

FT-Series

Encrypted Ethernet

Tunnel

User's Guide

Revised March 21, 2025

Firmware Version 4.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..2025 All rights reserved.

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

RoHS

All current hardware models are RoHS compliant.



TABLE OF CONTENTS

Table of Contents

FCC Statement.....	i
RoHS.....	i
Chapter 1 Introduction.....	7
FT Applications.....	7
Other Features.....	8
Protocols.....	8
FIPS 140-2.....	8
Ethernet Filtering.....	8
802.1q VLAN.....	8
Upgradeable Firmware.....	8
Security and Firewall Features.....	8
On-board Tools.....	8
Single-Interface operation.....	8
Package Contents.....	8
Software Requirements.....	9
FT-6602 Specific.....	10
Introduction.....	10
Configuration Options.....	10
FT-6602 Front Panel.....	10
Rear Panel LED Indicators.....	10
Rear Panel RS-232 Connector.....	10
Rear Panel Ethernet Connectors.....	10
Rear Panel USB Connectors.....	10
FT-6632 Specific – Two High Performance Ports.....	12
Introduction.....	12
Configuration Differences.....	12
FT-6632 Front Panel.....	12
FT-6632 Front Panel LED Indicators.....	12
FT-6632 Front USB Connectors.....	12
FT-6606.....	13
Introduction.....	13
Configuration.....	13
Rear Panel LED Indicators.....	13
Front Panel LED Indicators.....	13
Ethernet Connectors.....	14
FT-6615.....	15
Introduction.....	15
Configuration.....	15
Ethernet Port LED Indicators.....	15

Panel Indicators.....	15
USB Connectors.....	15
HDMI Connectors.....	16
Audio Connector.....	16
RS-232 COM Port.....	16
Ethernet Connectors.....	16
FT-Soft.....	17
Introduction.....	17
Configuration.....	17
FT-Soft Log Window.....	18
Virtual Ethernet Adapter.....	18
Chapter 2 Installation.....	19
Overview.....	19
Quick Start.....	19
Help Screens and Field Edits.....	19
Installation and Configuration.....	19
1. Configure the Bridge's IP address.....	19
2. Connect the Ethernet Cable.....	21
3. Verify the IP Address Configuration.....	21
4. Enter Your Configuration.....	22
5. Minimum Configuration.....	22
Chapter 3 The Configuration Process.....	23
Overview.....	23
Using the Configuration Flexibility.....	23
Configuration Process Examples.....	24
Change, test then save.....	24
Change, save, then reset.....	24
Restore with a saved configuration.....	24
Chapter 4 Configuration.....	25
Overview.....	25
Administration.....	25
Admin Password.....	26
Fields.....	26
Notes.....	26
Admin Access Control.....	27
Fields.....	27
Notes.....	27
Web Server Firewall.....	28
Fields.....	28
Notes.....	29
New Web Certificate.....	30
Fields.....	30
Notes.....	31
Set Clock.....	32

Fields.....	32
Notes.....	32
Set Name.....	33
Fields.....	33
Remote Syslog.....	34
Fields.....	34
Set All Defaults.....	35
Configuration File.....	36
Fields.....	36
Notes.....	36
Firmware Upgrade.....	37
Fields.....	37
Notes.....	37
System Reboot.....	38
Fields.....	38
Notes.....	38
Version Information Screen.....	39
LAN 1 Ethernet Mode.....	40
Fields.....	40
Notes.....	40
LAN 2/3/4 Ethernet Mode.....	41
Fields.....	41
Notes.....	41
LAN1 IP Configuration.....	42
Fields.....	42
Notes.....	43
LAN2/3/4 IP Configuration.....	44
Fields.....	44
Notes.....	45
LAN1/2/3/4 IPv6 Configuration.....	46
Fields.....	46
Notes.....	47
DHCP Server Configuration.....	48
Fields.....	48
Notes.....	48
Ethernet PPPoE Configuration.....	49
Fields.....	49
Tunnel Mode.....	51
Fields.....	51
Encrypted Tunnel Configuration.....	52
Fields.....	52
Server Mode Enabled:.....	52
Client Mode Enabled:.....	52
On Failure: (Optional).....	53
Notes.....	53
Generate Certificate Authority Key.....	54
Fields.....	54

Notes.....	55
Generate Local Key.....	56
Fields.....	56
Notes.....	56
Advanced Tunnel Configuration.....	57
Fields.....	57
Notes.....	58
Ethernet (MAC) Address Filters Screen.....	59
Fields.....	59
Notes.....	60
IP Address Filters Screen.....	60
Fields.....	60
Notes.....	61
UDP Address Filters Screen.....	62
Fields.....	62
Notes.....	63
TCP Address Filters Screen.....	63
Fields.....	63
Notes.....	64
Server Firewall.....	65
Fields.....	65
Notes.....	65
Ping Screen.....	67
Fields.....	67
Notes.....	67
Traceroute Screen.....	68
Fields.....	68
Notes.....	68
Packet Sniffer Screen.....	69
Fields.....	69
Notes.....	69
Interface Status Screen.....	70
Routing Table Screen.....	71
Store Configuration Screen.....	72
Activate Configuration Screen.....	72
Tunnel Log Screen.....	73
Tunnel Nodes Screen.....	73
Tunnel Addresses Screen.....	74
DHCP Status Screen.....	74
PPPoE Log.....	75
Audit Ports.....	76
IPv4 Firewall.....	77
IPv6 Firewall.....	78
FIPS Module Status.....	79
FT-Soft Tunnel Configuration.....	80
Fields.....	80

Notes.....	81
FT-Soft Generate Local Key.....	82
Fields.....	82
Notes.....	82
Chapter 5 Quick-Start Guide.....	84
Overview.....	84
Step 1: Setting Initial LAN1 IP address.....	84
Step 2: Accessing the Web Interface.....	85
Step 3: Configure LAN1.....	85
Step 4: Activate Changes.....	86
Step 5: Store Configuration.....	86
Step 6: Configure LAN2.....	86
Step 7: Configure LAN3.....	86
Step 8: Set the Clock.....	86
Step 9: Tunnel – Generate CA Key.....	86
Step 10: Tunnel – Generate Local Key.....	87
Step 11: Tunnel – Mode.....	87
Step 12: Tunnel – Configuration (Server).....	87
Step 13: Tunnel – Configuration (Client).....	88
Step 14: Activate & Store Changes.....	88
Chapter 6 Troubleshooting.....	90
Hardware Problems.....	90
Can't Connect via the LAN.....	90
Other Problems.....	91
Checking Bridge Operation.....	91
Certificate Errors.....	91
Appendix A Specifications.....	93
FT-6602 Bridge Specifications.....	93
FT-6606 Bridge Specifications.....	94
FT-6615 Bridge Specifications.....	95
FT-6632 Bridge Specifications.....	96
FT-Soft Specifications.....	97
RS-232 PIN Assignments – Management Port.....	98
Control Signal Operation.....	98
DCD.....	98
Receive Data.....	98
Transmit Data.....	98
DTR.....	98
Signal Ground.....	98
DSR.....	98
RTS.....	98
CTS.....	99
Ring Indicator.....	99

Cables.....	99
To PC 9-pin COM: port.....	99
FT-6615 Serial (COM) Port.....	99
Bridge to hub or Ethernet switch.....	100
Appendix B Open Source Software Information.....	101
Introduction.....	101
Obtaining the Source Code.....	101
Appendix C 802.1Q VLAN Tagging.....	102
Introduction.....	102
VLAN Configuration Differences.....	102

Chapter 1

Introduction

This chapter provides an overview of the FT Series Bridge features and capabilities.

Congratulations on the purchase of your new FT Series Bridge. This is a simple, easily configured tunneling device containing up to 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 140-2 level-1 certified encryption module and AES-256 encryption.

The bridge transports all valid Ethernet protocols. It provides a virtual private network by bridging the LANs over an IP tunnel that is 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 encrypted communication between the FT devices is based on the TLS protocol. Authentication utilizes X.509 certificates. The FT devices are capable of generating a private Certificate Authority on a USB attached drive and then generating signed local keys from that Certificate Authority.

This manual corresponds to FT firmware version 4.x. Firmware version 4.x is **not fully compatible with firmware versions 3.x and prior. Please see the DCB document, *FT v4.x Migration Guide*, for information on moving an existing application forward.**

FT Applications

The FT 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. Multiple client FT devices connect to a central FT server. The server acts as the relay point. All sites, including the server site, have full layer-2 communication. The server will relay network packets between the remote sites as needed.

In some applications, the FT 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.

FIPS 140-2

The FT series uses a FIPS 140-2 level-1 validated cryptographic module, developed by the OpenSSL Software Foundation. At the time of this writing, the certificate is #4282. This is subject to modification. Contact DCB for current certificate information.

DHCP Protocol

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

Ethernet 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 any web browser that supports TLS v1.2 or v1.3. Older 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 FT uses TLS v1.2 or v1.3 as the transport protocol and limits the encryption algorithm to FIPS supported mode of AES-256.

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 bridge may be configured in a “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
- 2 – standard Ethernet cables.
- A null-modem serial cable for models with a serial port.
- USB flash drive 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 (Microsoft Edge, Chrome, or Firefox are recommended.) may be used for configuration once the FT device is configured with a valid IP address. Web browsers that predate support for TLS v1.2 or later will be unable to establish communication. The use of a secure web server connection for configuration (<https://>) is required.

