FT-Series

Encrypted Ethernet Tunnel

User's Guide

Revised April 29, 2010

Firmware Version 1.x

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.

Copyright © 2009, 2010 All rights reserved.

Version 1.0x

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

RoHS

Some models of this product is available in RoHS versions.

TABLE OF CONTENTS

Chapter 1
Introduction

This chapter provides an overview of the EtherSeries FT-6602 Ethernet Tunnel Bridge's features and capabilities.

Congratulations on the purchase of your new EtherSeries FT-6602 Encrypted Ethernet Bridge. This is a simple, easily configured tunneling device containing three Ethernet interfaces.

Two or more bridges connect using standard TCP/IP using any insecure IP connection path. They tunnel all Ethernet packets from the secure interface of each device to the other devices using a FIPS certified encryption module and AES encryption.

The bridge transports all valid Ethernet protocols. It provides a virtual private network by bridging the LANs with an IP tunnel that may be encrypted using the AES algorithm. 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.

The FT-6602 includes the ability to create self-signed certificates. The certificate authority is stored on a USB dongle, that allows the certificates to be shared between FT-6602 devices as well as web browsers used for configuration.

EtherSeries FT-6602 Applications

The FT-6602 connects multiple LAN segments by using standard IP protocols between the bridges. It is commonly used to connect a remote LAN to a central LAN. In this application, the bridges connect via any valid TCP/IP path, negotiate an encrypted link, and then bridge all non-filtered 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.

In some applications, the FT-6602 is used to provide a path for multi-cast IP packets over a network not designed for multi-casting. This is common for radio dispatch and VOIP applications.

Other Features

Protocols

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

DHCP Protocol

The bridge supports the DHCP protocol as a client or server. DHCP may be served through the tunnelled link.

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 most web browsers. Internet Explorer Version 7 and newer or the latest Firefox versions (version 2 or newer) are recommended. Older versions of web browsers may fail due to TLS negotiation.

Security and Firewall Features

The bridge supports a number of security features. On the "insecure" side, all traffic is encrypted, including the FT to FT negotiation. The encryption methodology is industry-standard AES using a FIPS certified encryption module. It may be configured so only workstations on the "secure" side of a unit may be used to configure or control it, and certificates may be required..

On-board Tools

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

Single-Interface operation

The FT-6602 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 bridge:

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

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

Software Requirements

The bridge supports IP and associated protocols such as UDP, ICMP, PPPoE, 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.

A standard web browser (Internet Explorer Version 7 and newer or Firefox Version 2 or newer) are recommended.) may be used for configuration once the bridge is configured with a valid IP address. Older

versions of web browsers often fail due to TLS negotiation. The use of a secure web browser connection for configuration (HTTPS://) is required.

FT-6602 Specific

The FT-6600 family consists of various models with different internal hardware or firmware options. The FT-6602 includes three ethernet ports .

Introduction

The FT-6602 model bridge contains three ethernet interfaces. It is often connected directly to an Ethernet WAN connection using a public high speed network, DSL modem, or Cable modem. This model supports 50 simultaneous remote units with throughput exceeding 10 Mbps.

Configuration Options

This model contains a single serial interface to be used in initial setup (if needed). This serial port is always available for setup. Once a compatible IP address is available, the browser setup screens are much easier to use. A secure web browser connection for configuration (https://) is required.

FT-6602 Front

FT-6602 Rear

FT-6602 Front Panel

The front panel contains a LED indicator for power.

Rear Panel LED Indicators

One set of indicators For Each Ethernet Port

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

Rear Panel USB Connectors

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

Rear Panel RS-232 Connector

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

Rear Panel Ethernet Connectors

The three 10/100BaseT connectors are auto-sensing

Rear Panel USB Connectors

There are two USB connectors. They are interchangeable, and only the first one that senses a USB device connection is activated. These are used only for a "certificate authority" USB memory device.

FT-6630 Specific – Two High Performance Ports

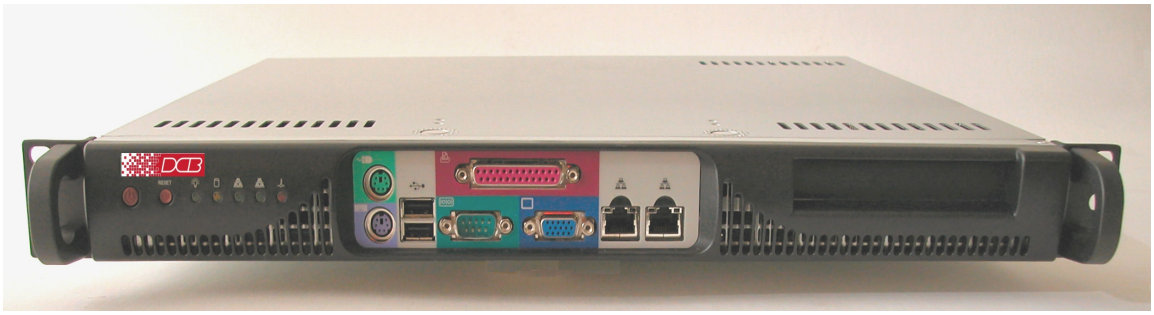
The FT-6600 family consists of various models with different internal hardware or firmware options. The FT-6630 includes two 10/100/1000BaseT High Performance Ethernet ports.

Introduction

The FT-6630 bridge contains two gigabit Ethernet ports and is normally used at the head end to support multiple remote ET products. It is often connected directly to an Ethernet WAN connection using a public high speed network, DSL modem, or Cable modem. This model supports 50 simultaneous remote units 120 Mbps throughput. The configuration is similar to the other FT models with the following changes.

Configuration Differences

This model contains a single serial interface to be used in initial setup (if needed). IF the default IP address is not appropriate for your LAN, then connect a 9-pin serial terminal cable and follow the command line setup instructions. Once a compatible IP address is available, use the browser setup screens . This model requires a secure web browser connection for configuration (https:// IP_Address)



ET-6620

FT-6630 Front Panel

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

FT-6630 Front Panel LED Indicators

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

Chapter 2
Installation

This Chapter details the installation process for the EtherSeries Bridge.

Overview

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

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

The CDROM contains a Quick-Start 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. That same information is in chapter 5 of this manual.

Quick Start

Quick start instructions are in chapter 5. 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.

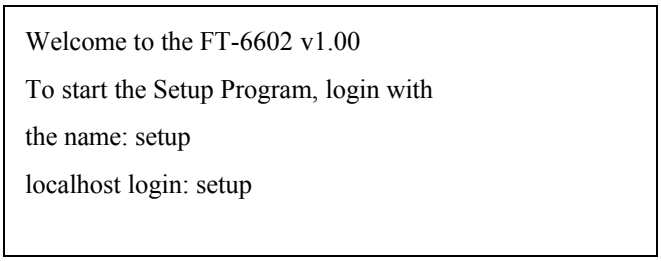
Entries are always tested for valid values. However, there are many "valid" values that are not appropriate for any given configuration. So, "appropriateness" isn't tested. For example, an IP address of 300.400.500.256 will not be accepted, but the field will accept an IP address that is not appropriate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

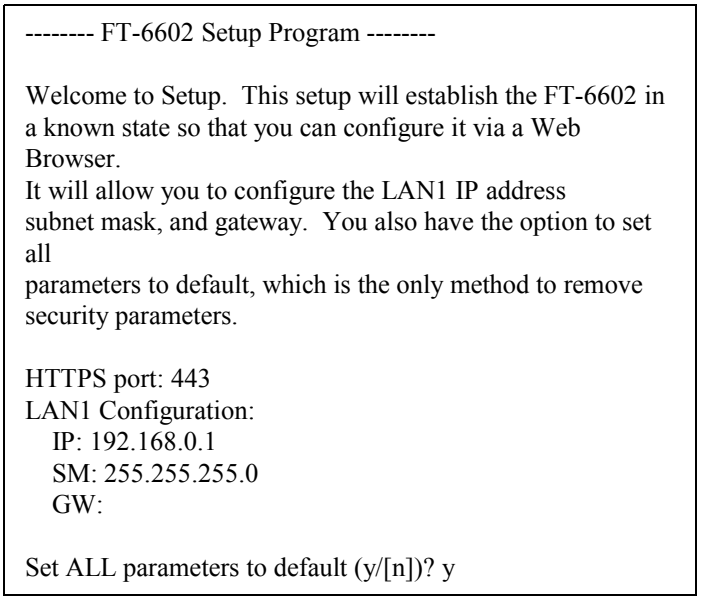
1. Connect a terminal or PC running terminal emulation program (Hyperterm, Procomm, etc) to the serial port of the bridge.
2. Start the terminal emulation program using 9600 bps, 8-bits, No parity, No flow control.
3. Power up the bridge.



Login Screen

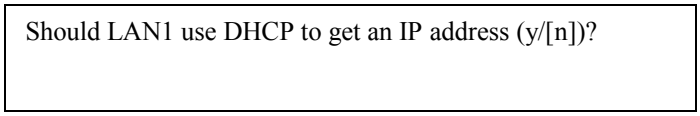
4. The Bridge will reboot pausing at a login screen. For initial setup, enter the login name "setup" in lower case letters. No password is required.

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



Default Screen

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



DHCP Screen

7. If you answered no to that question, you will be prompted to enter the unit's IP address, subnet mask, and gateway. Enter the values for the Ethernet A interface. If it LAN1 is will be connected to an 802.1Q VLAN trunk, enter "Y" for that value, otherwise use the default "N".

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...

Setup complete.

After rebooting the system, you will be able to configure the unit from a Web Browser. Use the URL
https://205.166.54.173
rebooting system.

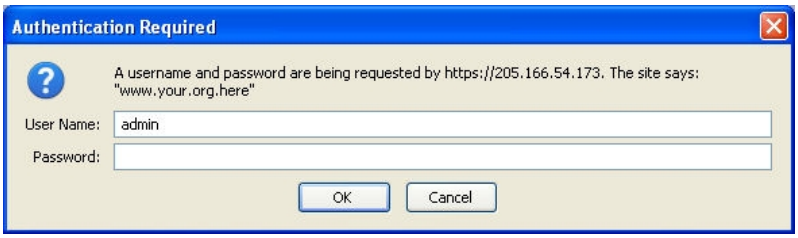
9. The bridge will now reboot.

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 using (https://). If your web browser does not see the bridge, verify that you do not have a proxy server configured in the browser. If so, properly configure the browser to bypass the proxy server for this URL. The bridge's default address is 192.168.0.1. This address must be appropriate for your local LAN and workstation, or step 1 above must be followed.

3. Verify the IP Address Configuration

Enter the URL from step 1 (or http://192.168.0.1 if using the default address) into your web browser. The login screen below should be displayed. A secure web browser connection is required (such as https://192.168.0.1).



Login Screen

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

4. Enter Your Configuration

Initial Main Menu

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

5. Minimum Configuration

The minimum configuration items required for basic LAN-to-LAN bridging are:

1. Secure side ethernet configuration. Configure ethernet LAN 1 (IP address, etc. if not using DHCP).
2. Insecure side ethernet port configuration. The insecure side may use either ethernet port LAN 2 or LAN 3. Default is to use DHCP on Ethernet port LAN 2, and disable the third LAN 3 port..
3. IP Tunnel Configuration. Connect-to Server IP address , port, and LAN interface for client mode, Listen-to port for server mode. Some Advanced Tunnel Configuration may be need.
4. Generate CA key and local key. Then distribute the local key to the remote units via the USB dongle.

Configure these items and the bridge is ready for use. Of course, you need to perform a similar installation for any companion bridge on the additional LANs so it can do useful work. You should also read chapter 5 or the quick-start guide for more detailed instrucitons.

Chapter 3
The Configuration Process

This Chapter describes the configuration management process on the FT-6602 bridge using a Web Browser.

Overview

The FT-6602 bridge contains a quite flexible configuration management system. By using this system correctly, after initial configuration, 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.

NOTE: Internet Explorer Version 7 and newer or Firefox version 2 or newer are recommended. Older versions of web browsers may fail due to TLS negotiation issues.

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

Change, test then save

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.

Change, save, then reset

Make configuration changes, save them with s*ave*, the 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.

Restore with a saved configuration

T**ransfer a saved configuration to the bridge, save it, reset the bridge to activate the new configuration.**

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

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

NOTE: The encryption certificates are stored along with the configuration in an encrypted file.

Note regarding saved configurations

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

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

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

NOTE: The encryption certificates are stored along with the configuration in an encrypted file.

Chapter 4
Configuration

This Chapter describes configuration screens and some configuration hints for the EtherSeries FT-6602 Bridge

Overview

The FT-6602 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, bridging, or routing. Familiarity with IP and related information is required before you can configure any ethernet product. Minimum knowledge of encryption certificates is required.

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.

For best security, configuration screens should be made available only 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. A secure web browser connection is required for configuration (https://)

FT-6602 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.

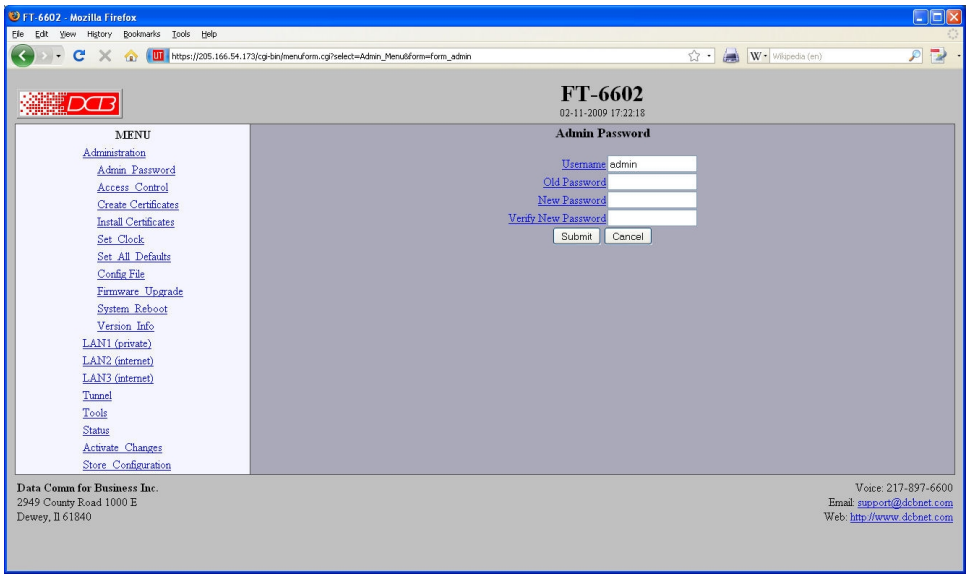
Note that some screens are model specific, and some models do not contain all screens shown.

NOTE: Internet Explorer Version 7 and newer or Firefox version 2 or newer are recommended. Older versions of web browsers may fail due to TLS negotiation issues.

Administration

The Administration section contains screens used to configure system-wide settings and perform a few high level operations. Menu options are Admin Password, Access Control, Make Certificates, Install Certificates, Set Clock, Set All Defaults, Config File, Firmware Upgrade, System Reboot, and Version Info.

Admin Password



Admin Password Screen

The FT-6602 web server screens are available ONLY via the secure side of the bridge.

Access to the FT-6602 Web Server is protected requires a secure web browser using https:// .

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.

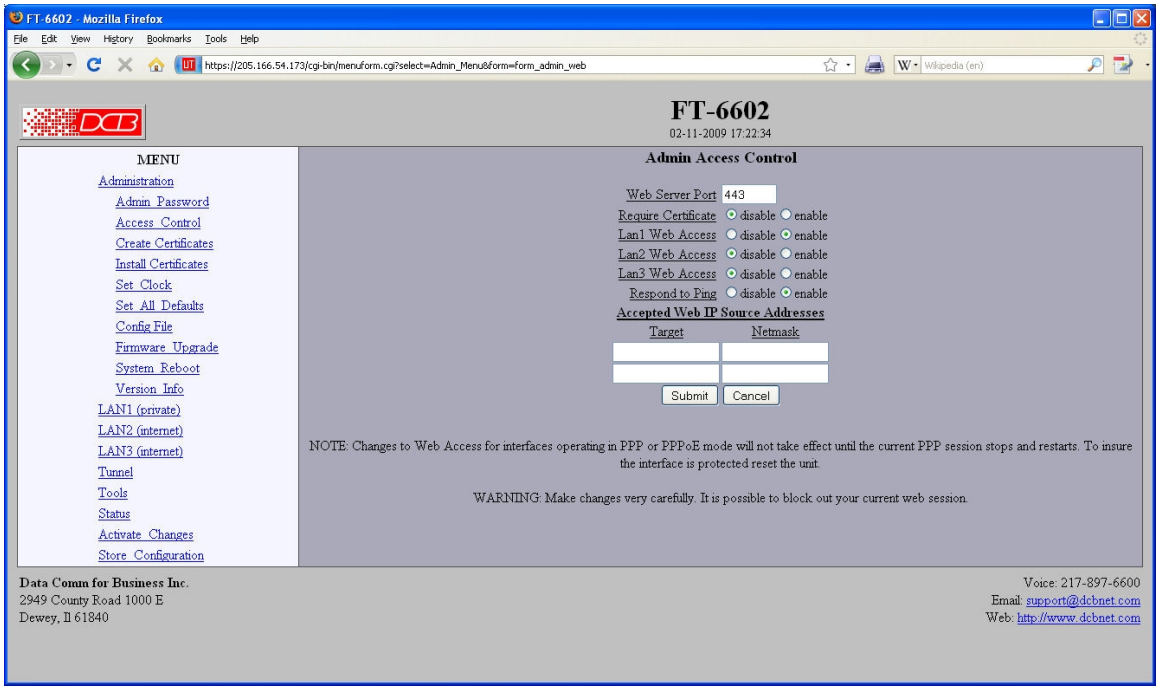
Fields

- 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. The default is admin .
- 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. The default is a blank 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.
- **THERE IS NO WAY TO RECOVER THIS USER NAME AND PASSWORD IF YOU LOSE IT.**

Admin Access Control



Administrative Access Control Screen

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

Fields

- Web Server Port
  This is the TCP Port to use for the FT's internal Web Server. Typically it is set to port 443. 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 FT'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 443, remember that you will have to include the port number in your URL. For example, https://192.168.0.1:7995 .

