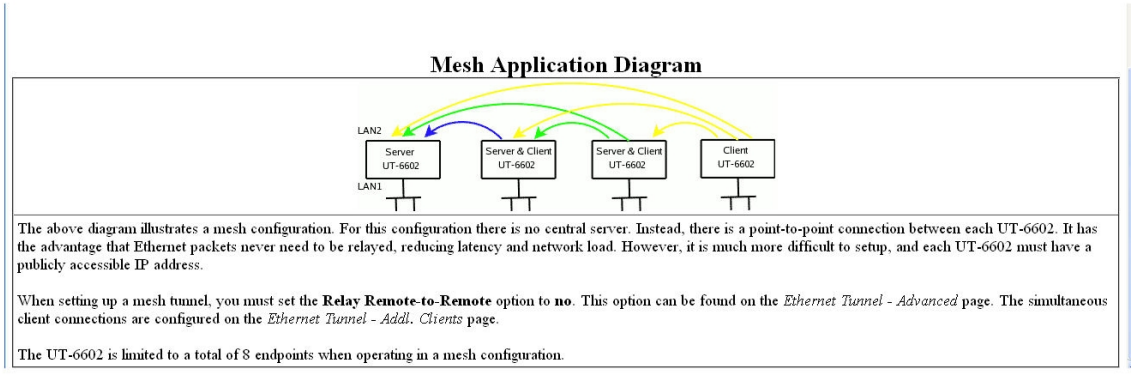
Remote LAN to Local LAN via Ad-hoc connections

As in the above configurations, except there are multiple UT-3300 remote locations that are used “ad-hoc”, and with DHCP providing local IP configuration and the path back to the host UT.

Typical Application Diagrams

This diagram may be displayed by pressing the “Press here for application diagrams” link on the Quick Setup Screen.





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.

Can't Connect via the LAN

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

- Insure that you are addressing the UT 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, by typing the following command at the command prompt or *Run* dialog box.: `ARP * -d` **. This is a common problem with test-bench setups.**
- Check that you are using the proper Ethernet connection on the bridge. Only Ethernet Port A works at 100BaseT, 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.
- Hold the configuration button depressed for at least 3 or 4 seconds.
- 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.

***P*:** How to set the bridge back to factory defaults?
S: 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 .

***P*:** How do I regain administrative use of the serial port?
S: The serial port is always active as a configuration port.

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 on the trusted side of ALL bridges in the system should be in the same IP subnet address range.

Appendix A

Specifications

EtherSeries UT-6630 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense X2
- USB Interface: (one optional) USB for certificate transfer
- Serial Port (1) RS-232 port for setup
- OS: linux
- CPU: Dual Core 32 bit or higher performance processor
- Memory: 2Gig or more RAM
- Throughput: Greater than 260 Mbps with AES, greater with encryption disabled
- Supports 100 simultaneous client UTs
- Bridge/Tunnel supports 4096 MAC address table entries
- Power: 120 VAC ~260 watts
- LED: Over-temperature warning, LAN Activity, LAN status (two per interface), Power
- Default LAN 1 IP address: 192.168.0.1
- Default LAN 2 IP addresses: DHCP Client
- Browser Management port: 443 (HTTPS)
- Operational Temperature: Office environment
- Dimensions 1U high rack chassis

Cables

Commonly used cable connections:

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 or equivalent without using a hub.

Use the following pinout to build an ethernet crossover cable:

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

Appendix B

Open Source Software Information

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

Introduction

Some models of the bridge were designed and programmed with Open Source Linux software in mind. 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

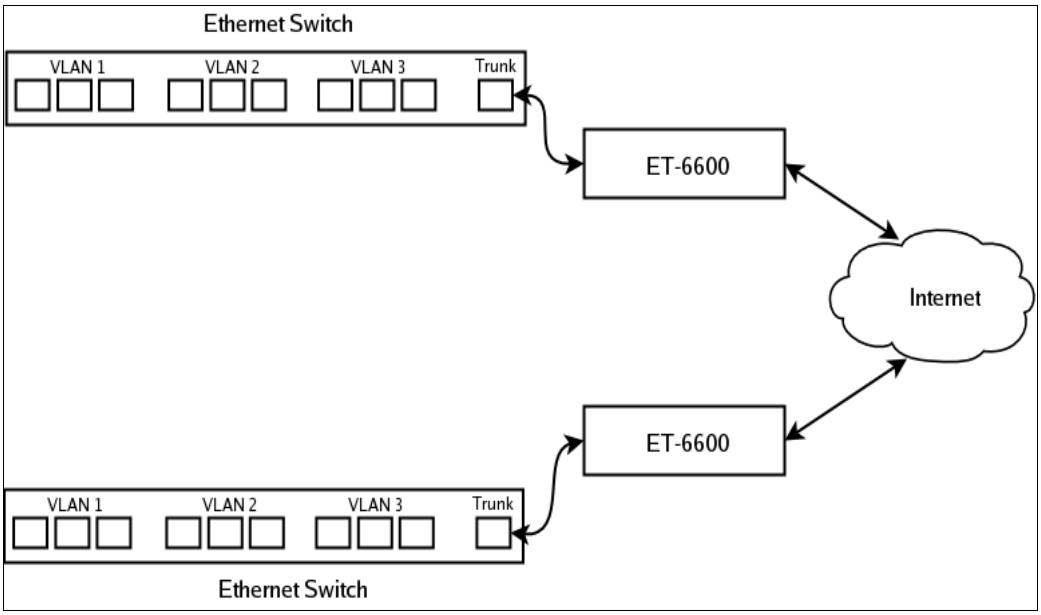
Appendix C

802.1Q VLAN Tagging

The UT family supports bridging of 802.1Q VLAN packets.

Introduction

Firmware versions 1. and later for the UT 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 UT 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 UT from the VLAN that you specified. In other words, if you set the VLAN ID to 2, you will be able to access the UT 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 UT 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 UT, as it's seeing the ethernet port as a trunk port.