FT-6602 Specific

The FT-6602 is a discontinued model. For new applications, please consider the FT-6615.

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, broadband modem, or cable modem. This model supports 25 simultaneous remote units with a maximum throughput of approximately 10Mbps.

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 FT) (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 FT) activity.

Rear Panel RS-232 Connector

The DE-9 (PC 9-pin) connector is used for command line setup. A null-modem 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" stored on a USB flash drive.

FT-6632 Specific – Two High Performance Ports

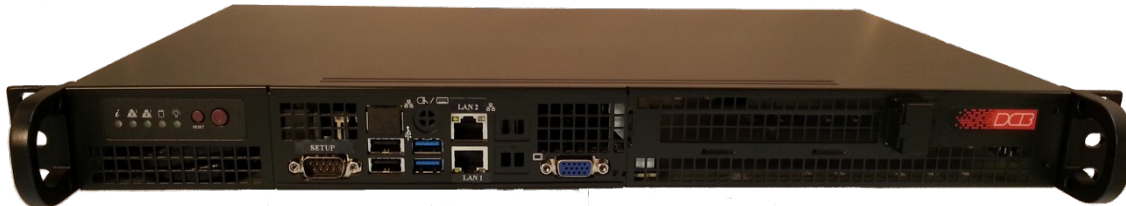
The FT family consists of various models with different internal hardware or firmware options. The FT-6632 includes two 10/100/1000BaseT High Performance Ethernet ports.

Introduction

The FT-6632 bridge contains two gigabit Ethernet ports and may be used at the head end to support multiple remote FT products or for high performance links. It is often connected directly to an Ethernet WAN connection using a public high speed network, broadband modem, or cable modem. This model supports 50 simultaneous remote units and approximately 720Mbps 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. In addition, the device can support a VGA monitor and USB keyboard for initial setup. 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](https://IP_Address)).



FT-6632

FT-6632 Front Panel

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

FT-6632 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.

FT-6632 Front USB Connectors

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

FT-6606

The FT-6606 is a discontinued model. Please consider the FT-6615 as a replacement.

Introduction

The FT-6606 model contains two untrusted Ethernet ports, one trusted Ethernet port supporting VLAN tagging, and one serial port. It is designed for operation with a direct wired Ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, satellite, Cable modem, or any network path terminating in copper Ethernet. It supports up to 25 simultaneous remote FT clients when in server mode and a maximum throughput of approximately 40Mbps.

Configuration

This model contains a serial interface that may be used for initial setup (if needed). If the default IP address (192.168.0.1) is not appropriate for your LAN, connect a terminal to the serial port following the instructions in the configuration section. If enabled, the setup port is always active on this model. Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are required for additional configuration.



FT-6606

Rear Panel LED Indicators

One set of indicators For Each Ethernet Port

- The green LED to the left of each Ethernet port is a LAN activity indicator. This LED flashes with activity on the Ethernet (even if the activity isn't directly to this unit).
- The yellow/green LED to the right of each Ethernet port is the Ethernet Status indicator. It is lit amber when the port is connected to a 1000BaseT switch, green for 100BaseT. It is not lit for 10BaseT connections.

Front Panel LED Indicators

- Power indicator. It should be on.

RS-232 Panel Connector

The DE-9 (PC 9-pin) connector is used for initial IP addressing setup and a TDP/UDP terminal server connection. **A null-modem cable is required to use this with any standard PC serial port.** Terminal configuration is 9600 bps, 8N1.

Ethernet Connectors

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

FT-6615

The FT family consists of various models with different internal hardware or firmware options. The FT-6615 includes four 10/100/1000BaseT Ethernet ports. It supports up to 25 clients and throughput rates up to 125Mbps.

Introduction

The FT-6615 model contains three untrusted Ethernet ports, one trusted Ethernet ports, and one serial port. It is designed for operation with a direct wired Ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, satellite, Cable modem, or any network path terminating in copper Ethernet. It supports up to 25 simultaneous remote FT clients when in server mode and a maximum throughput of approximately 125Mbps.

Configuration

This model contains a serial interface that may be used for initial setup (if needed). If the default IP address (192.168.0.1) is not appropriate for your LAN, connect a terminal to the serial port following the instructions in the configuration section. If enabled, the setup port is always active on this model. Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are required for additional configuration.



FT-6615

Ethernet Port LED Indicators

One set of indicators for each Ethernet port

- The green LED to the left of each Ethernet port is a link status indicator.
- The yellow LED to the right of each Ethernet port is an activity indicator. It flashes with all network activity

Panel Indicators

- Red LED – internal SSD activity indicator
- Green power indicator.
- Blue power switch indicator.

USB Connectors

There are two USB connectors. A USB keyboard and HDMI monitor may be used for initial configuration. Either USB connector may be used

HDMI Connectors

There are two HDMI connectors. A USB keyboard and HDMI monitor may be used for initial configuration. Either HDMI connector may be used.

Audio Connector

The device has an audio connector that is unused for this application.

RS-232 COM Port

The device supports a RS-232 COM port implemented on a RJ45 connector. A cable is supplied with the device that allows the port to be directly connected a standard PC DE9 COM port. The COM port may be used for initial configuration or may be configured to support a terminal server feature. The default COM port configuration is *setup mode, 9600 bps, 8N1*.

Ethernet Connectors

The four 10/100/1000BaseT connectors are auto-sensing. Only LAN1 may be used for initial configuration via a web browser.

FT-Soft

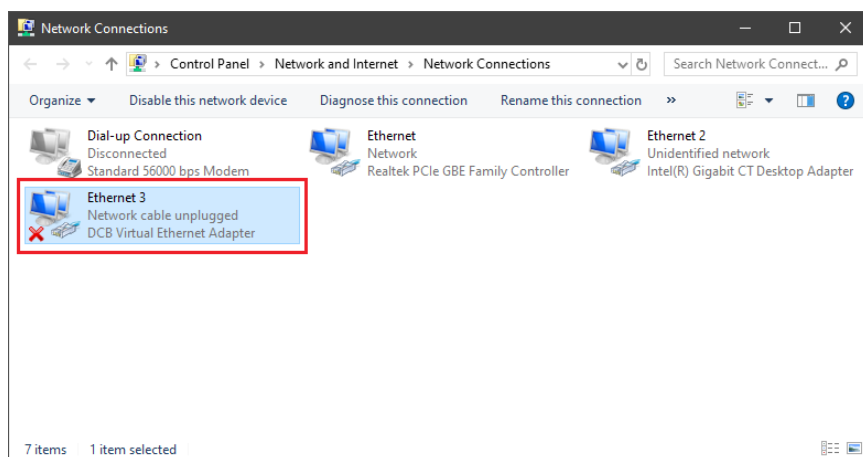
FT-Soft is a software implementation of an FT client that runs on Windows. It provides an Ethernet level (layer-2) attachment between the PC and a private FT network.

Introduction

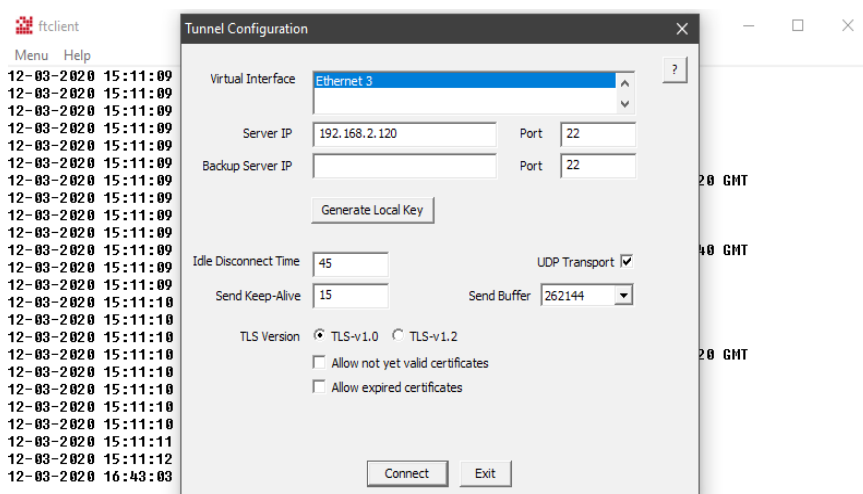
FT-Soft is a software package that runs on x86 Windows PCs. The software package emulates an FT client device. The PC's native network connection serves as the public or untrusted network interface. A virtual Ethernet Adapter, emulated by the FT-Soft package, serves as the private or trusted network interface.

Configuration

FT-Soft consists of two components, a virtual Ethernet adapter and the FT-Soft client. The virtual Ethernet adapter is a Windows NDIS Ethernet driver. Configuration is performed through the system's network connection control panel, similar to configuration of a native Ethernet adapter.



The FT-Soft client is a user-level application. It provides the conduit between the remote FT server device and the virtual Ethernet adapter. Configuration is performed through the FT-Soft GUI.



FT-Soft Log Window

While FT-Soft is running, a log window is available to show the current status of the connection and to show any events that have occurred.

Virtual Ethernet Adapter

Link status tracks the connection state. When the client is connected to the server, the link state is up. When not connected, the link state is down.