- Require Certificate
  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 is allowed via a public interface. Note that some browsers do not handle self-signed certificates correctly. Certain versions of Firefox have exhibited this problem.

- Web Access
  These options allow blocking web access through the specified interface. If using the tunnel to bridge across a public network, it is strongly advised to disable web access via the public interfaces or to enable certificate based authentication.

- Respond to Ping
  This item allows you to block ping requests to the FT. Ping is a valuable tool for diagnosing network problems, but can also become a security problem. Disabling ping causes the FT to not respond to ping requests for one of its IP addresses. It has no effect on the FT's passing of ping request and responses from other network nodes.
- Web Access
  These options allow you to block web access through the specified interface. If you are using the tunnel to bridge across a public network, you are strongly advised to disable web access from the interface attached to the public network.
- Accepted Web IP Source Address
  This table allows you to control what hosts or networks have access to the FT-6602's web server. If empty, any host may access the unit.

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

  To allow access to all hosts in the range 192.168.10.1 to 192.168.10.255, enter:

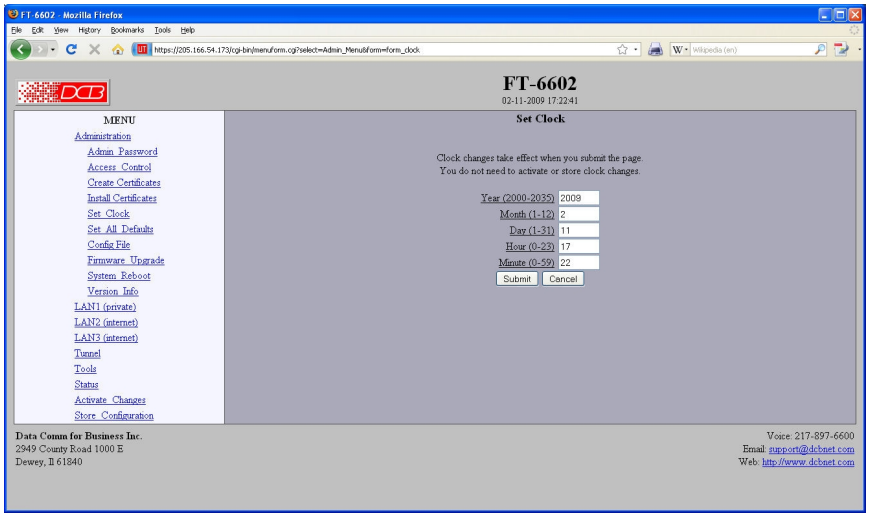
  Target: 192.168.10.0 Netmask: 255.255.255.0
- Target
  Host or Network address.
- Netmask
  If blank or set to 255.255.255.255, target is assumed to be a host address. Otherwise, target is treated as a network address.

Notes

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

NOTE: Internet Explorer Version 7 and newer or Firefox version 2 or newer are recommended. Older versions of web browsers may fail due to TLS negotiation issues.

Set Clock



Set Clock Screen

This form allows you to set the FT's clock. The setting will take effect when you press submit..

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.

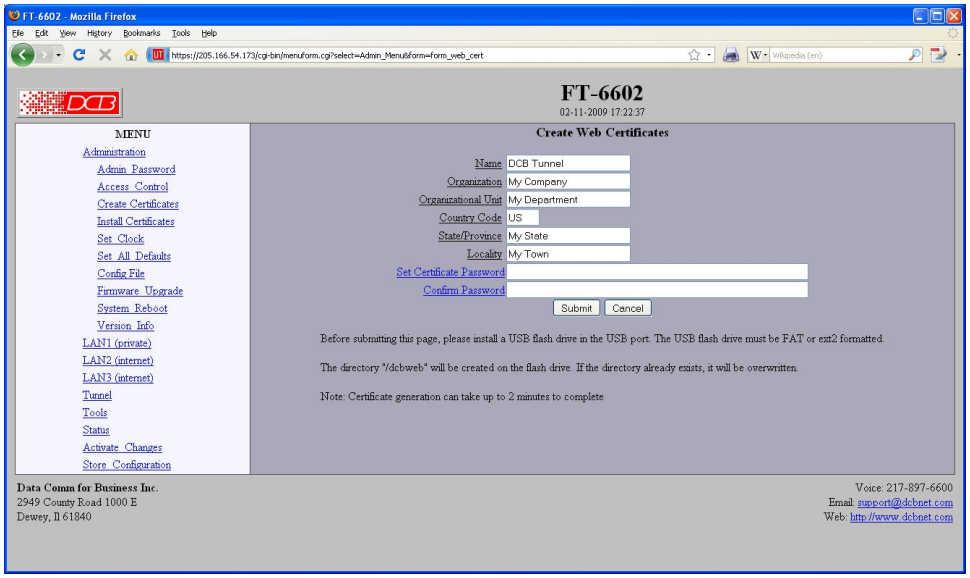
Hour Hour of the day in the range 0 to 23.

Minute Minutes in the range 0 to 59.

Notes

•

Create Web Certificates



Create Web Certificates

This form will allow you to install two x509 certificates into the tunnel's secure web server. One certificate is used to identify the web server. The second is used to verify the identity of the web browser. To install these certificates, insert the USB Flash drive that contains the previously generated certificate files into the tunnel's USB port. Enter the password used when the certificates were created and submit the page. The necessary files will be imported from the USB Flash drive. Activate and store the configuration to make them permanent. *You may want to hold off storing the changes until you have successfully imported the certificates into your web browser.*

After the new certificates are activated, the tunnel's web server will refuse to communicate with your web browser. You will need to import the certificate files from the USB Flash Drive into your web browser. The actual method depends upon your browser and version, but the method for Internet Explorer and Firefox is described below.

- Insert the USB Flash Drive into your computer.
- For Firefox 1 and 2:

  Go to "Edit/Preferences/Advanced/Security".
- For Firefox 3

  Go to "Tools/Options/Advanced/Encryption".
- For Internet Explorer:

  Go to "Tools/Options/Privacy".
- Click on the "View Certificates" button.

Browser Certificate

- Make sure the "Your Certificates" tab is selected.
- Press the "Import" button.

- You will be prompted for your Master Password. The Master password is for protecting your web browser's certificates. If this is the first time you have imported a certificate, you will be asked to create a password.
- Select the file "dcbweb/wbrowser.p12" from the USB drive.
- You will be prompted for the password used encrypt the certificate. Enter the same password you used when you generated the certificates.

Server Certificate (Internet Explorer and Firefox 1 and 2)

- Select the "Web Sites" tab.
- Press the "Import" button.
- Select the file "dcbweb/wserver.pem" from the USB drive.
- After import, highlight the server's certificate.
- Press the "Edit" button.
- Select "Trust the authenticity of this certificate"
- Press "OK"

Server Certificate (Firefox 3)

- Firefox 3 imports the certificate directly from the FT-6602 device. The FT-6602's IP address will be combined with the certificate making it necessary to import the certificate for every FT-6602 using that same certificate.
- Active the changes in the FT-6602 to insure it is using the new certificate.
- Attempt to access the FT-6602's web server. You should receive a "Security Connection Failed" message.
- Press the "or you can add an exception" link.
- Press the "Add Exception" button.
- Press the "Get Certificate" button.
- Make sure the "Permanently store this exception" box is checked.
- Press the "Confirm Security Exception" button.

Your browser should now be able to communicate with the server. It is normal to get a "Domain Name Mismatch" warning when you connect to the server. However, you should not get a "Website Certified by an Unknown Authority" or an "Untrusted Website" warning. If you do, it indicates that certificate presented by the device does not match the one stored in your web browser and that you may be communicating with an imposter device.

Note: It is permissible to install the same pair of certificates to multiple devices allowing all to be administered with the same set of certificates.
Note: Certificate generation may take several minutes to complete.

Fields

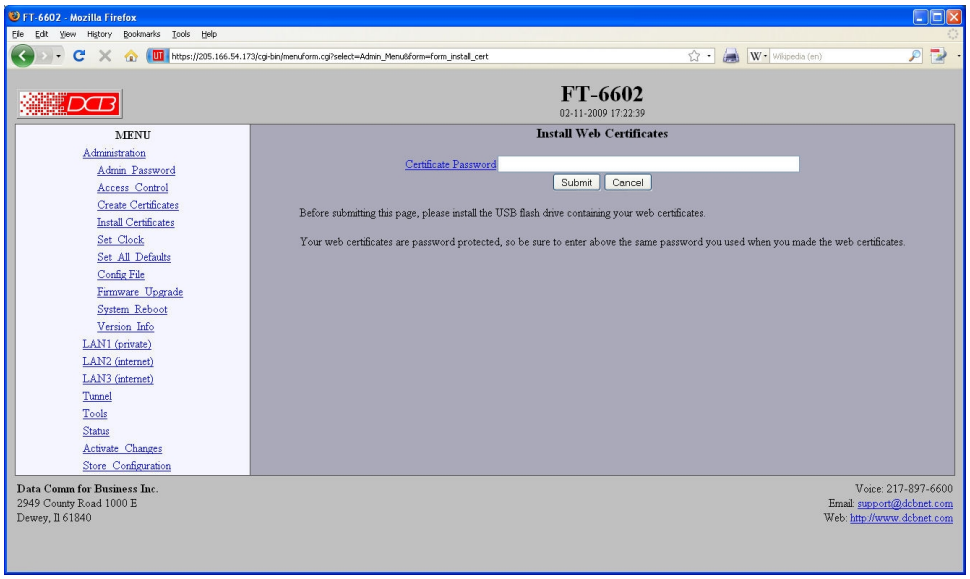
- Name
  The common name given to the certificate. The supplied name will be appended with the word "Server" for the server certificate and the word "Browser" for the browser certificate. Name may be 1 to 64 characters in length, limit to alph-numeric characters.
- Organization
  The organizational name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.
- Organizational Unit
  The organizational unit name or departmental name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.
- Country Code
  The country code given to the certificate. It is 2 characters in length, limit to alph-numeric characters.
- State/Province
  The State or Province name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.
- Set Certificate Password
  The password used to protect the private keys stored in the certificate. It may be 1 to 64 characters in length, limited to alph-numeric characters. You will need to know this password when you install the certificates. **THIS PASSWORD CAN NOT BE RECOVERED AND SHOULD BE RETAINED.**
- Confirm Password
  Re-enter the password for confirmation.

Notes

- The password can not be recovered if lost. In case of a lost password, the entire certificate generation and installation must be repeated.
- Before submitting this page, please install a USB flash drive in the USB port. The USB flash drive must be FAT or ext2 formatted.

  The directory "/dcbweb" will be created on the flash drive. If the directory already exists, it will be overwritten.
- Certificate generation can take up to 2 minutes to complete
- Internet Explorer Version 7 and newer or Firefox version 2 or newer are recommended. Older versions of web browsers may fail due to TLS negotiation issues.

Install Certificates



Install Web Certificates

This form will allow you to install two x509 certificates into the tunnel's secure web server. One certificate is used to identify the web server. The second is used to verify the identity of the web browser. To install these certificates, insert the USB Flash drive that contains the previously generated certificate files into the tunnel's USB port. Enter the password used when the certificates were created and submit the page. The necessary files will be imported from the USB Flash drive. Activate and store the configuration to make them permanent. *You may want to hold off storing the changes until you have successfully imported the certificates into your web browser.*

After the new certificates are activated, the tunnel's web server will refuse to communicate with your web browser. You will need to import the certificate files from the USB Flash Drive into your web browser. The actual method depends upon your browser and version, but the method for Internet Explorer and Firefox is described below.

```
- Insert the USB Flash Drive into your computer.
- For Firefox:
      Go to "Edit/Preferences/Advanced/Security".
- For Internet Explorer:
      Go to "Tools/Options/Privacy".
- Click on the "View Certificates" button.

Browser Certificate
- Make sure the "Your Certificates" tab is selected.
- Press the "Import" button.
- You will be prompted for your Master Password.  The Master
  password is for protecting your web browser's certificates.
  If this is the first time you have imported a certificate,
  you will be asked to create a password.
- Select the file "dcbweb/wbrowser.p12" from the USB drive.
```

```
   - You will be prompted for the password used encrypt the
     certificate.  Enter the same password you used when you
     generated the certificates.

   Server Certificate
   - Select the "Web Sites" tab.
   - Press the "Import" button.
   - Select the file "dcbweb/wserver.pem" from the USB drive.
   - After import, highlight the server's certificate.
   - Press the "Edit" button.
   - Select "Trust the authenticity of this certificate"
   - Press "OK"
   Your browser should now be able to communicate with the server. It
is normal to get a "Domain Name Mismatch" warning when you connect to
the server. However, you should not get a "Website Certified by an
Unknown Authority" or an "Untrusted Website" warning. If you do, it
indicates that certificate presented by the device does not match the
one stored in your web browser and that you may be communicating with
an impostor device.


Some web browser versions do not handle self-signed certificates
correctly.  At least one version of Mozilla has this problem, and can
not be used in this application.


Note: It is permissible to install the same pair of certificates to
multiple devices allowing all to be administered with the same set of
certificates.
```

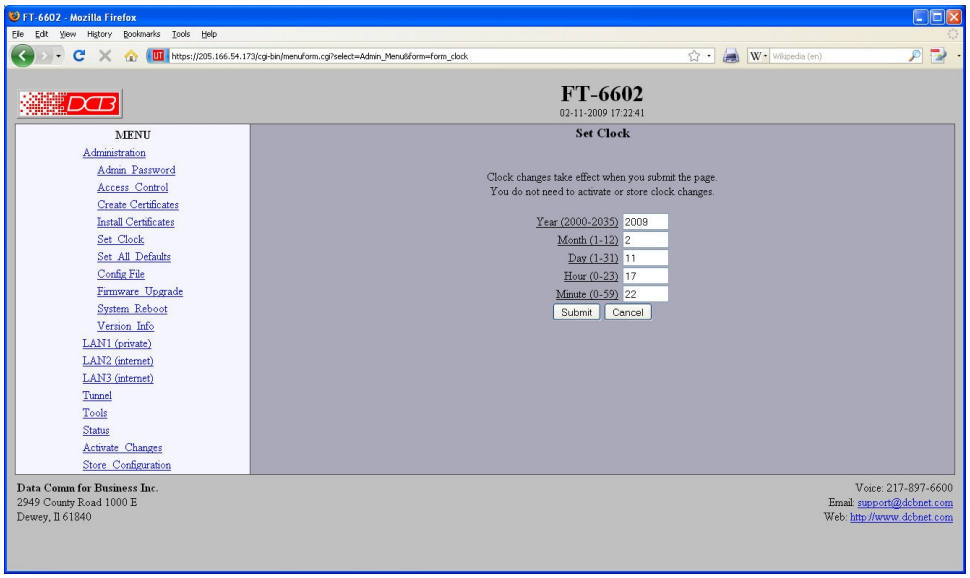
Fields

- Certificate Password
  The password to use to decrypt the private key stored in the certificate files. This must be the same password used when the certificates files were generated.

Notes

- The certificate password can not be recovered if lost. In case of a lost password, the entire certificate generation and installation must be repeated.
- Some web browser versions do not handle self-signed certificates correctly. At least one version of Mozilla has this problem, and can not be used in this application.
- Note: It is permissible to install the same pair of certificates to multiple devices allowing all to be administered with the same set of certificates.

Set Clock



Set Clock Screen

This form allows you to set the FT's software clock. The setting will take effect when you submit the page. Storing or activating the changes is not needed.

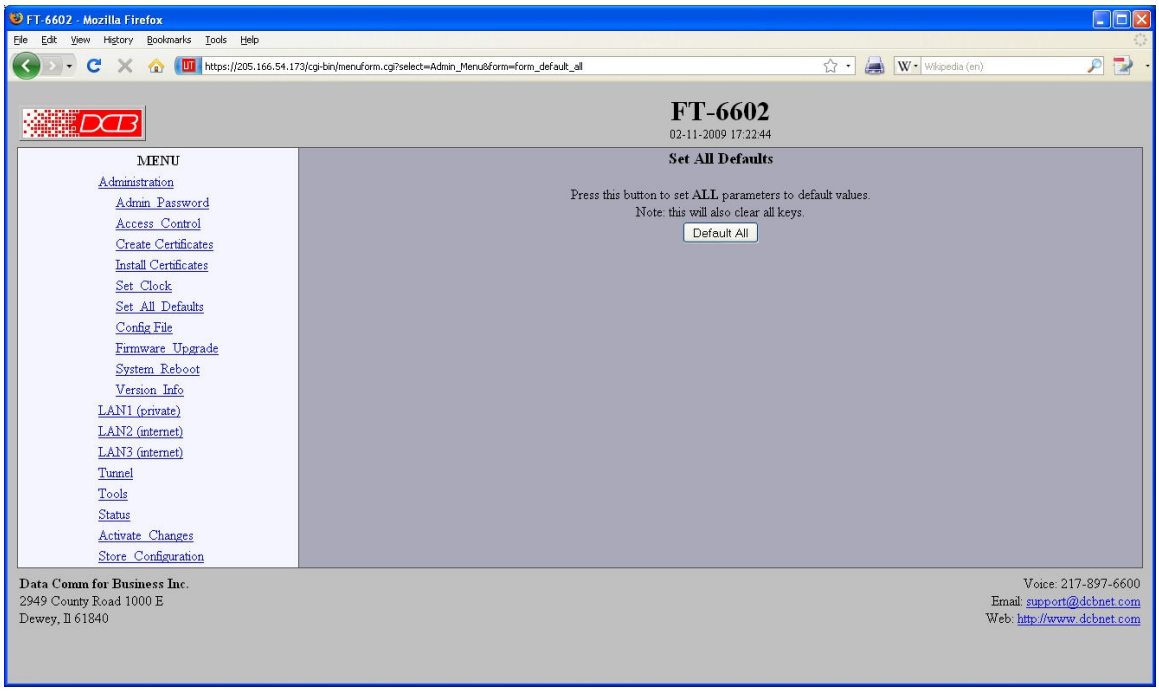
Fields

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

- The default values shown on this screen for those products are the “boot” values… not the current time.

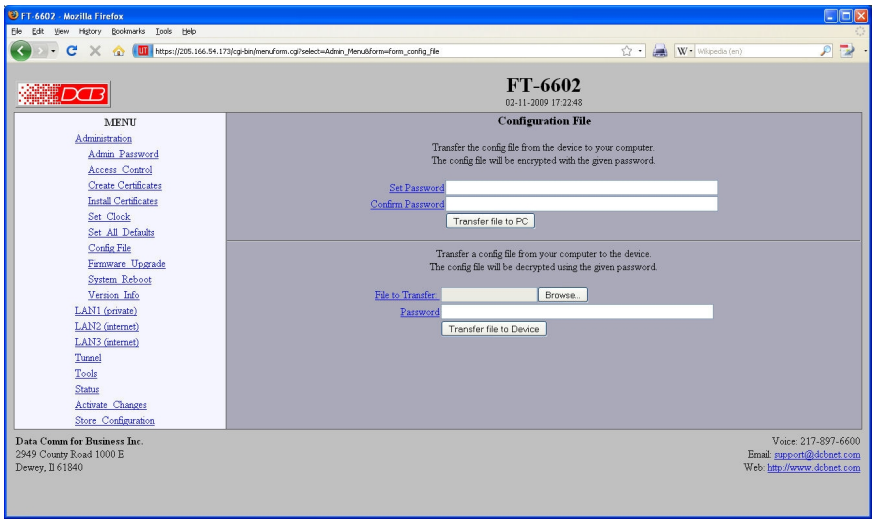
Set All Defaults



Set All Defaults Screen

This form will allow you to set all bridge 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. This will also reset all the certificates stored within the unit.

Configuration File



Configuration File Screen

This form will allow you to copy the FT-6602'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. The configuration is stored on the PC in an encrypted file.

After entering a password and confirming it, press the "Transfer file to PC" button, the configuration file will be encrypted and its name displayed as a link. Right click on the link and use the "save as" browser feature to save the file to the name of your choice. Keeping the .bin file extension is recommended.

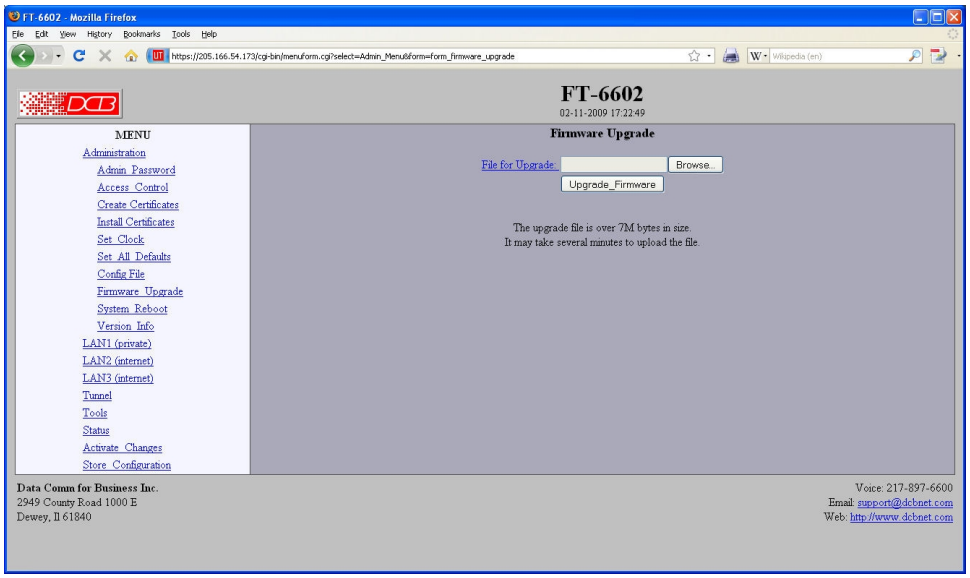
Fields

- Set Password
  This password will be used to encrypt the stored configuration file.
- Confirm Password
  Re-type the password above.
- Transfer file to PC (action)
  Transfers the current bridge configuration file to this PC.
- File to Transfer
  The file containing the encrypted configuration. There is also a Browse button.
- Password
  The password used to encrypt the file.
- Transfer file to Bridge (action)
  Transfers the named file to the bridge.

Notes

- The configuration file is a specially formatted encrypted file. It may not be edited.
- 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.

Firmware Upgrade



Firmware Upgrade Screen

This form will allow you to load new firmware into the FT-6602. The firmware will be saved to non-volatile memory, replacing the current firmware. The firmware file larger than 7 Mbytes. It may several minutes to upload the file.

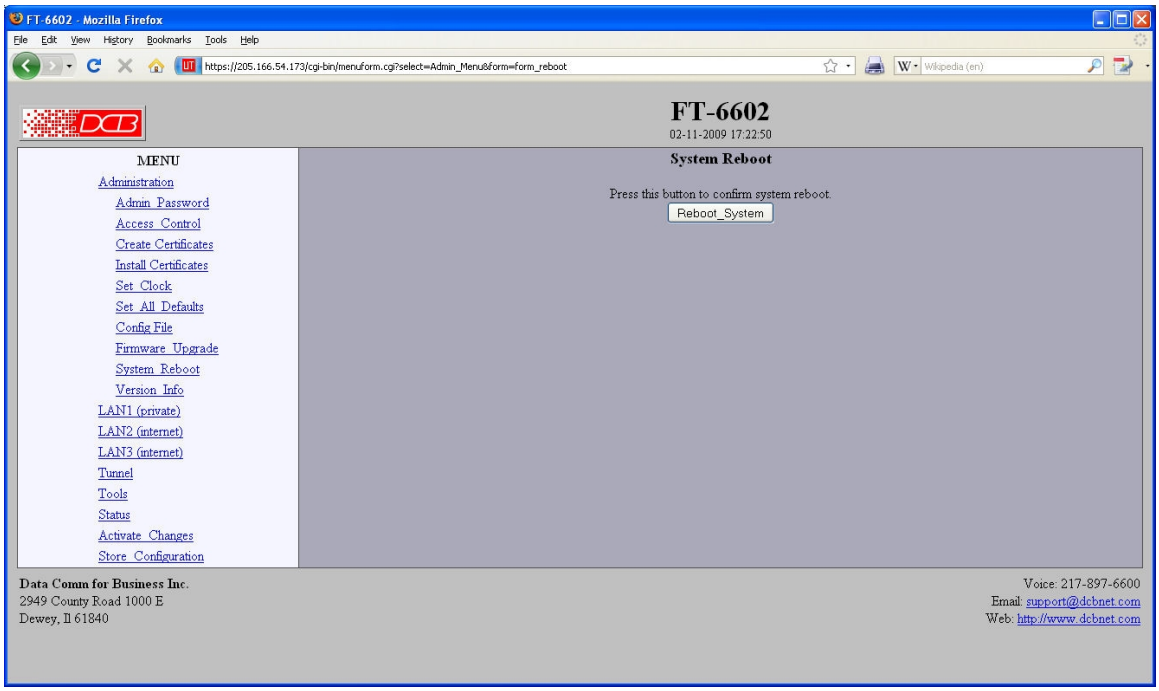
Fields

- File Name
  This is the name of the firmware image file to be transferred to the bridge. There is also a browse button.
- 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 FT-6602. If you have configuration changes that have not been saved to non-volatile memory, they will be lost.

This is the method to revert back to the previously stored configuration.

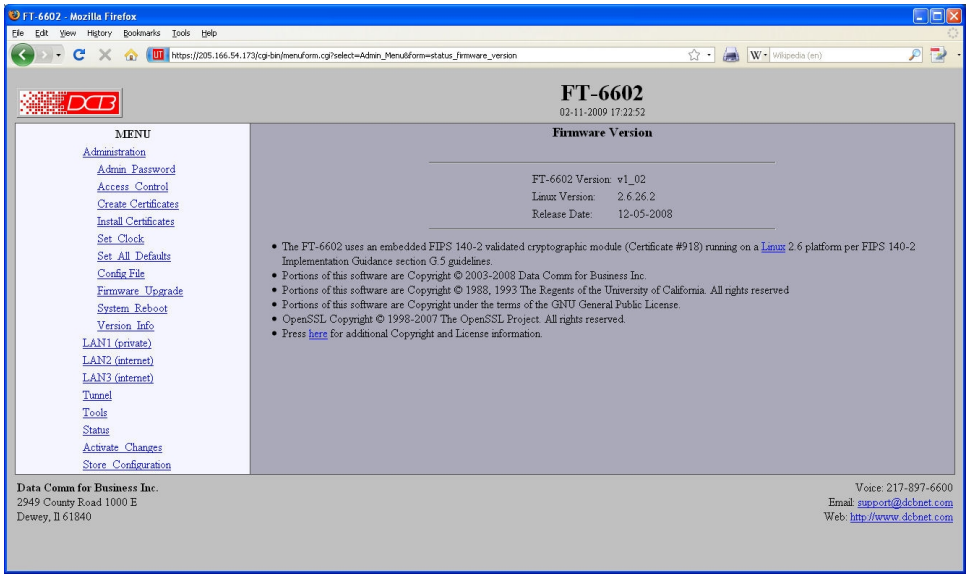
Fields

- 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.

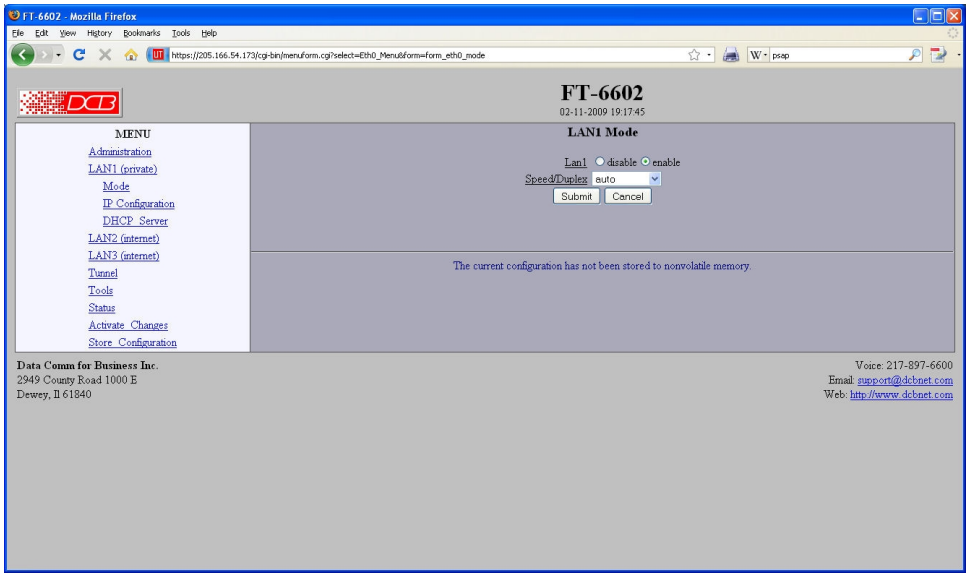
Version Information Screen



Version Information Screen

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

LAN 1 Ethernet Mode



LAN 1 Ethernet Mode Screen

The FT-6602 contains three ethernet interfaces.

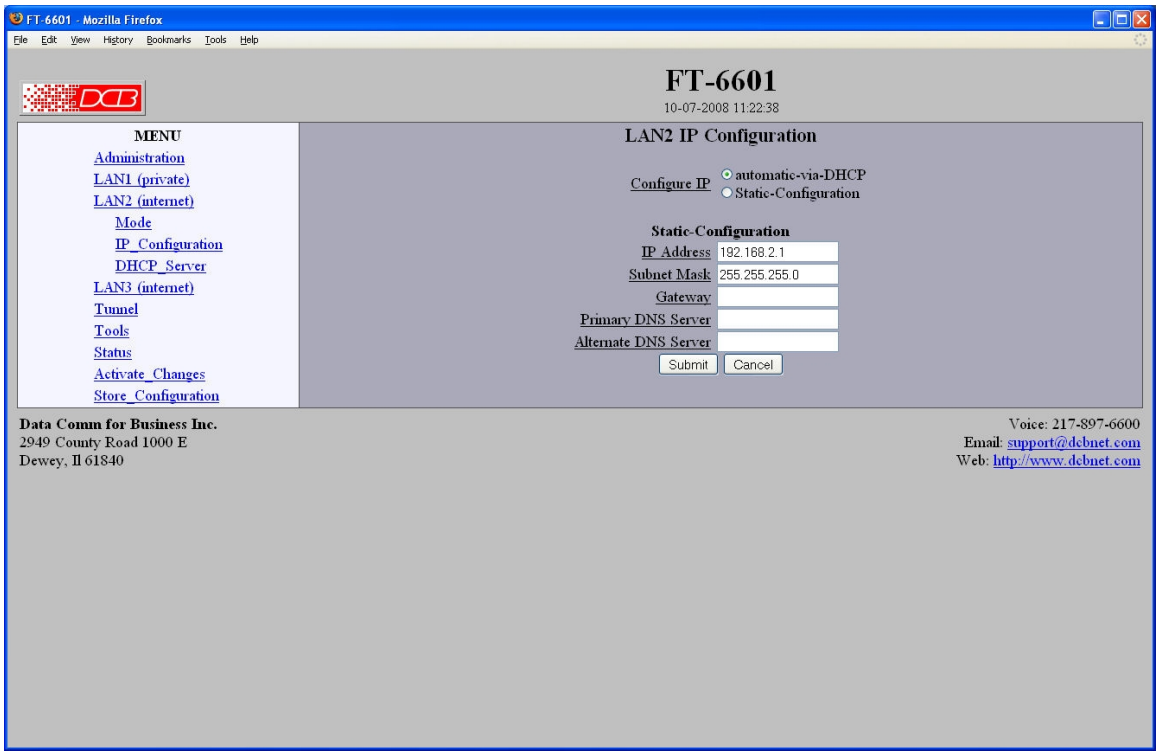
LAN 1 may be disabled or enabled, and the speed/duplex configured. In addition, LAN 2 and LAN 3 may be also be configured for PPPoE.

Fields

- LAN 1
  Enable or disable Lan 1. The default is enabled.
- Speed/Duplex
  Select 100 MB or 10 MB and half or full duplex, AUTO. The default is AUTO.

Notes:

Ethernet IP Configuration



Ethernet Configuration Screen

The FT-6602 contains three Ethernet interfaces. LAN 1 is always a local, secure side of the tunnel. The public network interface may be either LAN 2 or LAN 3. This screen is used to configure both IP parameters and DHCP server parameters (if the DHCP server function is used)

LAN 2 and LAN 3 may use PPPoE or IP. On those interfaces, there will be an Ethernet Mode screen, used to select the mode for the ethernet port. See the Ethernet PPPoE configuration screen section for information pertaining to PPPoE.