Chapter 2

Installation

This Chapter details the installation process for the FT Series Bridge.

Overview

Note: The factory default configuration for the FT, a DHCP server is enabled on the LAN1 interface. If your PC is configured to “obtain an IP address automatically”, you can simply connect your PC directly to the LAN1 interface and it will be assigned an address in the 192.168.0.0/24 subnet.

The FT device 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 <https://192.168.0.1> (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. Please note the use of secure https. The FT Series bridges will not respond to http.

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 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.

```
Welcome to the FT-6615 v4.03
To start the Setup Program, login with
the name: setup
FT-6615 login: setup
```

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”.

```
----- FT-6615 Setup Program -----

Welcome to Setup. This setup will establish the FT-6615 in
a known state so that you can configure it via a Web Browser.
It will allow you to configure the LAN1 IP address
subnet mask, and gateway. You also have the option to set all
parameters to default, which is the only method to remove
security parameters.

HTTPS port: 443
LAN1 Configuration:
  IP: 192.168.0.1
  SM: 255.255.255.0
  GW:

Set ALL parameters to default (y/[n])? y
```

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 LAN1, answer “y”, otherwise answer “n”.

```
Should LAN1 use DHCP to get an IP address (y/[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 LAN1 interface.
8. The bridge will now save the configuration to flash memory. Once complete, it will reboot.

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.

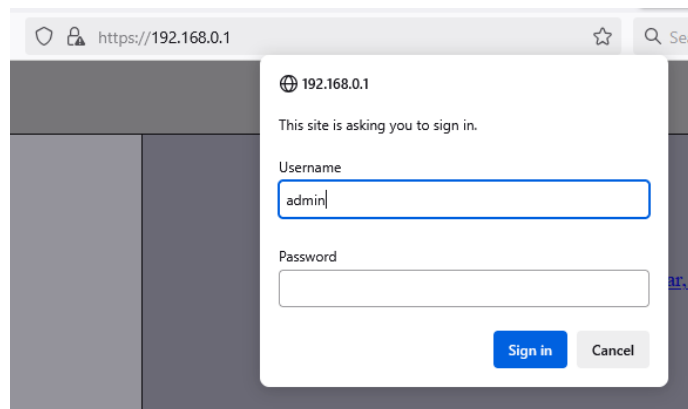
9. The bridge will now reboot.

2. Connect the Ethernet Cable

Connect a LAN cable from your hub or switch to LAN1. 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 <https://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. The DHCP server will be running on LAN1. If you plan to use static addressing on your trusted network or have a router on the network, make sure to disable the FT's DHCP server. The network should only have one primary DHCP server.
3. 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.
4. Tunnel Mode: One FT device will be configured for server mode. The other FT device will be configured for client mode.
5. 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 needed.
6. Generate a Certificate Authority (CA) on the a USB flash drive. Only do this once. Both FT devices will share the same CA.
7. Generate a local key for each FT device, using the previously generated CA.

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 instructions.

Chapter 3

The Configuration Process

This Chapter describes the configuration management process on the FT-66xx bridge using a Web Browser.

Overview

The FT-66xx bridge contains a 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 from 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: A web browser that supports TLS v1.2 or v1.3 is required. Web browsers running under Windows 7 and prior will probably not work.

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 *save*, 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

Transfer 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 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.

Chapter 4

Configuration

This Chapter describes configuration screens and some configuration hints for the FT Series Bridge

Overview

The FT-66xx 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: A web browser that supports TLS v1.2 or v1.3 is required. Web browsers running under Windows 7 and prior will probably not work.

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

The screenshot shows a web interface for an FT-6615 device. At the top left is the DCB logo. The title is 'FT-6615' with a timestamp '03-20-2025 15:25:11'. A 'MENU' sidebar on the left lists options: Administration, Admin Password, Access Control, Web Server Firewall, New Web Certificate, Set Clock, Set Name, Remote Syslog, and Set All Defaults. The main content area is titled 'Admin Password' and contains a form with the following fields: 'Username' (pre-filled with 'admin'), 'Old Password', 'New Password', and 'Verify New Password'. Below the form are 'Submit' and 'Cancel' buttons.

Admin Password Screen

Initial access to the web server screens are available ONLY via the secure side of the bridge. Access to the 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 or Console 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

DCB **FT-6615**
03-20-2025 15:30:53

MENU

- [Administration](#)
- [Admin Password](#)
- [Access Control](#)
- [Web Server Firewall](#)
- [New Web Certificate](#)
- [Set Clock](#)
- [Set Name](#)
- [Remote Syslog](#)
- [Set All Defaults](#)
- [Config File](#)
- [Firmware Upgrade](#)
- [System Reboot](#)
- [Version Info](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)

Admin Access Control

Web Server Port

LAN Web Access

Lan1 Web Access disable enable

Lan2 Web Access disable enable

Lan3 Web Access disable enable

Lan4 Web Access disable enable

Ping Response

Lan1 Ping Response disable enable

Lan2 Ping Response disable enable

Lan3 Ping Response disable enable

Lan4 Ping Response disable enable

NOTE: Changes to Web Access for interfaces operating in PPP or PPPoE mode will not take effect until the current PPP session stops and restarts. To insure the interface is protected reset the unit.

WARNING: Make changes very carefully. It is possible to block out your current web session.

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 a local firewall.

If you change the web server port number to any value other than 443, remember that you will have to include the port number in your URL. For example, <https://192.168.0.1:7995>
- **LAN 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. If access must be allowed from a public interface, it is recommended to change the admin username and to use a strong password. Also, use the *Web Server Firewall* to limit access.
- **Respond to Ping**
This item allows you to block ping requests (ICMP echo) 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.

Notes

Remember to submit the change by clicking the "SUBMIT" button.

Previous versions of FT firmware allowed the user to configure a list of allowed IP addresses to administer the device. This functionality has been replaced by the Web Server Firewall.

Web Server Firewall

DCB FT-6615
03-20-2025 15:40:06

MENU

- [Administration](#)
- [Admin Password](#)
- [Access Control](#)
- [Web Server Firewall](#)
- [New Web Certificate](#)
- [Set Clock](#)
- [Set Name](#)
- [Remote Syslog](#)
- [Set All Defaults](#)
- [Config File](#)
- [Firmware Upgrade](#)
- [System Reboot](#)
- [Version Info](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)

Web Server Firewall

Web Server Firewall disable enable

Policy accept-all drop-all

	Source IP	Action
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Page: 1 2

Submit Cancel

Web Server Firewall Screen

The Web Server Firewall may be used to block nuisance connection attempts to the Tunnel's HTTPS port. The rules in the table are applied when a browser attempts to connect to the web server. If the browser's IP address matches a rule, the specified action is taken. If none of the rules match, the policy rule will be applied.

The rules in the table are applied in sequential order. With this, it is possible to build either an allowlist, a denylist, or a combination of the two. For example, to build an allowlist, you would enter the IP address of each browser device with an ACCEPT action". The policy would be set to drop-all.

Fields

- **Web Server Firewall Enable/Disable**
This option allows the firewall to be easily enabled or disabled while retaining the policy and rule configuration.

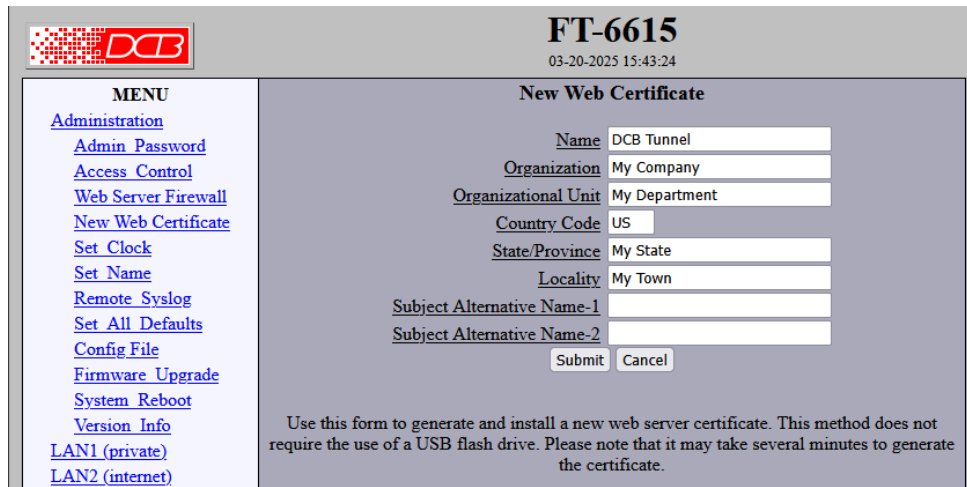
Note: if you enable the firewall with a policy of "drop-all", make sure you have at least one rule to allow your PC's IP address. Otherwise you will lock yourself out.
- **Policy**
This is the action that will be taken when the source address of a web browser does not match any of the rules listed in the table. The choices are to either **accept** the connection or to **drop** the connection.
- **Source IP**
The source IP may be specified as a single address or specified as an address/netmask or address/bits subnet. Both IPv4 and IPv6 addresses are allowed. (see the notes for examples)
- **Action**
This option selects the action to take when the incoming IP address matches the rule. The action may be to DROP or ACCEPT the network packet. If no action is specified, the rule is ignored.

Notes

Examples of Source IP rules:

- | | |
|----------------------------|-------------------------------|
| 192.168.10.50 | - Single address |
| 192.168.10.0/255.255.255.0 | - Class C subnet 192.168.10.0 |
| 192.168.0.0/16 | - Class B subnet 192.168.0.0 |
| 0.0.0.0/0 | - All IPv4 addresses |
| 2001:db8:78:1::50 | - Single IPv6 address |
| 2001:db8:78:1::/64 | - IPv6 subnet |
| ::/0 | - All IPv6 addresses |

New Web Certificate



FT-6615
03-20-2025 15:43:24

MENU

- [Administration](#)
- [Admin Password](#)
- [Access Control](#)
- [Web Server Firewall](#)
- [New Web Certificate](#)
- [Set Clock](#)
- [Set Name](#)
- [Remote Syslog](#)
- [Set All Defaults](#)
- [Config File](#)
- [Firmware Upgrade](#)
- [System Reboot](#)
- [Version Info](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)

New Web Certificate

Name DCB Tunnel
Organization My Company
Organizational Unit My Department
Country Code US
State/Province My State
Locality My Town
Subject Alternative Name-1
Subject Alternative Name-2

Submit Cancel

Use this form to generate and install a new web server certificate. This method does not require the use of a USB flash drive. Please note that it may take several minutes to generate the certificate.

New Web Certificate Screen

This form allows a new X.509 web certificate to be generated for the device, allowing the user to set the descriptive fields in certificate. The new certificate will replace the current certificate.

Fields

- **Name**