This screen is used to configure IP on all LAN interfaces that aren't set to PPPoE mode.

Fields

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

  This field is not used if DHCP Client has been enabled. The subnet mask will be assigned by the DHCP server.
- 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 source-based routing rules which allow each interface to have a gateway router defined. This is contrary to typical network devices where only one gateway router may be defined.
- 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.
- Primary DNS Server
  The IP address of the primary DNS server. This configuration item is shared by all LAN interfaces. Setting the DNS server is optional and only necessary when using host names.
- Secondary DNS Server
  The IP address of the secondary DNS server. This configuration item is shared by all LAN interfaces. Setting the DNS server is optional and only necessary when using hostnames.

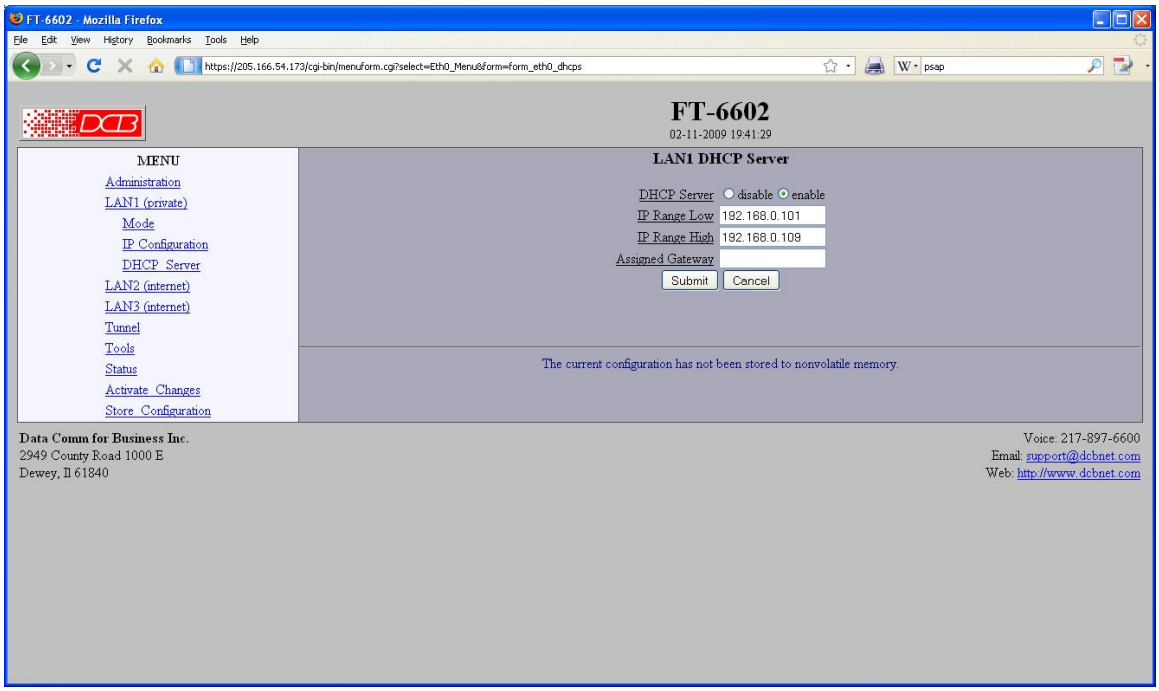
Notes:

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

For maximum throughput, always disable unused interfaces.

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

DHCP Server Configuration



DHCP Server Configuration Screen

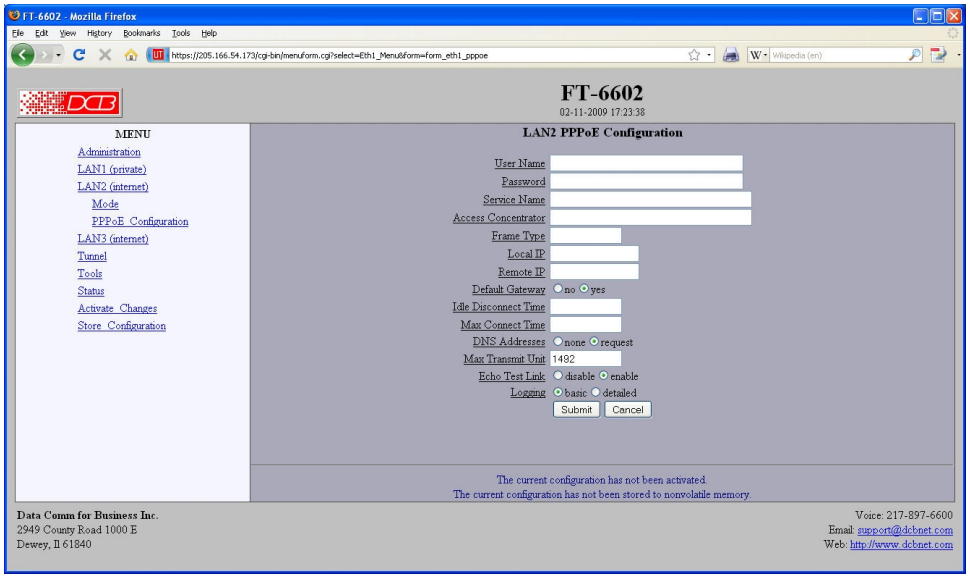
The FT-6602 may also provide DHCP services to clients on it's ethernet interfaces.

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 Range Low / IP Range High Address
  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.
- Assigned 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.

Notes:

Ethernet PPPoE Configuration



Ethernet PPPoE Configuration Screen

LAN 2 and LAN 3 interfaces may be configured to use PPPoE by using the Ethernet Mode screen. This screen is only displayed 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.
- FrameType
  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 PPPoE connection will have an IP address. This is the IP address to use for the local PPPoE device. With PPPoE, you will normally leave this field blank and the PPPoE server will automatically assign an IP address upon connection.

  If you leave this field blank when connecting on-demand, the FT 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 and 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 PPPoE 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.

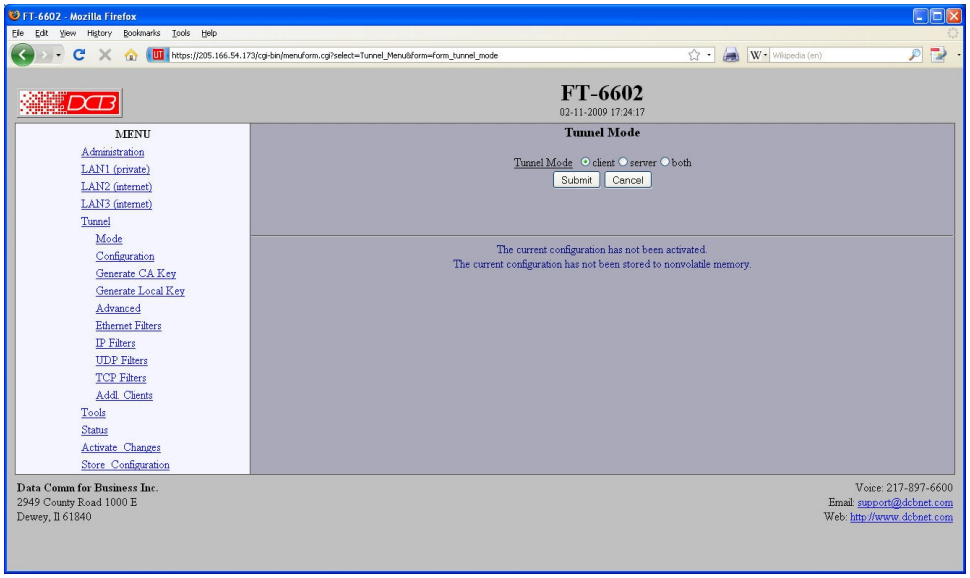
- DNS Addresses
  When set to *request*, the local FT will request DNS addresses from the PPPoE Server during PPPoE option negotiation. When set to *none*, the local FT will not request DNS addresses, and will use the static DNS configuration.

- 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 PPPoE log file.

Tunnel Mode



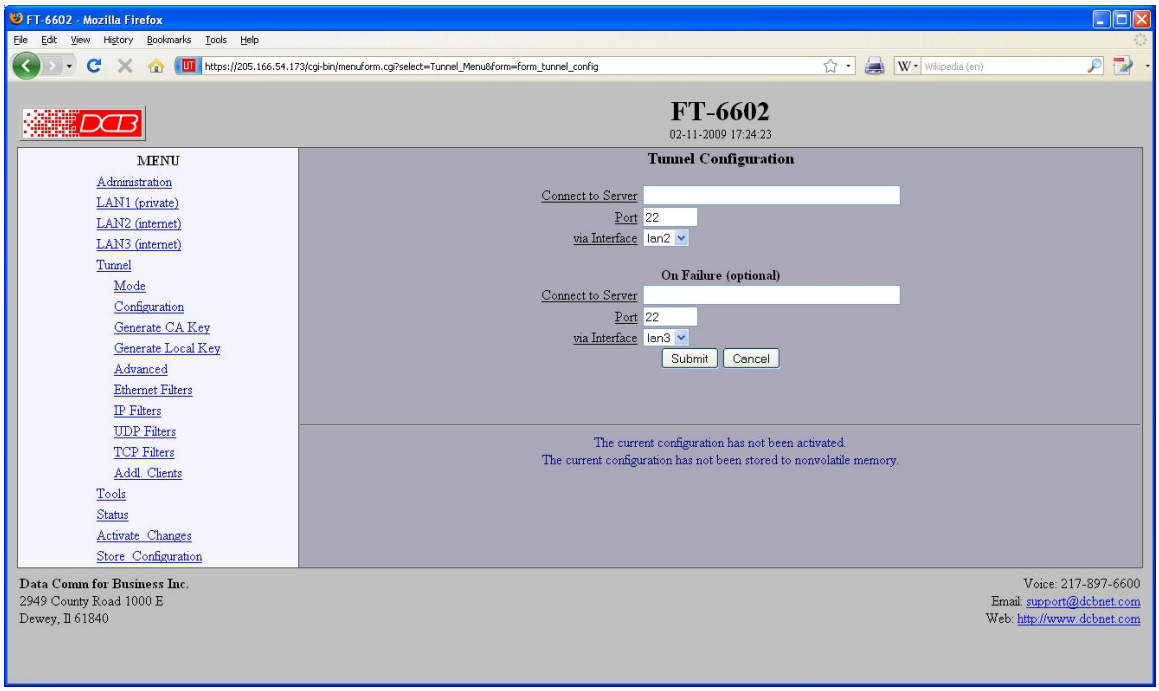
Tunnel Mode Screen

The FT-6602 may be configured as either a server, client, or both. FT-6602 clients connect to the server, so the server's IP address must be visible to the client either directly, or through a port-forwarding firewall.

Fields

Tunnel Mode
Select the operating mode of the tunnel, either client, server or both. A typical setup will have one server tunnel and one or more client tunnels. The server tunnel listens for connections from the clients. The client tunnels initiate connections with the server.

Encrypted Tunnel Configuration



Tunnel Configuration Screen

Some fields on this screen do not display if the associated mode is not selected.

Fields

Server Mode Enabled:

Listen-to Port

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

Secondary Listen-to Port

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

Client Mode Enabled:

Connect-to Server

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

Port

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

Via Interface
Which network interface to use when connecting to the server.

On Failure: (Optional)

Connect-to Server

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

Port

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

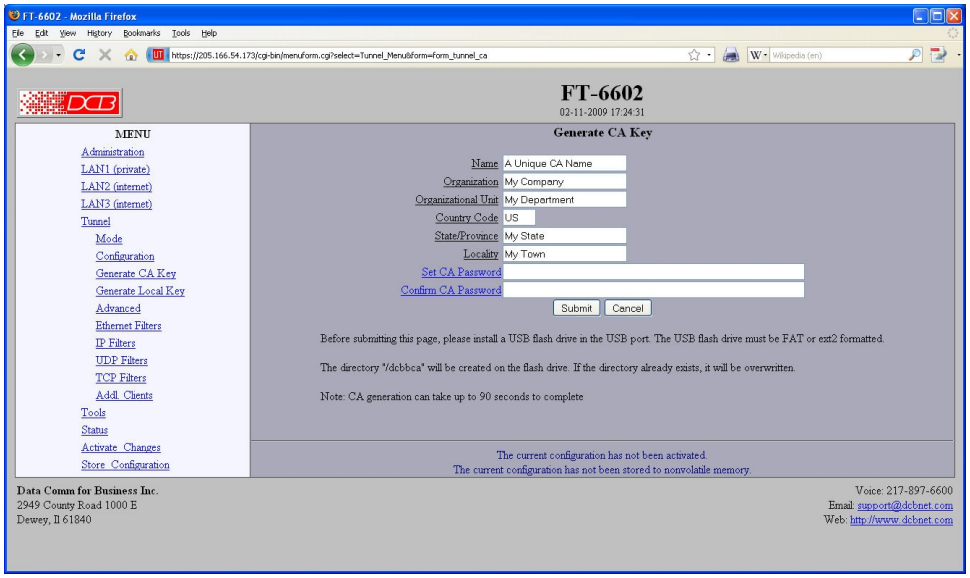
Via Interface
Which network interface to use when connecting to the server.

User Passphrase

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

Notes

Generate Certificate Authority Key



Generate CA Key

The tunnel makes use of certificates (public-key cryptography) to identify and authenticate the endpoints. Before you can generate endpoint certificates (local keys), you first need to create a Certificate Authority (CA). The CA will be stored on a USB Flash Drive (supplied with the FT-6602). You can think of this USB Flash Drive as being your master CA key.

This form generates the Certificate Authority Key and associated, management files, storing them on a USB Flash Drive inserted into the tunnel's USB port. These files will be written to the directory **dcbbca**. It is important that you protect the contents of the USB Flash Drive.

Before submitting this page, please install a USB flash drive in the USB port. The USB flash drive must be FAT or ext2 formatted. The directory "/dcbbca" will be created on the flash drive. If the directory already exists, it will be overwritten.

CA generation may take several minutes to complete

Fields

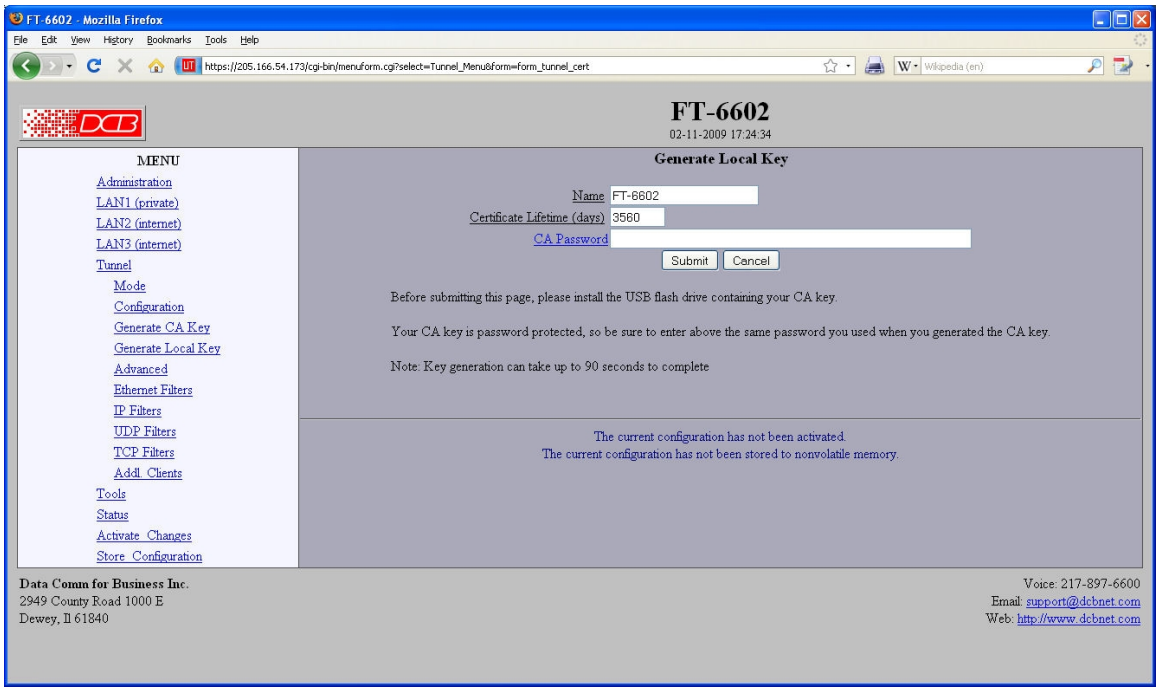
- Name
  The common name given to the certificate. The supplied name will be appended with the word "Server" for the server certificate and the word "Browser" for the browser certificate. Name may be 1 to 64 characters in length, limit to alph-numeric characters.
- Organization
  The organizational name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.
- Organizational Unit
  The organizational unit name or departmental name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.

- Country Code
  The country code given to the certificate. It is 2 characters in length, limit to alph-numeric characters.
- State/Province
  The State or Province name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.
- Set CA Password
  The password used to protect the private key stored in the Certificate Authority. It may be 1 to 64 characters in length, limited to alph-numeric characters. You will need to know this password when you generate local keys. **THIS PASSWORD CAN NOT BE RECOVERED AND SHOULD BE RETAINED.**
- Confirm Password
  Re-enter the password for confirmation.

Notes

- The password can not be recovered if lost. In case of a lost password, the entire certificate generation and installation must be repeated.
- Before submitting this page, please install a USB flash drive in the USB port. The USB flash drive must be FAT or ext2 formatted.
- The tunnel makes use of certificates (public-key cryptography) to identify and authenticate the endpoints. Before you can generate endpoint certificates (local keys), you first need to create a Certificate Authority (CA). The CA will be stored on a USB Flash Drive. You can think of this USB Flash Drive as being your master CA key.
- This form generates the Certificate Authority Key and associated, management files, storing them on a USB Flash Drive inserted into the tunnel's USB port. These files will be written to the directory **dcbbca**. It is important that you protect the contents of the USB Flash Drive.

Generate Local Key



Generate Local Key

The tunnel makes use of certificates (public-key cryptography) to identify and authenticate the endpoints. Before you can generate endpoint certificates (local keys), you first need to create a Certificate Authority (CA). The CA will be stored on a USB Flash Drive (supplied with the FT-6602). You can think of this USB Flash Drive as being your master CA key.

In order for a client tunnel to connect and communicate with a server tunnel, each must have a local key (or certificate) that was signed by the same Certificate Authority (CA) Key. This form will generate a local key, signed by the CA key inserted in the USB Flash Drive.

Note: this operation will update information stored on the USB Flash Drive.

Before submitting this page, please install the USB flash drive containing the CA key in the USB port.
Your CA key is password protected, so be sure to enter above the same password you used when you generated the CA key.

Key generation may take several minutes to complete

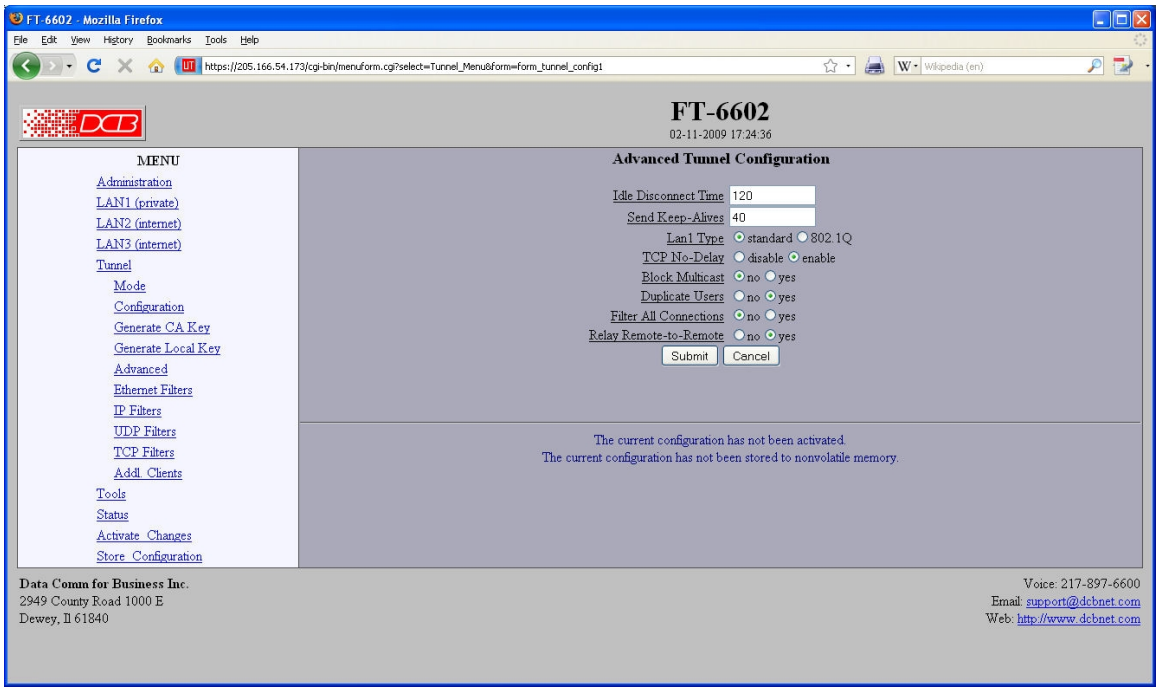
Fields

- Name
  The common name given to the local certificate. This name will display in the title of the web pages. It will also show up in the tunnel logs.
- Certificate Lifetime
  The lifetime, in days, that the certificate is to be valid.

- CA Password
  The Certificate Authority (CA) Key is password protected. You must enter the same password used with the CA was generated. .

Notes

Advanced Tunnel Configuration



Advanced Tunnel Configuration Screen

Fields

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

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

LAN1 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. .

Duplicate Client Names

This option only applies to the server tunnel. When set to *no*, the server will only allow one instance of a client, based on it name, to be connect

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.

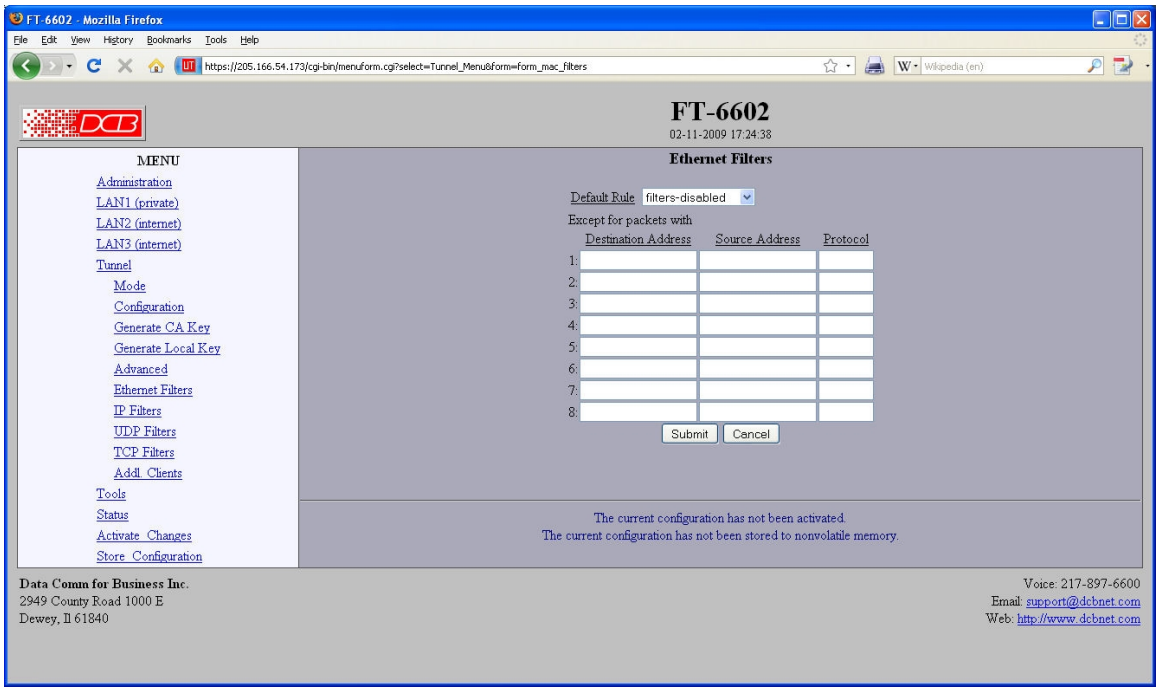
Important note, setting this feature to yes will eliminate the ability to have a service enabled at one endpoint while blocking that service in the opposite direction. The service is effectively disabled in all directions.

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

Ethernet (MAC) Address Filters Screen



Address Filters Screen

Ethernet filters are used to limit the Ethernet packets sent from the local tunnel to a remote tunnel. Filtering is performed by comparing the destination address, source address, and protocol ID addresses against a table of rules.

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

Next, you enter one or more exceptions to the default rule. An exception consists of a destination address, source address, and protocol ID. Any packet matching all three items will be considered an exception, causing the opposite of the default rule to be performed.

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

For Ethernet frames tagged an 802.1Q protocol ID, the protocol ID of the original frame will be used for comparison.

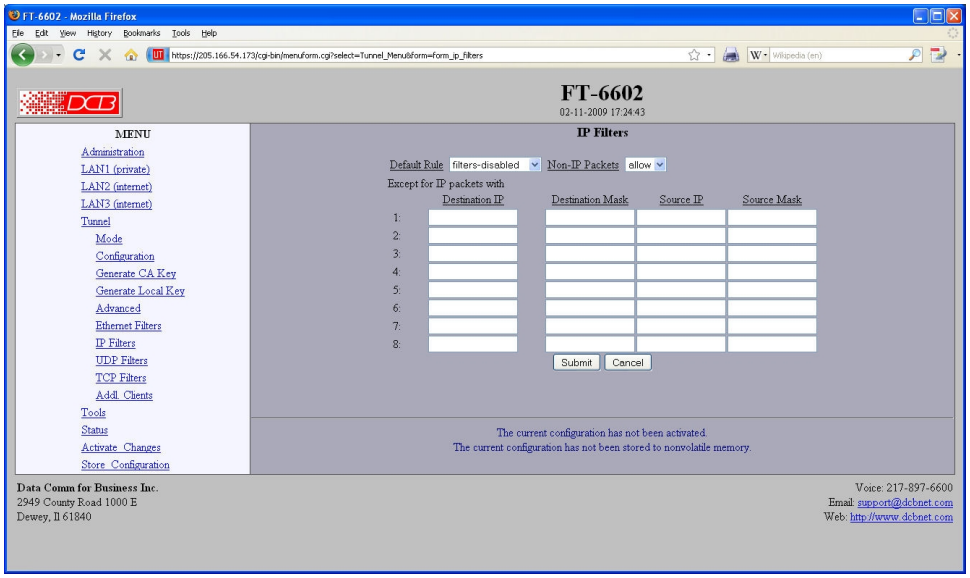
Fields

- Default Rule
  The table may be configured with the defaults of "allow all packets except", "drop all packets except", or filters disabled.
- Destination Address
  This field specifies the destination Ethernet address. If blank, it is interpreted to mean *any* address. The Ethernet address is a 6 byte number entered as 12 hexadecimal digits, with each byte optionally separated with a ':', '-', or ' ' character. For example, 00:06:3B:00:17:01, 00-06-3b-00-17-01, 00 06 3b 00 17 01, 00063b001701 are all valid input.
- Source Address
  This field specifies the source Ethernet address. If blank, it is interpreted to mean *any* address. See above for formatting examples.
- Protocol
  This field specifies the Ethernet Protocol ID. It is entered as a 4 digit hexadecimal number. The valid range is 0600 to FFFF. Example values are 0800 - IP, 0806 - ARP, 0835 - RARP, 8137 - IPX.

Notes

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

IP Address Filters Screen



Address Filters Screen

IP filters are used to limit the Ethernet packets sent from the local tunnel to a remote tunnel. This level of filtering is performed on IP(0800) and ARP(0806) packets by comparing the destination and source addresses against a table of rules.

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

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

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

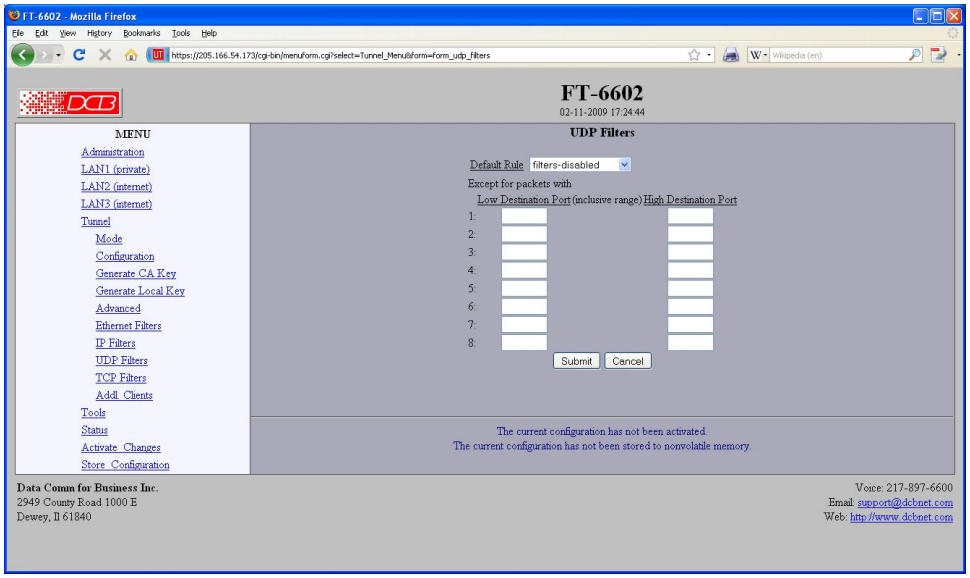
IP filtering is performed after Ethernet Filtering. Any packets discarded by Ethernet filtering will not reach IP filtering.

Fields

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

Notes

UDP Address Filters Screen



UDP Address Filters Screen

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 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 or TCP 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

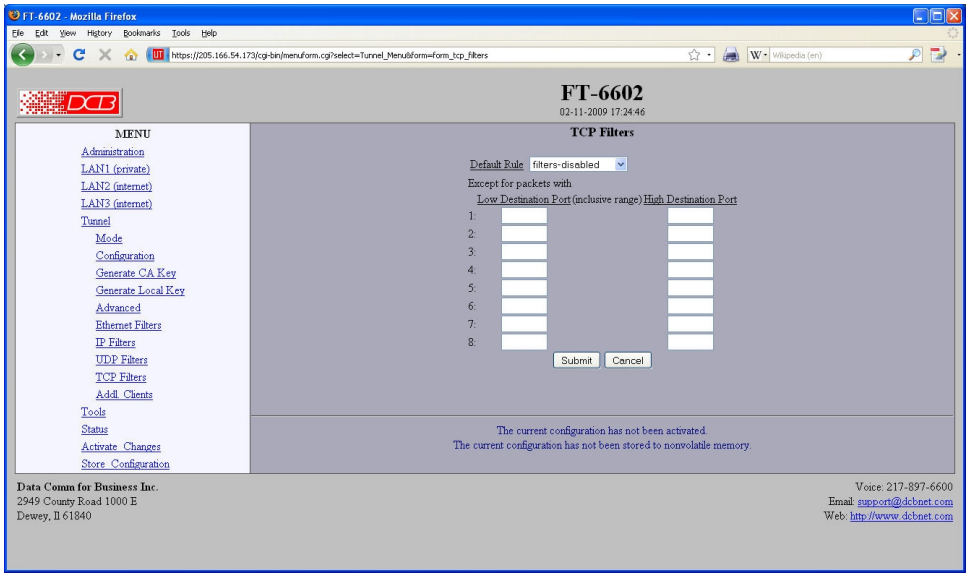
- Default Rule
  This field specifies the action to be taken when an UDP packet does not meet any of the exception rules.
- Low Destination Port
  This field specifies the Low Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the 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.

TCP Address Filters Screen



TCP Address Filters Screen

TCP filters are used to limit the TCP packets sent from the local tunnel to a remote tunnel. This level of filtering is performed on the TCP Destination Port Number. It would typically be used to eliminate a specific service. For example, you may not want Telnet requests to come in from a remote network. In this case you would block TCP port 23 in the remote tunnel device.