The common name given to the certificate. 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.
- **Locality**
The city or town name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.
- **Subject Alternative Name 1**
This field is optional. It allows alternative names to be added to the certificate. The alternative name may be a DNS name or an IP address.
- **Subject Alternative Name 2**
This field is optional. It allows alternative names to be added to the certificate. The alternative name may be a DNS name or an IP address.

Notes

By including the IP address of the device as a Subject Alternate Name in the certificate, it will eliminate the *Name Mismatch* error reported by some web browsers.

Set Clock

FT-6615
03-20-2025 15:45:11

MENU
[Administration](#)
[Admin Password](#)
[Access Control](#)
[Web Server Firewall](#)
[New Web Certificate](#)
[Set Clock](#)
[Set Name](#)
[Remote Syslog](#)
[Set All Defaults](#)
[Config File](#)
[Firmware Upgrade](#)

Set Clock

Clock changes take effect when you submit the page.
You do not need to activate or store clock changes.

Year (2000-2035) 2025
Month (1-12) 3
Day (1-31) 20
Hour (0-23) 15
Minute (0-59) 45
Submit Cancel

Set Clock Screen

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

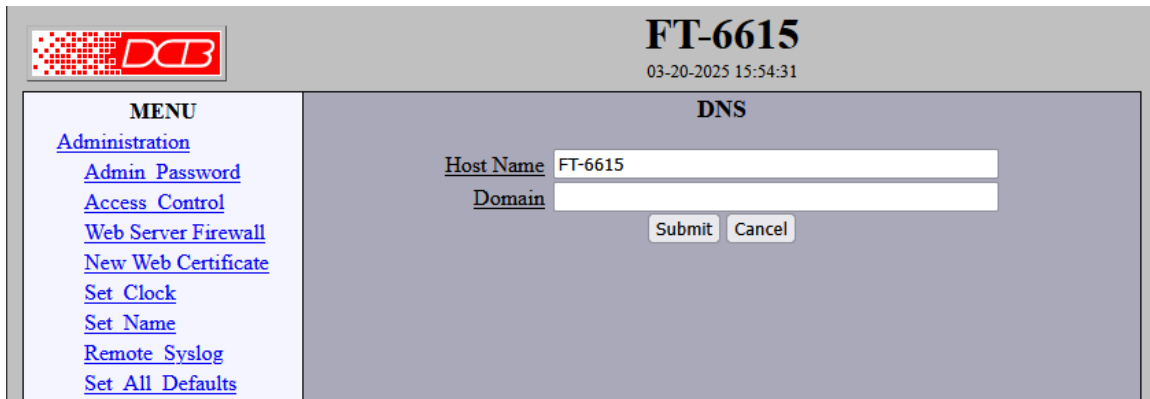
Fields

- 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

- If an NTP server is available, consider using the NTP feature found under tools to maintain the time.
- Even when the NTP feature is not enabled, the NTP time-zone setting will be applied to the time as displayed by the device.

Set Name



The screenshot shows a web interface for configuring a device. At the top left is the DCB logo. The main title is "FT-6615" with a timestamp "03-20-2025 15:54:31". Below this is a "MENU" section with links: Administration, Admin Password, Access Control, Web Server Firewall, New Web Certificate, Set Clock, Set Name, Remote Syslog, and Set All Defaults. The "Set Name" link is highlighted. To the right is the "DNS" configuration section, which includes a "Host Name" field containing "FT-6615" and an empty "Domain" field. Below these fields are "Submit" and "Cancel" buttons.

Set Name Screen

This form allows you to set the DNS Host Name and Domain for the unit. The FT is not running a local DNS server. This configuration has little effect on the unit.

Fields

Host Name	The DNS host name for the device.
Domain	The DNS default domain for the device.

Remote Syslog

The screenshot shows the configuration interface for the FT-6615 device. At the top, it displays the device name 'FT-6615' and the date/time '03-20-2025 16:03:04'. The main title is 'Remote Syslog'. On the left is a 'MENU' with various system administration links. The main configuration area includes:

- Remote Syslog:** disable enable
- Message Format:** rfc3164 rfc5424
- Periodic Report (minutes):** 0
- Table of Remote Syslog Servers:**

Dest_IP	Port	Interface
<input type="text"/>	514	lan1 v
<input type="text"/>	514	lan1 v
<input type="text"/>	514	lan1 v
<input type="text"/>	514	lan1 v

Buttons for 'Submit' and 'Cancel' are located at the bottom of the configuration area.

Remote Syslog Screen

The FT device can be configured to send log messages to up to four remote syslog servers. Log messages include the messages found in the *Tunnel Log* and also messages regarding configuration changes.

Fields

- **Remote Syslog**
Enable/Disable sending log messages to a remote syslog server.
- **Message Format**
There are two common formats for syslog messages, RFC3164 and RFC5424. If you are unsure which format to use, one of the distinguishing features is the format of the timestamp. For example, RFC3164 would format the time as "Feb 1 13:55:25" where RFC5424 would format the same time as "2015-02-01T13:55:25"
- **Destination IP**
The IPv4 or IPv6 address of the syslog server. Host names are not allowed.
- **Destination Port**
The UDP port number of the remote syslog server. UDP port 514 is the port reserved for rsyslog.
- **Interface**
The interface to use when sending log messages to the server. Messages can be sent over an untrusted interface, though this is not recommended.

Set All Defaults



The screenshot shows a web interface for a device labeled FT-6615. At the top left is a logo with a red grid pattern and the letters 'DCB'. To the right of the logo, the device name 'FT-6615' is displayed in a large font, with the timestamp '03-20-2025 16:26:19' below it. The main content area is divided into two sections. On the left is a 'MENU' with several blue underlined links: Administration, Admin Password, Access Control, Web Server Firewall, New Web Certificate, Set Clock, Set Name, Remote Syslog, and Set All Defaults. The 'Set All Defaults' link is highlighted. On the right is the 'Set All Defaults' section, which contains the text: 'Press this button to set ALL parameters to default values. Note: this will also clear all keys.' Below this text is a button labeled 'Default All'.

Set All Defaults Screen

This form will allow you to reset all configuration parameters to their default value. Before you "Activate Changes", you should configure the LAN interface that you are using to access the tunnel or set it to the new target IP address. Set All Defaults will also reset all the certificates stored within the unit.

Configuration File

FT-6615
03-20-2025 16:33:12

Configuration File

Transfer the config file from the device to your computer.
The config file will be encrypted with the given password.

Set Password:

Confirm Password:

Transfer a config file from your computer to the device.
The config file will be decrypted using the given password.

File to Transfer: No file selected.

Password:

Configuration File Screen

This form will allow you to copy the FT-66xx's configuration to a file on your PC. You can also use the form to transfer a configuration file from your PC to the FT-66xx. 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). You also have the option of modifying the configuration. 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

DCB **FT-6615**
03-20-2025 16:41:27

MENU
[Administration](#)
[Admin Password](#)
[Access Control](#)
[Web Server Firewall](#)
[New Web Certificate](#)
[Set Clock](#)
[Set Name](#)
[Remote Syslog](#)
[Set All Defaults](#)
[Config File](#)
[Firmware Upgrade](#)
[System Backup](#)

Firmware Upgrade

File for Upgrade: No file selected.

The upgrade file is large and may take several minutes to upload.

Firmware Upgrade Screen

This form will allow you to load new firmware into the FT-66xx. The firmware will be saved to non-volatile memory, replacing the current firmware. Firmware upgrade will retain the current configuration. It can also be performed remotely, through a tunnel connection.

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. Firmware images contain a digital signature and are self-authenticated prior to installing onto the device. The upgrade process will throw an “Invalid File” error if the file is corrupt or is not compatible with the hardware.

System Reboot

The screenshot shows a web interface for a device labeled FT-6615. At the top left is the DCB logo. The main header displays 'FT-6615' and the date/time '03-20-2025 16:47:55'. On the left, a 'MENU' section lists various administrative options: Administration, Admin Password, Access Control, Web Server Firewall, New Web Certificate, Set Clock, Set Name, Remote Syslog, Set All Defaults, Config File, Firmware Upgrade, System Reboot, and Version Info. The 'System Reboot' section in the center contains the instruction 'Press this button to confirm system reboot.' and a button labeled 'Reboot_System'.

System Reboot Screen

This form will allow you to reboot the FT-66xx. 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

FT-6615
03-20-2025 16:56:43

MENU

- [Administration](#)
- [Admin Password](#)
- [Access Control](#)
- [Web Server Firewall](#)
- [New Web Certificate](#)
- [Set Clock](#)
- [Set Name](#)
- [Remote Syslog](#)
- [Set All Defaults](#)
- [Config File](#)
- [Firmware Upgrade](#)
- [System Reboot](#)
- [Version Info](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)

Firmware Version

FT-6615 Version: v4_03
Linux Version: 4.4.302
Release Date: 03-18-2025

- The FT-6615 uses an embedded FIPS 140-2 validated cryptographic module (Certificate #4282) running on a [Linux](#) platform per FIPS 140-2 Implementation Guidance section G.5.
- Portions of this software are Copyright © 2003-2025 Data Comm for Business Inc.
- Portions of this software are Copyright © 1988, 1993 The Regents of the University of California. All rights reserved
- Portions of this software are Copyright under the terms of the GNU General Public License.
- Portions of this software are Copyright under the terms of the Apache License v2.
- Press [here](#) for additional Copyright and License information.

Version Information Screen

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

LAN 1 Ethernet Mode

The screenshot shows the configuration interface for the LAN 1 Ethernet Mode on an FT-6615 device. The top header includes the DCB logo and the device model name 'FT-6615' with a timestamp '03-20-2025 17:06:55'. A left-hand menu lists various configuration options: Administration, LAN1 (private), Mode, IP Configuration, IPv6 Configuration, DHCP Server, and LAN2 (internet). The main content area is titled 'LAN1 Mode' and features a radio button for 'Lan1' with 'disable' and 'enable' options, and a dropdown menu for 'Speed/Duplex' set to 'auto'. There are 'Submit' and 'Cancel' buttons at the bottom.

LAN 1 Ethernet Mode Screen

Depending on the FT hardware model, the device will have 2 to 4 LAN interfaces. LAN1 is always the trusted (or private) interface.

LAN1 may be disabled or enabled. Please note that even when LAN1 is disabled, it is still enabled for bridging packets. Disabling the interface only disables the interface at the layer-3 IP level. The device will no longer respond to any IP address configured on the interface.

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:

- 1000MB operation requires auto-negotiation.

LAN 2/3/4 Ethernet Mode

The screenshot shows the configuration interface for the FT-6615 device. At the top, there is a DCB logo and the device name 'FT-6615' with a timestamp '03-20-2025 18:05:09'. On the left, a 'MENU' sidebar lists various configuration options. The main content area is titled 'LAN2 Mode' and includes the following settings:

- Lan2:** disable enable
- Speed/Duplex:** auto (dropdown menu)
- Mode:** IP PPPoE
- Bridge to Private:** no yes

Buttons for 'Submit' and 'Cancel' are located at the bottom of the configuration area.

LAN 2/3/4 Ethernet Mode Screen

The FT-6606 and FT-6615 have an additional feature where unused LAN2, LAN3, or LAN4 ports can be disabled as a layer-3 interface, and then bridged to the LAN1 private network. The port then functions like a switch port in the same broadcast domain as LAN1. This can eliminate the need for an external Ethernet switch, when you only need to connect two or three devices to the private network.

Fields

- **LAN 2/3/4**
Enable or disable the LAN port. The default is enabled.
- **Speed/Duplex**
Select 100 MB or 10 MB and half or full duplex, AUTO. The default is AUTO. 1000 MB requires the port to be set for AUTO.
- **Mode**
Select IP mode or PPPoE mode.
- **Bridge to Private**
When the port is disabled, the port may be configured as a switch port to the LAN1 private network.

Notes:

To bridge the port to the trusted interface, it must be disabled. While this seems counter intuitive, the reason is to disable the port as a layer-3 interface.

LAN1 IP Configuration

The screenshot displays the LAN1 IP Configuration screen for device FT-6615. On the left is a navigation menu with links for Administration, LAN1 (private), Mode, IP Configuration, IPv6 Configuration, DHCP Server, LAN2 (internet), LAN3 (internet), LAN4 (internet), Tunnel, Tools, Status, Activate Changes, and Store Configuration. The main area is titled 'LAN1 IP Configuration' and shows two radio button options: 'automatic-via-DHCP' (unselected) and 'Static-Configuration' (selected). Under 'Static-Configuration', there are input fields for IP Address (192.168.0.1), Subnet Mask (255.255.255.0), Gateway, VLAN ID, Primary DNS Server, and Alternate DNS Server. At the bottom are 'Submit' and 'Cancel' buttons.

LAN1 IP Configuration Screen

LAN 1 is always the local, secure side of the tunnel.

Fields

- **Configure IP**
The interface can be configured automatically using DHCP or statically. If you choose to use DHCP, 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 host names.

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 LAN1 if it is configured for an 802.1Q VLAN.

LAN2/3/4 IP Configuration

FT-6615
03-20-2025 18:15:52

MENU
[Administration](#)
[LAN1 \(private\)](#)
[LAN2 \(internet\)](#)
[Mode](#)
[IP Configuration](#)
[IPv6 Configuration](#)
[Alias Configuration](#)
[DHCP Server](#)
[LAN3 \(internet\)](#)
[LAN4 \(internet\)](#)
[Tunnel](#)
[Tools](#)
[Status](#)
[Activate Changes](#)
[Store Configuration](#)

LAN2 IP Configuration

Configure IP automatic-via-DHCP Static-Configuration

Static-Configuration

IP Address 192.168.2.114

Subnet Mask 255.255.255.0

Gateway

Max Transmit Unit

Primary DNS Server

Alternate DNS Server

LAN2/3/4 IP Configuration Screen

FT units will have 2 to 4 LAN interfaces, depending on the hardware model. LAN2 and above all have the same configuration options.

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 DHCP, 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.

- **Max Transmission Unit**
The default MTU for an Ethernet interface is 1500 bytes, not including the Ethernet header. In some

applications it may be necessary to reduce the MTU of an untrusted interface to prevent IP fragmentation through a layer-3 routed network. This field may be used to modify the MTU of the interface. This is commonly needed when tunneling through another tunnel, such as through an IPSec tunnel.

- **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 host names.

Notes:

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

The DHCP Client may not be used on LAN1 if it is configured for an 802.1Q VLAN.

LAN1/2/3/4 IPv6 Configuration

FT-6615
03-20-2025 18:33:30

MENU
[Administration](#)
[LAN1 \(private\)](#)
[Mode](#)
[IP Configuration](#)
[IPv6 Configuration](#)
[DHCP Server](#)
[LAN2 \(internet\)](#)
[LAN3 \(internet\)](#)
[LAN4 \(internet\)](#)
[Tunnel](#)
[Tools](#)
[Status](#)
[Activate Changes](#)
[Store Configuration](#)

LAN1 IPv6 Configuration

IPv6 Enable disable enable

Configure IP Stateless-Autoconfigure
 Static-Configuration

Static-Configuration

IPv6 Address fc00:0:0:1::a001

Subnet Prefix Length 64

Gateway

DNS-Configuration

Primary IPv6 DNS Server

Alternate IPv6 DNS Server

Submit Cancel

LAN1/2/3/4 IPv6 Configuration Screen

FT units will have 1 to 4 LAN interfaces, depending on the hardware model. All LAN interfaces have the same set of IPv6 configuration options.

Fields

- **IPv6 Enable**
Enable/Disable IPv6 mode on the interface. Enabling IPv6 does not disable IPv4. The interface will operate with both IPv4 and IPv6 simultaneously.
- **Configure IP**
The interface can be configured statically or may use IPv6 stateless auto-configuration. IPv6 stateless auto-configuration requires an IPv6 router to be present on the network segment and that it is sending router advertisements.
- **IPv6 Address**
This field sets a static IPv6 address for the given interface. The field is ignored when IPv6 stateless auto-configuration is enabled. Please note that in addition to the static or auto-configured IPv6 address, the interface will also self-assign an IPv6 link-local address from the link-local pool fe80::/64.
- **Subnet Prefix Length**
The subnet prefix length specifies the number of bits in the subnet portion of the IP address. It is similar in concept to the IPv4 subnet mask. In practice, most IPv6 subnets will have a subnet prefix length of 64. This field is ignored when IPv6 stateless autoconfiguration is enabled.
- **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.

- **Primary IPv6 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 IPv6 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 host names.

Notes:

DHCP Server Configuration

The screenshot shows the DHCP Server Configuration screen for the FT-6615 device. The top header displays the device name 'FT-6615' and the timestamp '03-20-2025 18:46:58'. On the left, there is a 'MENU' section with links for Administration, LAN1 (private), Mode, IP Configuration, IPv6 Configuration, DHCP Server, LAN2 (internet), and LAN3 (internet). The main configuration area is titled 'LAN1 DHCP Server' and includes the following fields: 'DHCP Server' with radio buttons for 'disable' (selected) and 'enable'; 'IP Range Low' with a text input containing '192.168.0.101'; 'IP Range High' with a text input containing '192.168.0.109'; and 'Assigned Gateway' with an empty text input. At the bottom of the configuration area are 'Submit' and 'Cancel' buttons.

DHCP Server Configuration Screen

The FT device may also provide DHCP services on any of its Ethernet interfaces. Each interface will have a unique DHCP Server Configuration.

In the default configuration, the LAN1 DHCP server is enabled. This was done for convenience of initial setup. Please make sure there is only one DHCP server present on a network segment. In most cases, should not be providing DHCP service.

Fields

- **DHCP Server**
Enable/Disable a DHCP Server on the interface. Addresses will be dynamically assigned from the following pool in response to DHCP Client requests.
- **IP 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

DCB **FT-6615**
03-21-2025 15:03:39

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [Mode](#)
- [PPPoE Configuration](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Status](#)
- [Activate Changes](#)
- [Store Configuration](#)

LAN3 PPPoE Configuration

User Name

Password

Service Name

Access Concentrator

Frame Type

Local IP

Remote IP

Default Gateway no yes

Idle Disconnect Time

Max Connect Time

DNS Addresses none request

Max Transmit Unit

Echo Test Link disable enable

Logging basic detailed

Ethernet PPPoE Configuration Screen

The untrusted 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 hexadecimal 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).

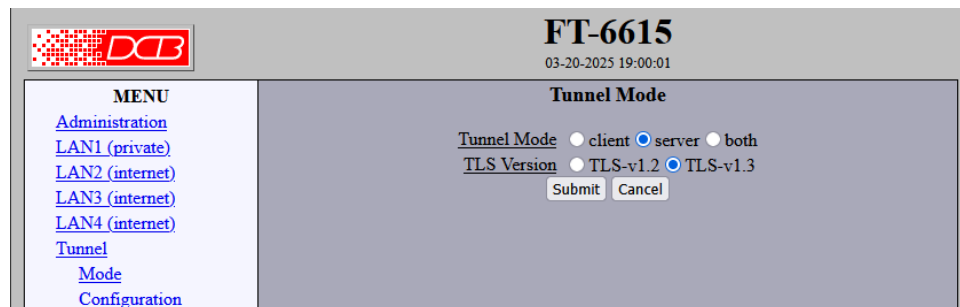
This feature is typically used when your ISP charges for service based on connect time.

- **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



The screenshot shows the configuration interface for the FT-6615 device. At the top left is the DCB logo. The title 'FT-6615' and the timestamp '03-20-2025 19:00:01' are at the top right. A 'MENU' sidebar on the left lists various system settings. The main 'Tunnel Mode' section contains two rows of radio button options: 'Tunnel Mode' with 'client', 'server' (selected), and 'both'; and 'TLS Version' with 'TLS-v1.2' and 'TLS-v1.3' (selected). 'Submit' and 'Cancel' buttons are located below the options.

Tunnel Mode Screen

The FT-66xx may be configured as either a server, client, or both. FT-66xx 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.

TLS Version

Select the minimum TLS version to use as the transport between the client and server. The choices are v1.2 or v1.3. All units in the system must support the same protocol. Older versions of FT firmware, that do not have this options, are operating in TLS v1.0 mode. The v4.x firmware is unable to interoperate with a FT device running in TLS v1.0 mode.

Note: With the v4.x firmware the TLS Version selects the minimum allowed version. If both units are set for v1.2, but both are capable of v1.3, they will choose to communicate with v1.3.

Encrypted Tunnel Configuration

FT-6615
03-20-2025 19:41:07

MENU
[Administration](#)
[LAN1 \(private\)](#)
[LAN2 \(internet\)](#)
[LAN3 \(internet\)](#)
[LAN4 \(internet\)](#)
[Tunnel](#)
[Mode](#)
[Configuration](#)

Tunnel Configuration

Listen to Port
(secondary) Listen to Port
Submit Cancel

Tunnel Configuration Screen (server mode)

FT-6615
03-20-2025 19:43:13

MENU
[Administration](#)
[LAN1 \(private\)](#)
[LAN2 \(internet\)](#)
[LAN3 \(internet\)](#)
[LAN4 \(internet\)](#)
[Tunnel](#)
[Mode](#)
[Configuration](#)
[Generate CA Key](#)
[Generate Local Key](#)

Tunnel Configuration

Connect to Server
Port
via Interface

On Failure (optional)

Connect to Server
Port
via Interface
Submit Cancel

Tunnel Configuration Screen (client mode)