To use TCP filtering, you first select a default rule. That is, you choose to **allow all** TCP packets by default, or to **drop all** TCP 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 TCP 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 TCP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

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

Fields

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

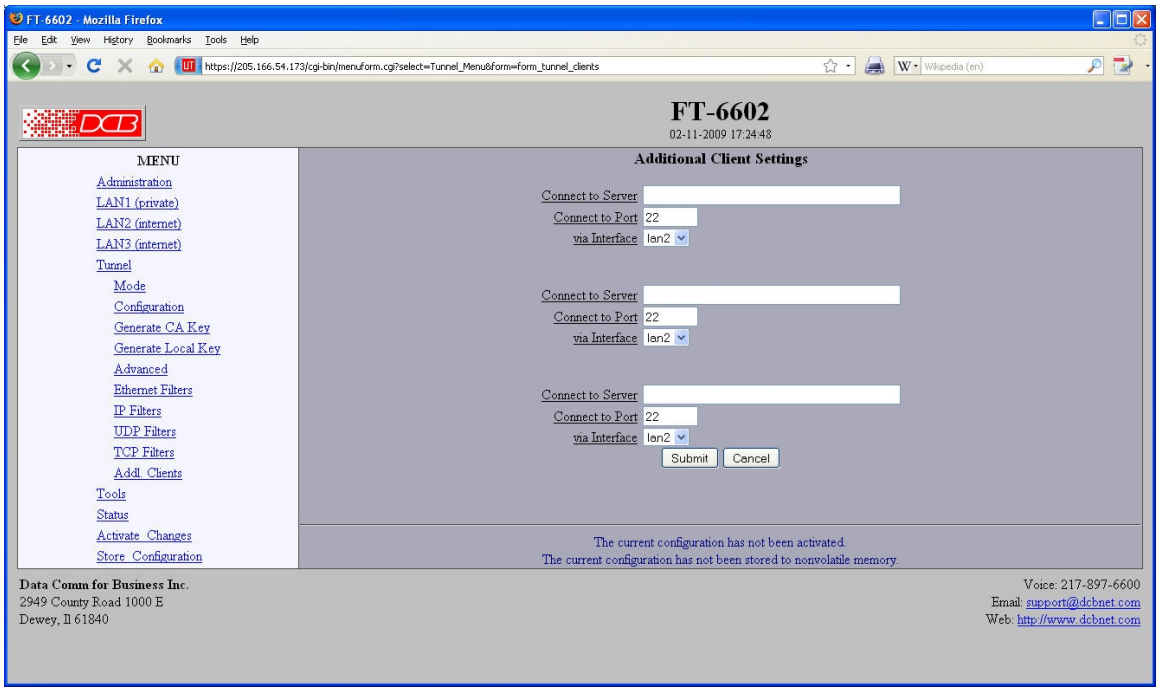
- Low Destination Port
  This field specifies the Low Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.
- High Destination Port
  This field specifies the High Destination Port Number in an inclusive range.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

Notes

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

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

Additional Client Settings



Additional Clients Configuration Screen

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

Fields

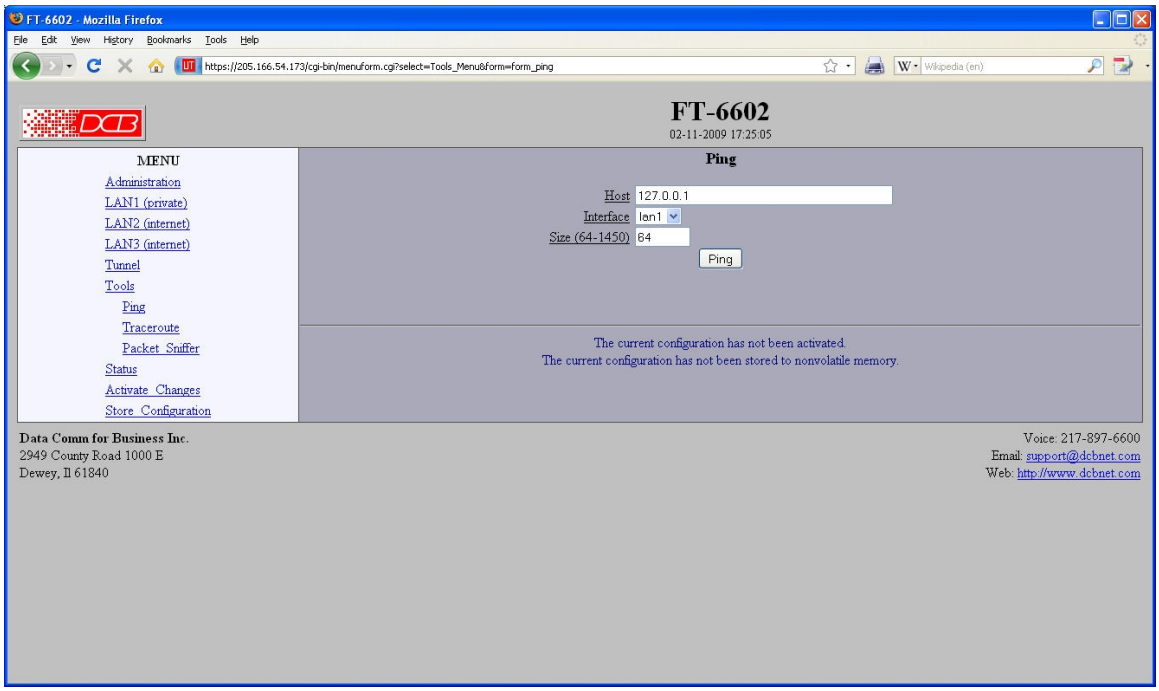
Connect-to Server
The hostname or IP address of the server tunnel.

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

Via Interface
Which network interface to use when connecting to the server.

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.

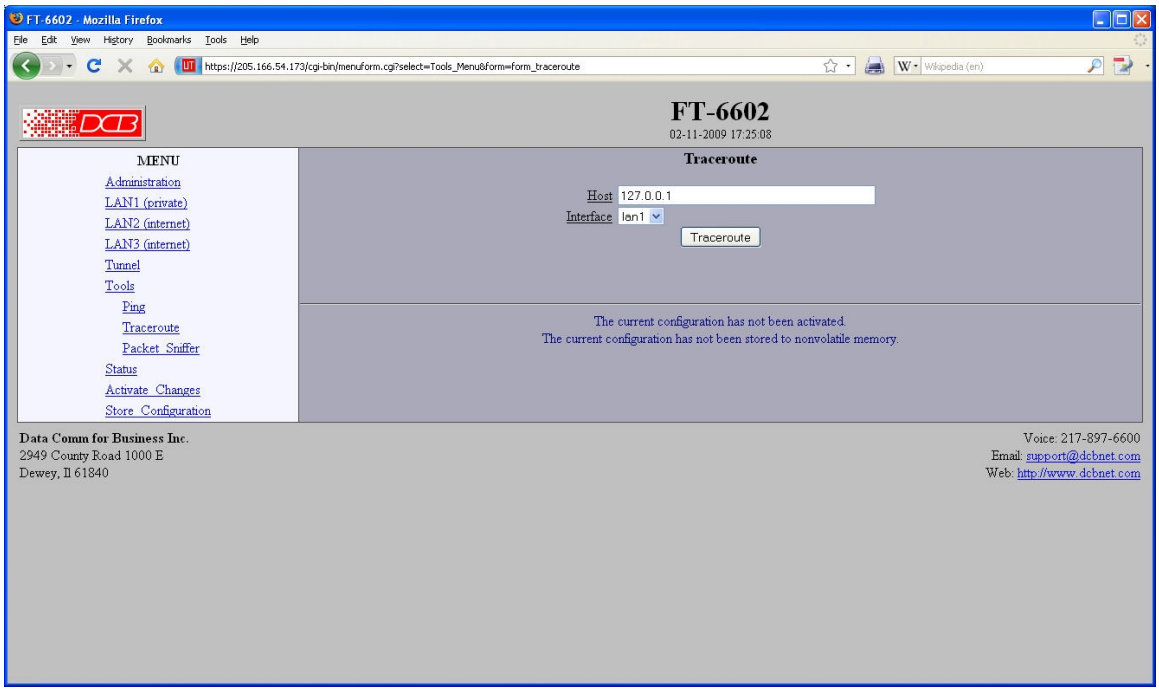
Fields

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

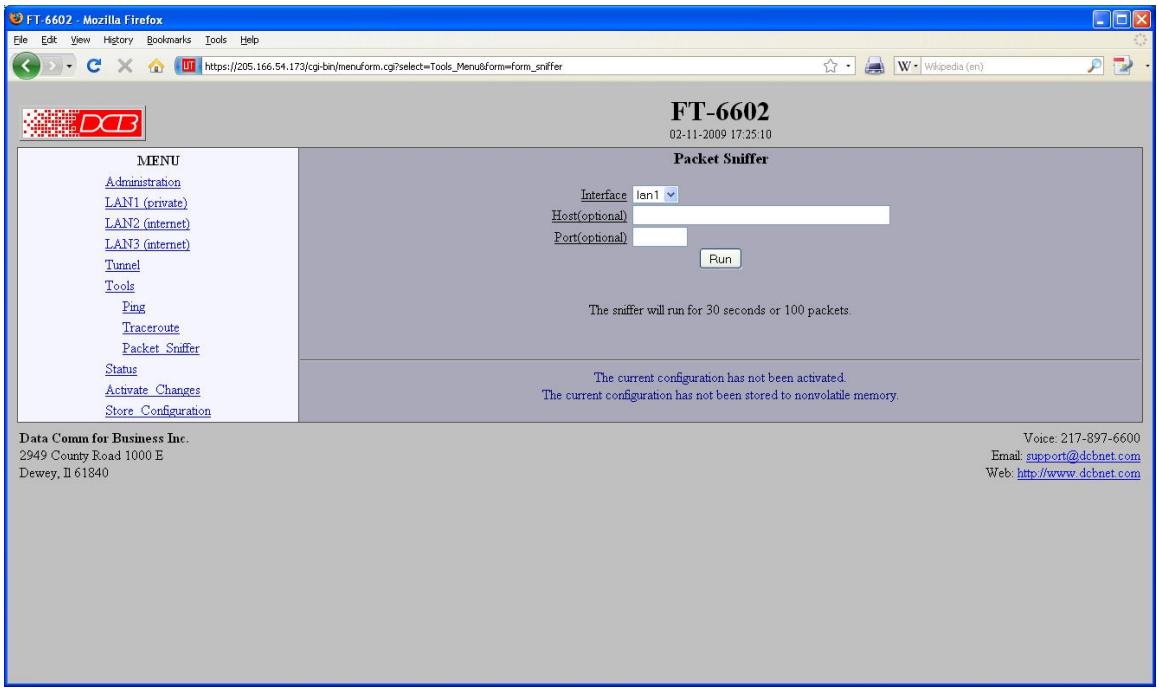
Fields

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.

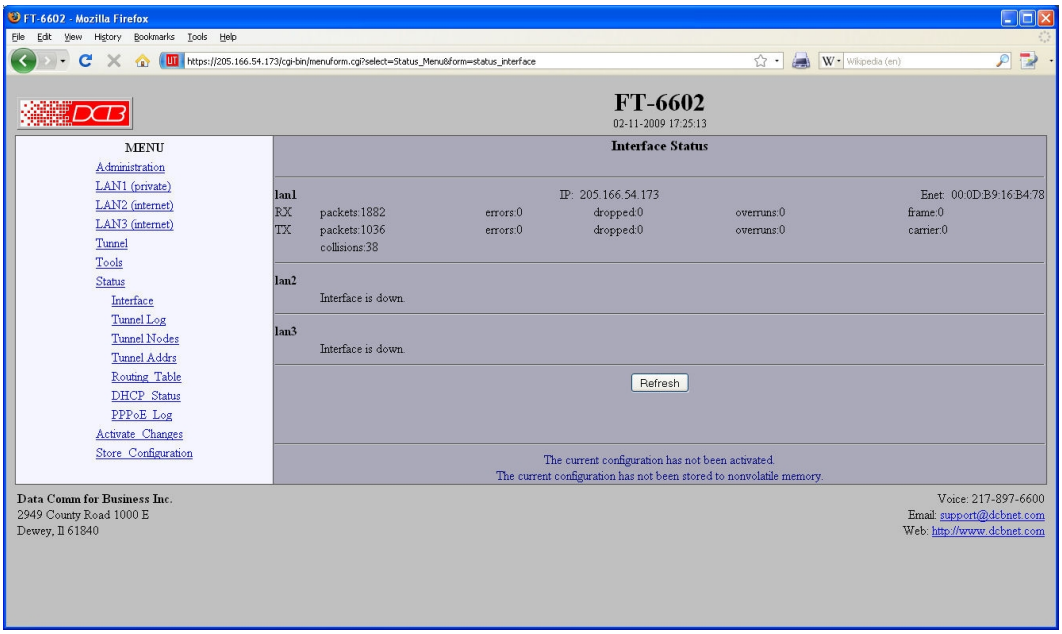
Fields

- Interface
  Which interface to use. On a PPPoE interface, You will not see low-level PPP traffic on the PPPoE connection, only the payload traffic.
- Host
  This applies a host filter. Only packets with a matching source or destination IP address will be included in the trace.
- Port
  This applies a port number filter. Only TCP or UDP packets with a matching source or destination port number will be included in the trace..

Notes

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

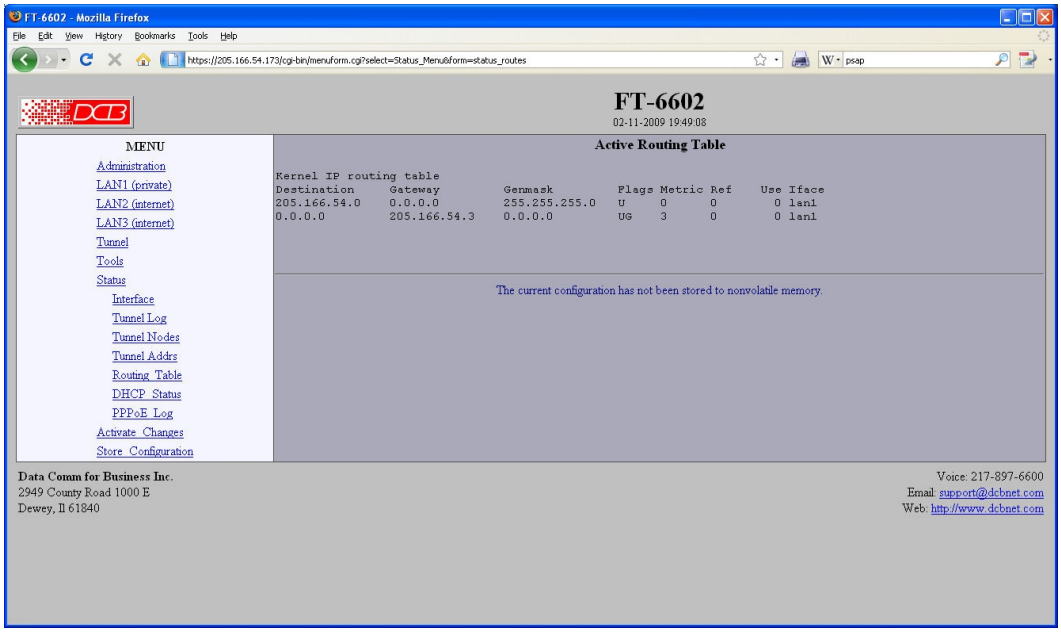
Interface Status Screen



Status Screen

The Interface Status screen shows port status and packet counters for each interface on the FT. It displays counters that are useful in diagnosing network connectivity problems.

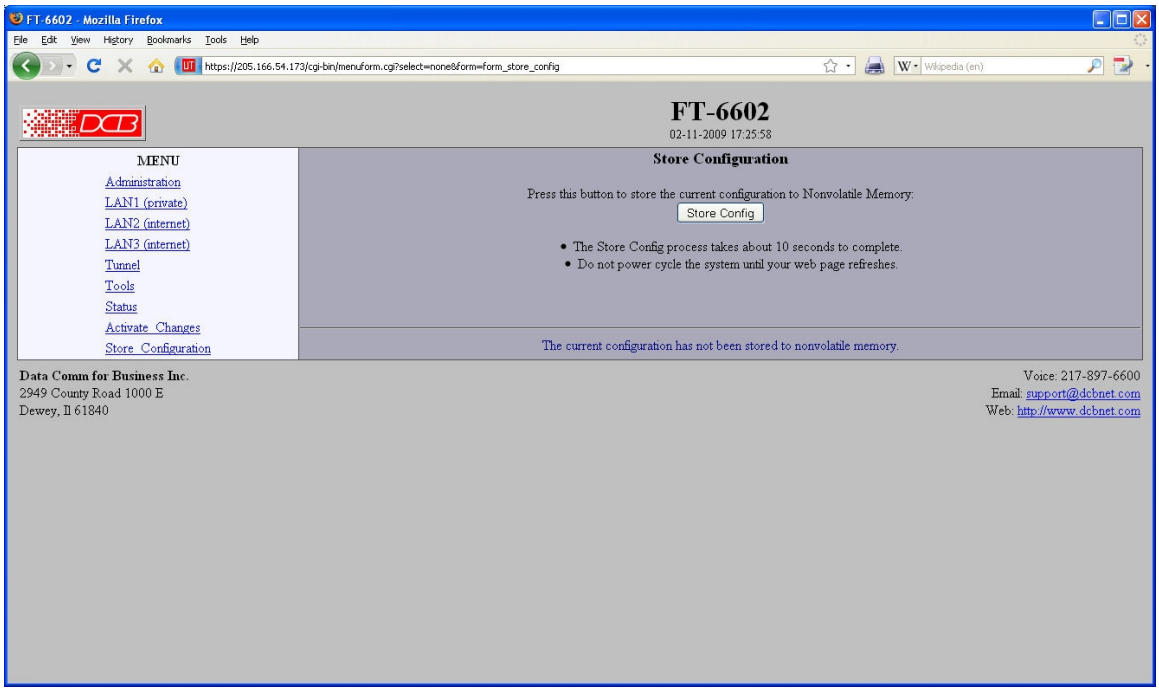
Routing Table Screen



Routing Table Screen

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

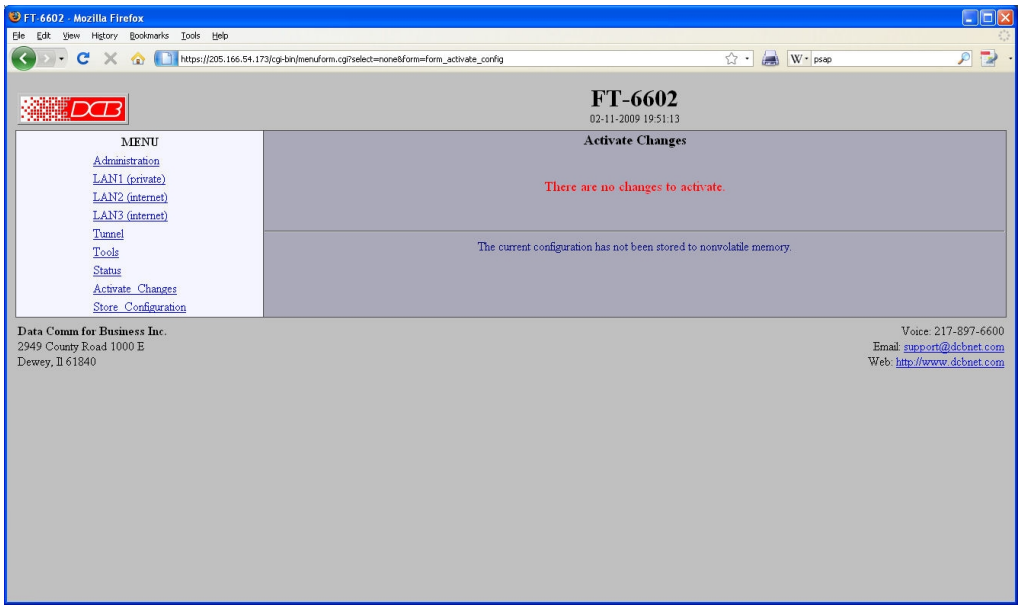
Store Configuration Screen



Store Configuration Screen

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

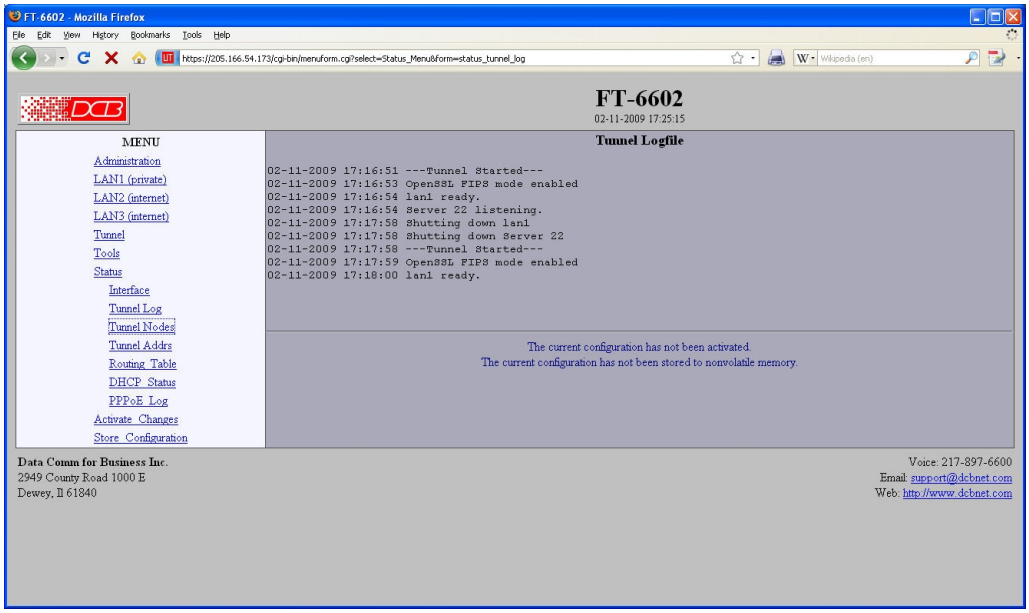
Activate Configuration Screen



Activate Configuration Screen

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

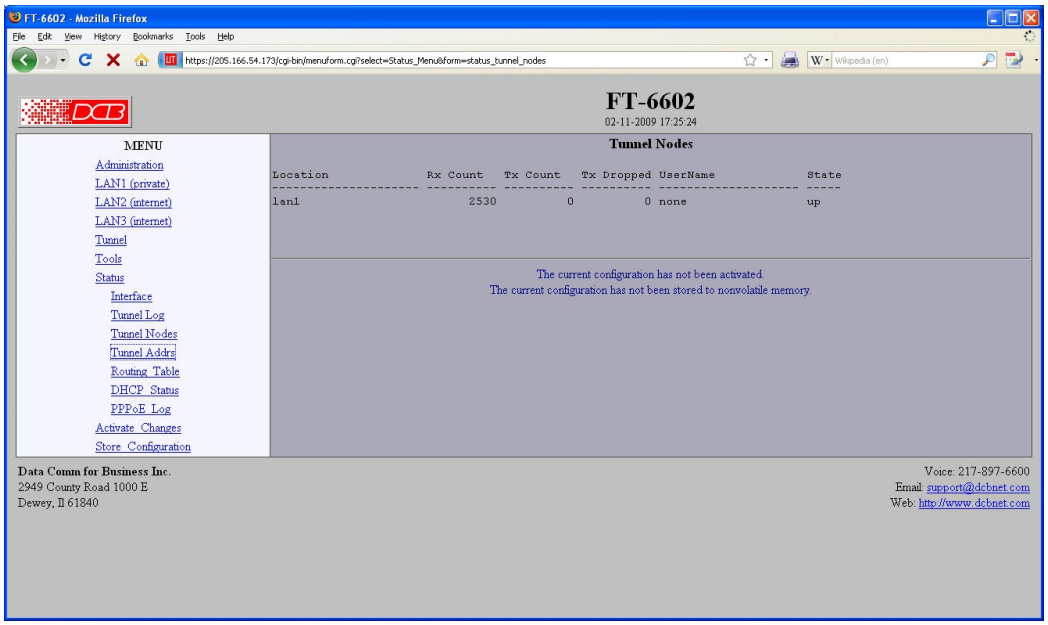
Tunnel Log Screen



Tunnel Log Screen

The Tunnel Log File Screen displays a record of all key changes, connections, authentications, and disconnects. It is quite useful in diagnosing connection problems.

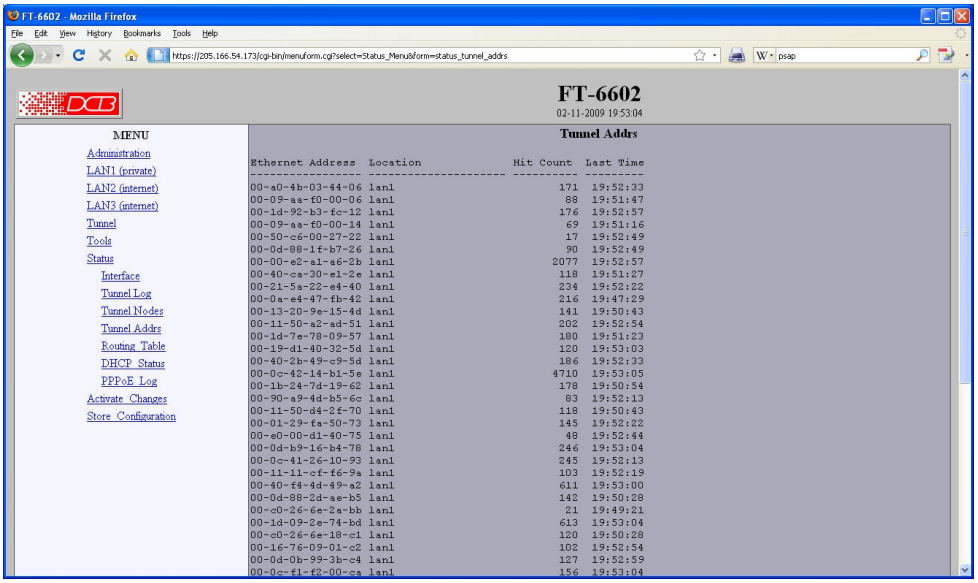
Tunnel Nodes Screen



Tunnel Nodes Screen

The Tunnel Nodes Screen displays currently connected remote nodes. These nodes are other FT-6602 units that have authenticated with this unit.

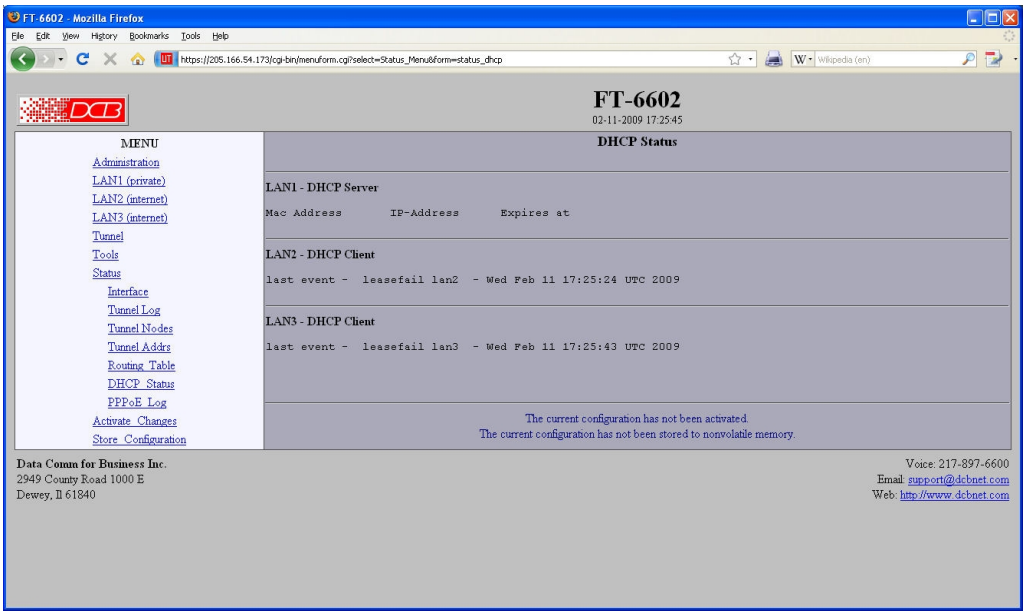
Tunnel Addresses Screen



Tunnel Addresses Screen

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

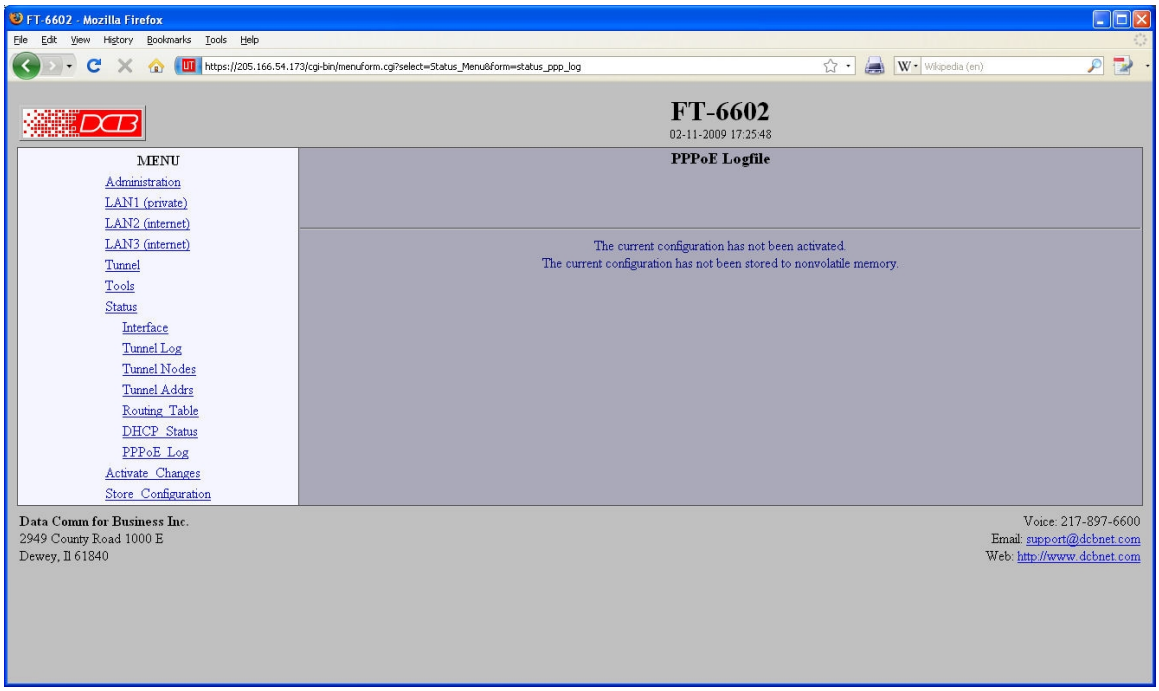
DHCP Status Screen



DHCP Status Screen

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

PPPoE Log



PPPoE Log Screen

The PPPoE Log screen displays recent PPPoE activity.

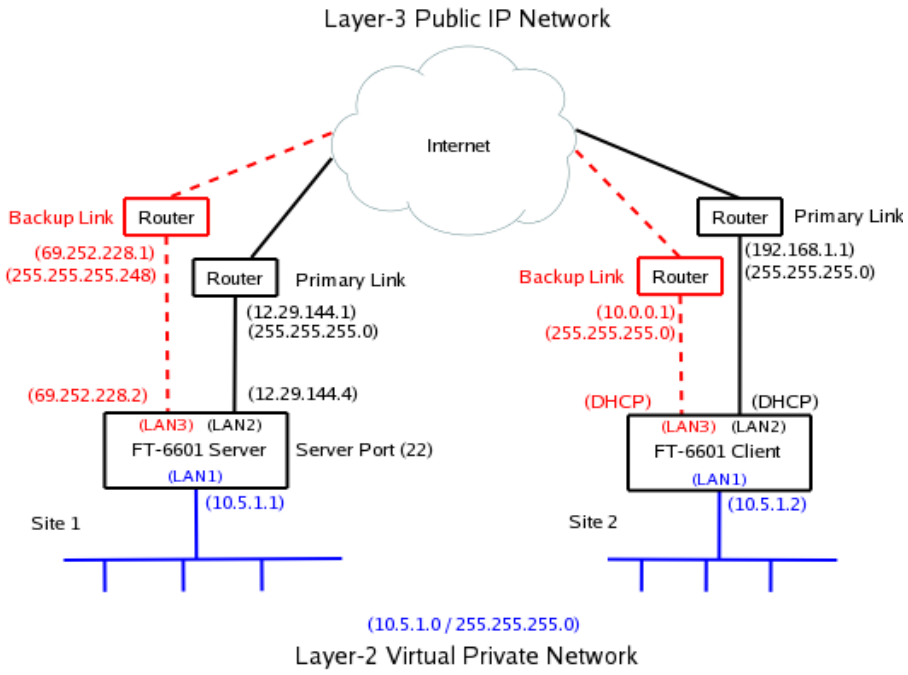
Chapter 5
Quick-Start Guide

This Chapter explains how to configure the FT-6602 for use.

Overview

This quick-start guide will walk you through the minimum steps necessary to setup a pair of FT-6602s to tunnel a private network over a public network. It will not go into detail, but will touch upon the steps and the order they should be performed. The steps should be repeated for each FT-6602 except where noted.

The FT-6602 uses a client-server architecture. One unit is designated as the server. It listens for connections from clients. One or more clients may be configured to connect to the server. For our walk-through, please refer to the following diagram. Addresses in the diagram are intended as an example. A blank copy of this diagram, which you may use to plan your configuration, can be found on the last page of this document.



Step 1: Setting Initial LAN1 IP address

LAN1's default IP address is 192.168.0.1 with a subnet mask of 255.255.255.0. LAN1 will also be running a DHCP server, assigning addresses in the range 192.168.0.101 through 192.168.0.109. You can skip to the next step if your computer is configured with an IP address on the 192.168.0.0/24 subnet.

You can change the LAN1 IP address and reset the FT-6602 to defaults through the COM port. The COM port operates at 9600 baud, 8 data, 1 stop, no parity, no flow control. You will need a null-modem cable to connect a PC COM port.

To enter serial setup mode, attach the serial cable and press <enter> on your terminal. You should then see a login prompt. Login using the name "setup" and follow the on-screen instruction.

Step 2: Accessing the Web Interface

To access the FT-6602's web interface use the following URL. Please note that it is https and not http.

https://192.168.0.1

Of course, if you changed the LAN1 IP address using the COM port, please use the new address in the above URL.

You will get a security warning, then the web browser should pop up an authentication screen. If this does not happen, see the Important Notes below. Login using the name "admin". Leave the password field blank. The name and password fields are case sensitive.