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. Both IPv4 and IPv6 addresses are supported.

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.

Notes

Generate Certificate Authority Key

DCB FT-6615
03-20-2025 19:47:39
Generate CA Key
MENU
[Administration](#)
[LAN1 \(private\)](#)
[LAN2 \(internet\)](#)
[LAN3 \(internet\)](#)
[LAN4 \(internet\)](#)
[Tunnel](#)
[Mode](#)
[Configuration](#)
[Generate CA Key](#)
[Generate Local Key](#)
[Advanced](#)
[Ethernet Filters](#)
[IP Filters](#)
[UDP Filters](#)
[TCP Filters](#)
[Server Firewall](#)
Tools
[Status](#)
[Activate Changes](#)
[Store Configuration](#)
Name A Unique CA Name
Organization My Company
Organizational Unit My Department
Country Code US
State/Province My State
Locality My Town
[Set CA Password](#)
[Confirm CA Password](#)
Submit Cancel
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.
Note: CA generation can take up to 90 seconds to complete

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-66xx). 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 alphanumeric characters.
- **Organization**
The organizational name given to the certificate. It may be 1 to 64 characters in length, limit to alphanumeric 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 alphanumeric characters.

- Country Code
The country code given to the certificate. It is 2 characters in length, limit to alphanumeric characters.
- State/Province
The State or Province name given to the certificate. It may be 1 to 64 characters in length, limit to alphanumeric 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 alphanumeric 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

- Be sure to set the clock to the correct time prior to generating the Certificate Authority. Clock discrepancies are the primary cause of errors when generating keys. These errors are not apparent until the client devices attempt to connect to the server.
- 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

The screenshot shows the 'Generate Local Key' page on the FT-6615 device. The page has a header with the DCB logo and the device name 'FT-6615' along with the date and time '03-20-2025 19:49:40'. On the left is a 'MENU' with links for Administration, LAN1 (private), LAN2 (internet), LAN3 (internet), LAN4 (internet), Tunnel, Mode, Configuration, Generate CA Key, Generate Local Key, Advanced, Ethernet Filters, and ID Filters. The main content area is titled 'Generate Local Key' and contains three input fields: 'Name' (FT-6615), 'Certificate Lifetime (days)' (3560), and 'CA Password'. There are 'Submit' and 'Cancel' buttons. Below the form, there is a warning: 'Before submitting this page, please install the USB flash drive containing your CA key. Your CA key is password protected, so be sure to enter above the same password you used when you generated the CA key.' A note at the bottom states: 'Note: Key generation can take up to 90 seconds to complete.'

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-66xx). 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

- Be sure to set the clock to the correct time prior to generating the Local Key. Clock discrepancies are the primary cause of errors when generating keys. These errors are not apparent until the client devices attempt to connect to the server.

Advanced Tunnel Configuration

FT-6615
03-20-2025 20:04:38

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
 - [Mode](#)
 - [Configuration](#)
 - [Generate CA Key](#)
 - [Generate Local Key](#)
 - [Advanced](#)
 - [Ethernet Filters](#)
 - [IP Filters](#)
 - [UDP Filters](#)
 - [TCP Filters](#)

Advanced Tunnel Configuration

Idle Disconnect Time

Send Keep-Alives

TCP No-Delay disable enable

Block Multicast no yes snoop

Snoop Purge Count

Multicast Query Interval

IGMP Query Version v2 v3

Duplicate Users no yes

Filter All Connections no yes

Relay Remote-to-Remote no yes

Allow not yet valid certs no yes

Allow expired certs no yes

UDP Transport disable enable

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.

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.

Snoop Purge Count

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

IGMP Query Version

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

Multicast Query Interval

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

When the tunnel is performing IGMP snooping, it is reading IGMP reports to determine where multicast

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

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

Duplicate Users

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

Filter All Connections

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

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

Relay Remote-to-Remote

When set to *yes*, the local tunnel will relay packets between remote tunnels. When set to *no* the local tunnel will only bridge packets to/from the local LAN.

Allow not yet valid certificates

When set to *yes*, the local tunnel will accept a peer certificate and/or CA certificate that is not yet valid. In other words, the start date for the certificate is in the future relative to the local tunnel's clock.

This feature is intended to mitigate connection failures in the event that the local real-time clock battery has failed causing the local clock to revert to an earlier date.

Allow expired certificates

When set to *yes*, the local tunnel will accept a peer certificate and/or CA certificate that has expired.

UDP Transport

The FT products initially connect and authenticate using a TCP connection. After authentication, the devices can continue to use the TCP connection for communication or can optionally switch to a UDP transport. The UDP transport is often preferred, especially when the primary application is streaming audio or video and the retry mechanism of TCP can cause unwanted delays and re-transmissions.

In order to enable the UDP Transport, it must be enabled in both the server and client. Otherwise the transport will continue to operate using TCP.

Notes

Ethernet (MAC) Address Filters Screen

FT-6615
03-20-2025 20:13:12

Ethernet Filters

Default Rule: filters-disabled

Except for packets with

	Destination Address	Source Address	Protocol
1:			
2:			
3:			
4:			
5:			
6:			
7:			
8:			

Submit Cancel

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

The screenshot shows the 'IP Filters' configuration page for device FT-6615. At the top right, the device name 'FT-6615' and the timestamp '03-20-2025 20:14:41' are displayed. On the left is a 'MENU' with various navigation links. The main content area is titled 'IP Filters' and contains a 'Default Rule' dropdown menu currently set to 'filters-disabled', and a 'Non-IP Packets' dropdown menu set to 'allow'. Below these is the instruction 'Except for IP packets with' followed by a table with four columns: 'Destination IP', 'Destination Mask', 'Source IP', and 'Source Mask'. The table has eight rows, numbered 1 through 8. At the bottom right of the table area are 'Submit' and 'Cancel' buttons.

Address Filters Screen

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

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

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

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

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

Fields

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

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

The screenshot shows the 'UDP Filters' configuration page for device FT-6615. On the left is a 'MENU' with links to various system functions. The main content area has a 'Default Rule' dropdown menu currently set to 'filters-disabled'. Below this, there is a section for exceptions: 'Except for packets with'. This section contains a table with two columns: 'Low Destination Port (inclusive range)' and 'High Destination Port'. There are eight rows of input fields for these ports, numbered 1 through 8. At the bottom right of the main area are 'Submit' and 'Cancel' buttons.

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.

Server Firewall

DCB FT-6615
03-20-2025 20:20:02

Tunnel Server Firewall

Server Firewall disable enable
Policy accept-all drop-all

	Source IP	Action
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Page: 1 2 3 4 5
Submit Cancel

Server Firewall Screen

The Tunnel Server Firewall Rules Table may be used to block nuisance connection attempts to the Tunnel's TCP port. It is only active when the tunnel is configured for server mode. The rules in the table are applied when a client device attempts to connect to the server. If the client's IP address matches a rule, the specified action is taken. If none of the rules match, the connection will be accepted.

The rules in the table are applied in sequential order. With this, it is possible to build either an allowlist, a denylist, or a combination of the two. For example, to build an allowlist, you would enter the IP address of each client device with an ACCEPT action". The policy would be set to drop-all.

Fields

Server Firewall

Enable/Disable the tunnel server firewall. This is a quick way to enable/disable all of the rules.

Policy

The policy selects the default action to take when there is no matching rule. The options are to either accept-all or to drop-all connection attempts.

Source IP

The source IP may be specified as a single address or specified as an address/netmask or address/bits subnet. Both IPv4 and IPv6 addresses are allowed.

Action

Action to take when a connection attempt matches the rule. The action can be **ACCEPT** or **DROP**. If no action is specified, the rule is ignored.

Notes


Examples of Source IP address rules:

192.168.10.50	- Single address
192.168.10.0/255.255.255.0	- Class C subnet 192.168.10.0
192.168.0.0/16	- Class B subnet 192.168.0.0
0.0.0.0/0	- All addresses
2001:db8:78:1::50	- Single IPv6 address

2001:db8:78:1::/64
::/0

- IPv6 subnet
- All IPv6 addresses

Ping Screen



FT-6615

03-21-2025 12:42:27

MENU

[Administration](#)

[LAN1 \(private\)](#)

[LAN2 \(internet\)](#)

[LAN3 \(internet\)](#)

[LAN4 \(internet\)](#)

[Tunnel](#)

Tools

[Ping](#)

[Traceroute](#)

[Packet Sniffer](#)

[NTP](#)

[Status](#)

[Activate Changes](#)

[Store Configuration](#)

Ping

Host

Interface

Size (64-1450)