Important Notes:

- After initial TLS negotiation, some web browsers will display a blank page. If this happens, press the refresh button.
- Your web browser must support the TLS 1.0 protocol. If you have trouble connecting, check your web browser options to make sure TLS 1.0 is enabled. For IE, you will find the TLS 1.0 setting under Advanced/Settings. For Firefox you will find it under Preferences/Advanced/Security.
- Internet Explorer Version 7 and newer or Firefox version 2 or newer are recommended. Older versions of web browsers may fail due to TLS negotiation issues.
- Firefox, Netscape, and Mozilla will not use the TLS 1.0 protocol if they have encountered an error with a server. You must exit all instances of the browser then restart it to clear the error condition.

Setup through the web interface is performed through web forms. There is a menu bar on the left side of the window where you navigate and select the active form. The active form is displayed on the right. You

make changes to the form, then press the "submit" button to send the changes to the FT-6602. If you navigate to a different form without submitting it first, any changes will be lost.

As you go through the forms, you will notice that the each configuration item is hyper-linked. Clicking the hyper-link will take you to a help page describing the configuration item in more detail.

Step 3: Configure LAN1

LAN1 will reside on your private network. Navigate to the LAN1 – IP Configuration form. Set the IP address and subnet mask. The other fields on this page are typically not needed and may be left blank. After making any changes, don't forget to press the "submit" button.

The LAN1 DHCP server is enabled by default to make it easier to do initial setup. However, in most cases you will not want it running. It will interfere any other DHCP servers you may have on your network. Navigate to the LAN1 – DHCP_Server form. Disable the DHCP server, or configure it appropriately for you network.

Step 4: Activate Changes

If you changed any of the LAN1 settings, now is a good time to Activate Changes and switch over to using LAN1's new IP address. After you activate the changes, you will need to change the URL in your web browser to the FT-6602's new IP address.

Step 5: Store Configuration

If you had changes to activate, then you should now Store Configuration. It is usually best to activate changes first, then store them. This give you a change to verify that the changes are OK before committing them to non-volatile storage. If the changes were bad, you can simply power-cycle the unit and get back to your previously working configuration.

Step 6: Configure LAN2

LAN2 is the primary link to the Internet. Navigate to the LAN2 – IP Configuration form. Set the IP address, subnet mask, and gateway. Unlike the LAN1 configuration, a gateway address is almost always needed for LAN2. It should be the address of your Internet router. The other fields on this page are typically not needed and may be left blank.

LAN2 can also connect to the Internet using PPPoE. If your ISP requires PPPoE, navigate to the LAN2-Mode form and set the mode to PPPoE. Then navigate to the LAN2 - PPPoE Configuration form and set the configuration per you ISP's instruction. In most cases, you will only need to set the User Name and Password fields.

Step 7: Configure LAN3

If you have a secondary Internet connection it can be used as backup link. Configure LAN3 in the same manner as LAN2. Otherwise, navigate to the LAN3 – Mode form and disable it.

Step 8: Tunnel – Generate CA Key

This step will only be performed once. You should not repeat it for each FT-6602.

A USB flash drive was included with your FT-6602. Insert the USB flash drive into one of the USB ports on the FT-6602. Go to Tunnel – Generate CA Key form. Fill out the form. All of the fields, except the password fields, are informational. It really doesn't matter what you put in them, but its best to use information meaningful to you.

The two password fields are the most critical. On this form, you are creating the password. Enter the same password in both places. Make sure to use a password you can remember. You will need it later when you generate local keys.

Press the "submit" button, then wait patiently. Key generation is a slow process. Also, make sure to read any error messages. USB flash drives sometimes fail to register correctly. Upon error, it may be necessary to remove the USB drive, wait 5 or so seconds, then reinsert the drive.

If you forget your password, there is no way to recover it. Your only option is to generate new a CA key, which will overwrite the old one.

Step 9: Tunnel – Generate Local Key

Insert the USB flash drive, containing your CA Key, into one of the USB ports on the FT-6602. Navigate to the Tunnel – Generate Local Key form. For the name field, use a unique and descriptive name for the device. For example, the server FT-6602 could be named "Home Office Server" and the client FT-6602 could be named "Remote Office Client". The lifetime field specifies the number of days that the key is to be certified. Unless you plan to frequently change your keys, its best to choose a big number.

For the password field, enter the same password you set when you generated the CA key.

Press the "submit" button, then wait patiently. Key generation is a slow process. Also, make sure to watch for any error messages. USB flash drives sometimes fail to register

correctly. Upon error, it may be necessary to remove the USB drive, wait 5 or so seconds, then reinsert the drive.

Remove the USB Flash drive and store it in a safe place. You will need it in the future if you plan to add more client FT-6602 devices to your server.

Step 10: Tunnel – Mode

Navigate to the Tunnel – Mode form and select whether the FT-6602 is operating as the server or the client.

Step 11: Tunnel – Configuration (Server)

This step is only performed for the server tunnel.

The server will default to listening to TCP port 22. For most applications there is no need to change this value. However, if you need to use a different TCP port for you application, navigate to the Tunnel – Configuration form and set the port number. You may optionally have the server listen to a second port number, but again, this is usually not necessary.

Step 12: Tunnel – Configuration (Client)

This step is only performed for the client tunnel(s).

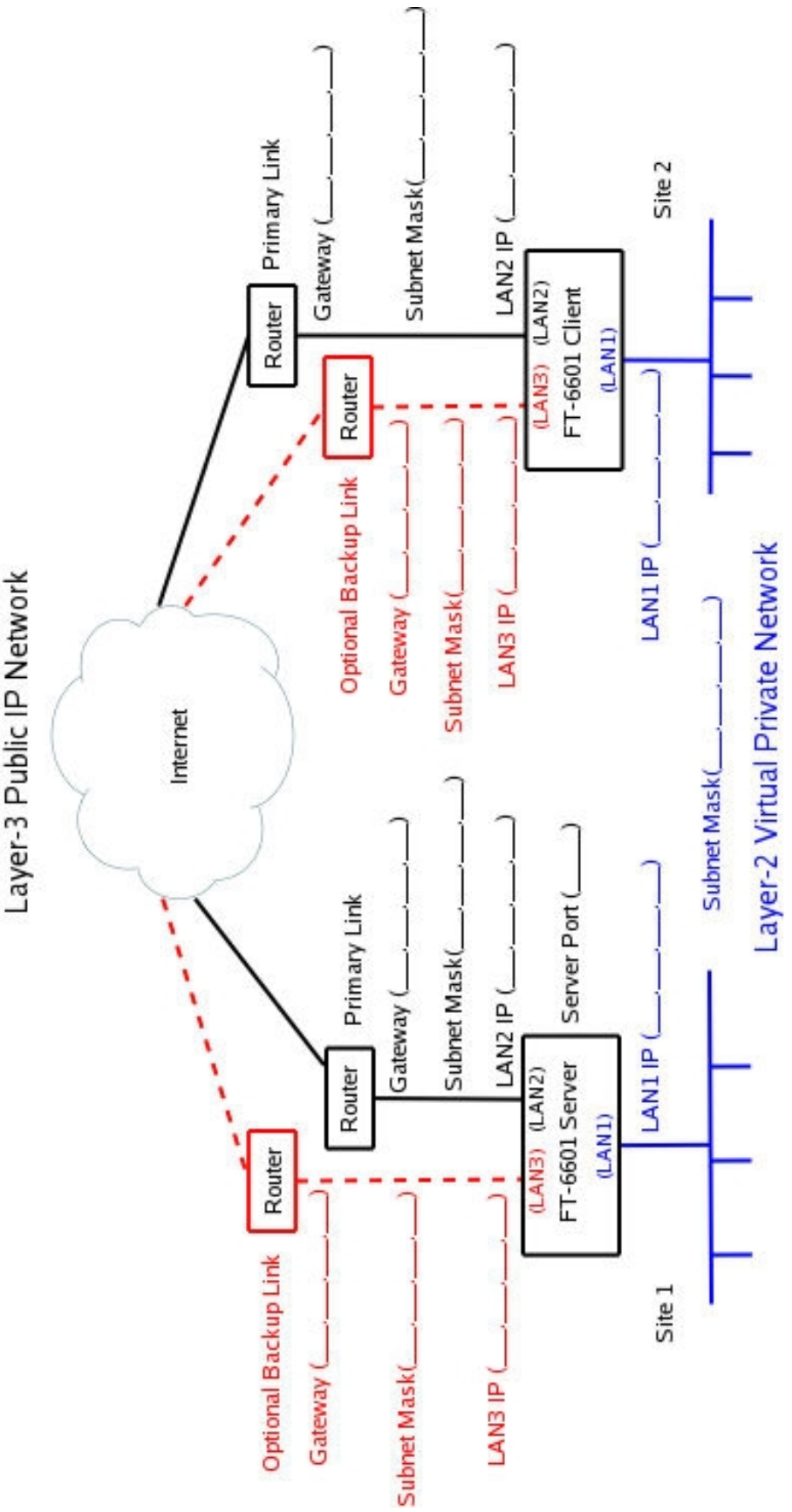
Navigate to the Tunnel – Configuration form. Set the "Connect to Server" field to the Server's LAN2 IP address. Referring to example setup, this would be the 12.29.144.4 address. Set the "port" field to the same port number set in the previous step. Set the "via interface" to LAN2.

If you have a backup Internet connection on LAN3, you can also set the fail-over fields. In our example configuration this wold be the 69.252.228.2 address. The "port" field is the same as above and the "via interface" would be LAN3.

Note: If you have a backup link at client side but not at the server side, it is OK to use the same "Connect to Server" for both the primary and fail-over settings. Only the "via interface" field needs to be different. Likewise, if you have a backup link at the server side but not at the client side, the "via interface" would both be set to LAN2 but the "Connect to Server" would differ for the primary and fail-over settings.

Step 13: Activate & Store Changes

Activate and save the final configuration. You can now navigate to the Status – Interface page and verify LAN interfaces. You can also navigate to the Status – Tunnel Log page to determine the state of the tunnel.


Layer-3 Public IP Network
Internet
Router
Primary Link
Gateway (___.___.___.___)
Subnet Mask(___.___.___.___)
LAN2 IP (___.___.___.___)
(LAN3)
(LAN2)
FT-6601 Client
(LAN1)
Site 2
Optional Backup Link
Gateway (___.___.___.___)
Subnet Mask(___.___.___.___)
LAN3 IP (___.___.___.___)
LAN1 IP (___.___.___.___)
Server Port (___)
FT-6601 Server
Site 1
Layer-2 Virtual Private Network

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 FT correctly ie. https:// instead of http:// .
- Start troubleshooting from a known state. Power the bridge OFF and ON to reboot.
- Is a proper IP address configured in the bridge and PC?
- "Ping" the bridge to see if it responds. From the Windows command prompt or "Run" dialog box, use the command:

  ```
  ping IP_Address
  ```

  Where `IP_Address` is the IP Address of the bridge (e.g. `ping 192.168.0.1`). If it does not respond, then check all LAN connections. If the LAN connection are OK, the problem is in the LAN addresses or routing **The most common problem cause is incorrect IP address configurations. Make sure the workstation and bridge have compatible IP addresses.**
- It may be that your "ARP table" contains invalid entries. You can clear the "ARP table" by rebooting, or, on Windows 95 , by typing the following command at the command prompt or *Run* dialog box.: `ARP * -d`
- Check that you are using the proper Ethernet connection on the bridge. Only Ethernet Port A works at 100BaseT on some models, and the port in use must be enabled. Ethernet Port A is the local, secure side.
- Is the FT configured to require a certificate on the web browser? If so turn that feature off and try connecting. (see the web browser certificate generation section).

- 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.
- Power is available... an LED is on.
- The terminal program is operating properly. Try a loopback connector at the bridge end of the cable to verify program operation and the proper COM: port.
- The most common problems causing this symptom are incorrect RS-232 wiring or the Windows Hyperterm program not operating correctly.

Checking Bridge Operation

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

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

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

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

Appendix A
Specifications

FT-6602 Bridge Specifications

- Flash Memory:
- DRAM:
- LAN 1 Interface: 10/100/BaseT, Autosense
- LAN 2 Interface: 10/100/BaseT, Autosense
- LAN 3 Interface: 10/100/BaseT, Autosense
- OS: uCLinux
- Power: 7-20 VDC 4 watts average, 6 watts maximum
  or Optional power supplies.
  Supplied with 100-240 VAC external supply
- Stand alone package
- Throughput: greater than 10 Mbps
- Supports 50 simultaneous client FTs
- LED: (LAN Activity, LAN Status (per interface), Power)
- Default IP address: 192.168.0.1
- Internal Certificate Authority and key generation
- Browser Management port: 443 SSL
- Operational Temperature -20C to +70C
- Dimensions 6 ¼ x 6 x 1 inches

FT-6630 Bridge Specifications

- Flash Memory: 128 M bytes or more
- DRAM: 1 GB or more
- LAN A Interface: 10/100/1000BaseT, Autosense
- LAN B Interface: 10/100/1000BaseT, Autosense
- CPU: Xenon dual core 2.4 Ghz
- OS: Linux
- Power: 120 VAC or 240 VAC, 260 Watts Maximum
- Rack-mount: 1U high
- Throughput: greater than 120 Mbps
- Supports 50 simultaneous client FTs
- LED: (Over-temperature warning, LAN Activity, LAN Status (two per interface), Power)

- Default IP address: 192.168.0.1
- Authentication with built-in database using certificates
- Browser Management port: 443 SSL
- Operational Temperature 0C to +50C

RS-232 PIN Assignments – Management Port

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

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

RS-232 Port Pin Assignments

Control Signal Operation

DCD

Input.

Receive Data

Input, data into the bridge

Transmit Data

Output, Data from the bridge

DTR

Output.

Signal Ground

Common ground

DSR

Input. Ignored

RTS

Output.

CTS

Input.

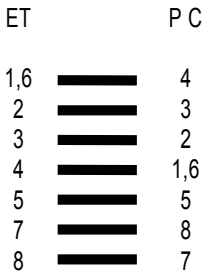
Ring Indicator

Not used

Cables

Commonly used cable connections:

To PC 9-pin COM: port



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

Bridge to hub or ethernet switch

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

Appendix B

Open Source Software Information

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

Introduction

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

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

Obtaining the Source Code

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

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

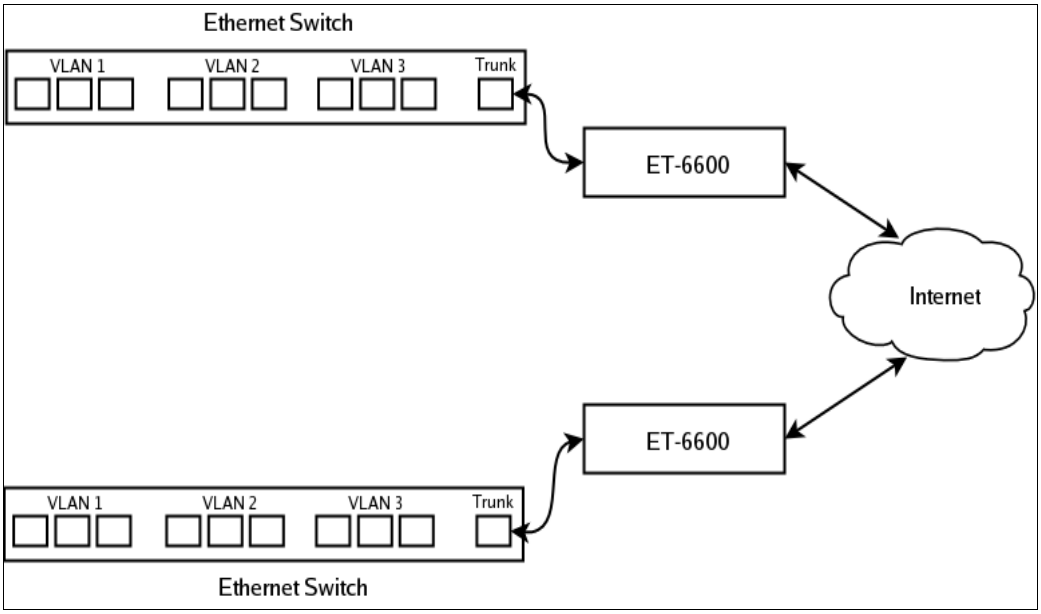
Appendix C

802.1Q VLAN Tagging

The FT-6602 supports bridging of 802.1Q VLAN packets.

Introduction

The FT-6602 supports bridging 802.1Q Tagged Ethernet. An application for this is shown below (using ET-6600 units as an example) where two 802.1Q VLAN switches are being tunneled across the Internet.



VLAN Configuration Differences

The default configuration for the FT is for Standard Ethernet. You cannot attach LAN 1 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 LAN 1 to a VLAN trunk. If you answer "yes", it will then ask for a VLAN ID. When you complete serial setup, you can attach LAN 1 to the VLAN trunk and will be able to access the FT from the VLAN that you specified. In other words, if you set the VLAN ID to 2, you will be able to access the FT 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 FT 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 FT, as it's seeing the ethernet port as a trunk port.