```

PING 192.168.0.20 (192.168.0.20): 64 data bytes
72 bytes from 192.168.0.20: seq=0 ttl=64 time=0.523 ms
72 bytes from 192.168.0.20: seq=1 ttl=64 time=1.195 ms
72 bytes from 192.168.0.20: seq=2 ttl=64 time=1.136 ms
72 bytes from 192.168.0.20: seq=3 ttl=64 time=0.450 ms

--- 192.168.0.20 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.450/0.826/1.195 ms
          
```

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. Both IPv4 and IPv6 addresses are supported.
- Size
Number of data bytes to send.

Notes

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

Traceroute Screen

The screenshot shows the FT-6615 Traceroute screen. On the left is a menu with options: Administration, LAN1 (private), LAN2 (internet), LAN3 (internet), LAN4 (internet), Tunnel, Tools, Ping, Traceroute, Packet Sniffer, NTP, Status, Activate Changes, and Store Configuration. The main area is titled 'Traceroute' and contains a form with 'Host' set to '8.8.8.8' and 'Interface' set to 'lan1'. A 'Traceroute' button is visible. Below the form, the traceroute results are displayed as a table:

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1 192.168.1.254  0.364 ms  0.241 ms  0.165 ms
 2 206.109.185.129  8.172 ms  10.090 ms  12.019 ms
 3 192.34.31.190  7.237 ms  7.279 ms  7.784 ms
 4 10.214.0.12  9.517 ms  12.809 ms  17.526 ms
 5 10.214.0.30  14.401 ms  12.068 ms  10.179 ms
 6 10.209.0.4  11.980 ms  12.600 ms  9.675 ms
 7 199.26.57.45  12.671 ms  14.619 ms  12.424 ms
 8 142.250.168.68  12.253 ms  *  14.573 ms
 9 * * *
10 8.8.8.8  14.584 ms  12.526 ms  12.329 ms
```

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.

Notes

Packet Sniffer Screen

DCB **FT-6615**
03-21-2025 13:10:57

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Ping](#)
- [Traceroute](#)
- [Packet Sniffer](#)
- [NTP](#)
- [Status](#)
- [Activate Changes](#)
- [Store Configuration](#)

Packet Sniffer

Interface: lan1
Host(optional): 192.168.1.20
Port(optional):
Run

The sniffer will run for 30 seconds or 100 packets.

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lan1, link-type EN10MB (Ethernet), capture size 262144 bytes
13:11:00.185654 IP 192.168.1.20 > 239.255.255.250: igmp
13:11:02.456555 IP 192.168.1.20 > 192.168.1.1: ICMP echo request, id 5, seq 1, length 64
13:11:02.456637 IP 192.168.1.1 > 192.168.1.20: ICMP echo reply, id 5, seq 1, length 64
13:11:03.513880 IP 192.168.1.20 > 192.168.1.1: ICMP echo request, id 5, seq 2, length 64
13:11:03.513969 IP 192.168.1.1 > 192.168.1.20: ICMP echo reply, id 5, seq 2, length 64
```

5 packets captured
5 packets received by filter
0 packets dropped by kernel

Packet sniffer time-limit exceeded. Operation aborted.

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

DCB

FT-6615
03-21-2025 13:15:50

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Status](#)
- [Interface](#)
- [Tunnel Log](#)
- [Tunnel Nodes](#)
- [Tunnel Addr](#)
- [Routing Table](#)
- [DHCP Status](#)
- [PPPoE Log](#)
- [Audit Ports](#)
- [IPv4 Firewall](#)
- [IPv6 Firewall](#)
- [FIPS Module](#)
- [Activate Changes](#)
- [Store Configuration](#)

Interface Status

lan1

```
lan1  Link encap:Ethernet HWaddr 00:E0:67:2C:72:4C
      inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:1116 errors:0 dropped:0 overruns:0 frame:0
      TX packets:495 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:223928 (218.6 KiB) TX bytes:163915 (160.0 KiB)
```

lan1p

```
lan1p  RX packets:1144 errors:0 dropped:27 overruns:0 frame:0
      TX packets:546 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:244337 (238.6 KiB) TX bytes:170978 (166.9 KiB)
```

lan1t

```
lan1t  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:629 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:79698 (77.8 KiB)
```

lan2

```
lan2  Link encap:Ethernet HWaddr 00:E0:67:2C:72:4D
      inet addr:192.168.2.114 Bcast:192.168.2.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:661 errors:0 dropped:0 overruns:0 frame:0
      TX packets:659 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:47059 (45.9 KiB) TX bytes:144193 (140.8 KiB)
```

lan3

```
lan3  Link encap:Ethernet HWaddr 00:E0:67:2C:72:4E
      inet addr:192.168.3.1 Bcast:192.168.3.255 Mask:255.255.255.0
      UP BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

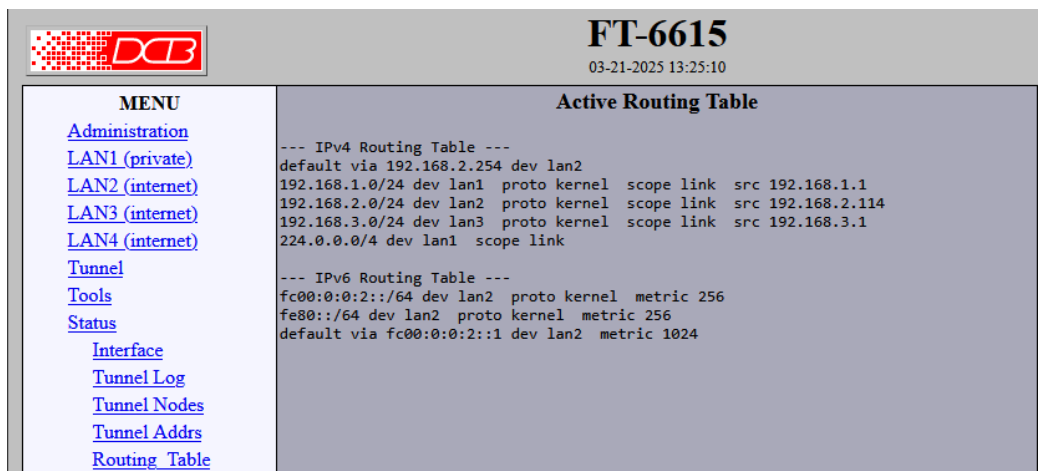
lan4

Interface 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.

Note: The LAN1 interface is a composite interface consisting of physical *lan1p* port and the virtual tunnel *lan1t* port.

Routing Table Screen



FT-6615
03-21-2025 13:25:10

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Status](#)
- [Interface](#)
- [Tunnel Log](#)
- [Tunnel Nodes](#)
- [Tunnel Addr](#)
- [Routing Table](#)

Active Routing Table

```
--- IPv4 Routing Table ---
default via 192.168.2.254 dev lan2
192.168.1.0/24 dev lan1 proto kernel scope link src 192.168.1.1
192.168.2.0/24 dev lan2 proto kernel scope link src 192.168.2.114
192.168.3.0/24 dev lan3 proto kernel scope link src 192.168.3.1
224.0.0.0/4 dev lan1 scope link

--- IPv6 Routing Table ---
fc00:0:0:2::/64 dev lan2 proto kernel metric 256
fe80::/64 dev lan2 proto kernel metric 256
default via fc00:0:0:2::1 dev lan2 metric 1024
```

Routing Table Screen

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

Store Configuration Screen

The screenshot shows the Store Configuration screen for device FT-6615. At the top left is the DCB logo. The top right displays the device name 'FT-6615' and the timestamp '03-21-2025 13:27:44'. On the left is a 'MENU' section with links: Administration, LAN1 (private), LAN2 (internet), LAN3 (internet), LAN4 (internet), Tunnel, Tools, Status, Activate Changes, and Store Configuration. The main area is titled 'Store Configuration' and contains the text: 'Press this button to store the current configuration to Nonvolatile Memory:' followed by a 'Store Config' button. Below the button are two bullet points: 'The Store Config process takes about 10 seconds to complete.' and 'Do not power cycle the system until your web page refreshes.'

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 preexisting 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

The screenshot shows the Activate Configuration screen for device FT-6615. At the top left is the DCB logo. The top right displays the device name 'FT-6615' and the timestamp '03-21-2025 13:29:20'. On the left is a 'MENU' section with links: Administration, LAN1 (private), LAN2 (internet), LAN3 (internet), LAN4 (internet), Tunnel, Tools, Status, Activate Changes, and Store Configuration. The main area is titled 'Activate Changes' and displays 'Changes Activated.' in red text. Below this is a message: 'The current configuration has not been stored to nonvolatile memory.'

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 preexisting 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

Location	Rx Count	Tx Count	Tx Dropped	UserName	State
lan1t	1617	0	0	none	up
192.168.2.115:35310	51	1607	0	FT-6615-Client	up

Tunnel Nodes Screen

The Tunnel Nodes Screen displays currently connected remote nodes. These nodes are other FT-66xx units that have authenticated with this unit.

Tunnel Addresses Screen

FT-6615
03-21-2025 13:40:49

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Status](#)
- [Interface](#)
- [Tunnel Log](#)
- [Tunnel Nodes](#)
- [Tunnel Addr](#)

Tunnel Addr

Ethernet Address	Location	Hit Count	Last Time
04-a3-16-ed-b0-0b	lan1t	24674	13:40:29
68-05-ca-3c-c2-29	lan1t	83	13:40:33
4c-5e-0c-c4-3a-46	lan1t	77	13:40:31
00-e0-67-2c-72-4c	lan1t	4	13:23:17
68-05-ca-3c-f0-5c	lan1t	294	13:40:32
78-9a-18-b6-db-95	lan1t	1310	13:40:48
38-d2-69-42-46-e0	192.168.2.115:35310	24667	13:40:29

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

FT-6615-Client
03-21-2025 13:53:56

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Status](#)
- [Interface](#)
- [Tunnel Log](#)
- [Tunnel Nodes](#)
- [Tunnel Addr](#)
- [Routing Table](#)
- [DHCP Status](#)
- [PPPoE Log](#)

DHCP Status

LAN1 - DHCP Not Enabled

LAN2 - DHCP Client

last event - bound lan2 - Fri Mar 21 13:49:13 UTC 2025
ip: 192.168.2.101
subnet: 255.255.255.0
router: 192.168.2.254
lease: 86400 seconds
serverid: 192.168.2.114

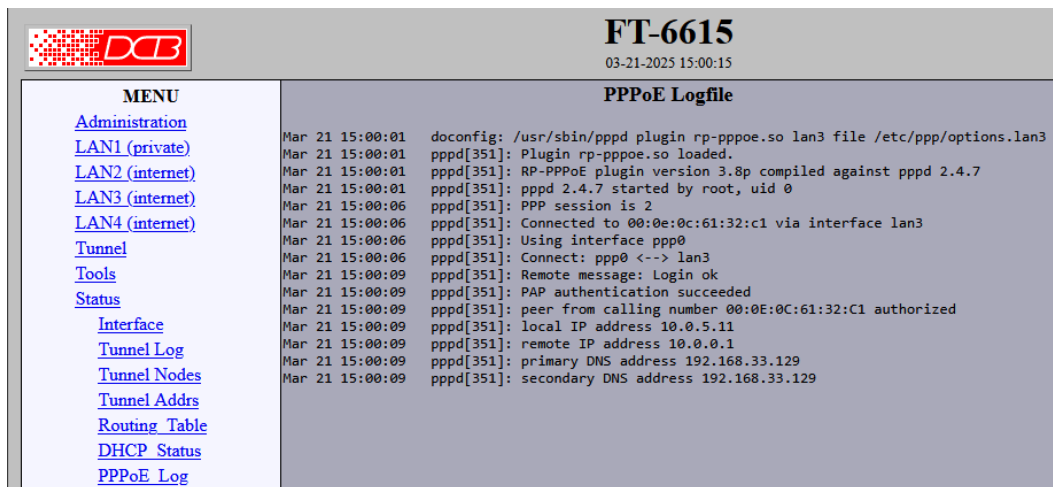
LAN3 - DHCP Not Enabled

LAN4 - DHCP Not Enabled

DHCP Status Screen

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

PPPoE Log



DCB **FT-6615**
03-21-2025 15:00:15

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Status](#)
- [Interface](#)
- [Tunnel Log](#)
- [Tunnel Nodes](#)
- [Tunnel Addr](#)
- [Routing Table](#)
- [DHCP Status](#)
- [PPPoE Log](#)


PPPoE Logfile

```
Mar 21 15:00:01 doconfig: /usr/sbin/pppd plugin rp-pppoe.so lan3 file /etc/ppp/options.lan3
Mar 21 15:00:01 pppd[351]: Plugin rp-pppoe.so loaded.
Mar 21 15:00:01 pppd[351]: RP-PPPoE plugin version 3.8p compiled against pppd 2.4.7
Mar 21 15:00:01 pppd[351]: pppd 2.4.7 started by root, uid 0
Mar 21 15:00:06 pppd[351]: PPP session is 2
Mar 21 15:00:06 pppd[351]: Connected to 00:0e:0c:61:32:c1 via interface lan3
Mar 21 15:00:06 pppd[351]: Using interface ppp0
Mar 21 15:00:06 pppd[351]: Connect: ppp0 <-> lan3
Mar 21 15:00:09 pppd[351]: Remote message: Login ok
Mar 21 15:00:09 pppd[351]: PAP authentication succeeded
Mar 21 15:00:09 pppd[351]: peer from calling number 00:0E:0C:61:32:C1 authorized
Mar 21 15:00:09 pppd[351]: local IP address 10.0.5.11
Mar 21 15:00:09 pppd[351]: remote IP address 10.0.0.1
Mar 21 15:00:09 pppd[351]: primary DNS address 192.168.33.129
Mar 21 15:00:09 pppd[351]: secondary DNS address 192.168.33.129
```

PPPoE Log Screen

The PPPoE Log screen displays recent PPPoE activity.

Audit Ports



FT-6615
03-21-2025 14:13:05

MENU

- [Administration](#)
- [LAN1 \(private\)](#)
- [LAN2 \(internet\)](#)
- [LAN3 \(internet\)](#)
- [LAN4 \(internet\)](#)
- [Tunnel](#)
- [Tools](#)
- [Status](#)
- [Interface](#)
- [Tunnel Log](#)
- [Tunnel Nodes](#)
- [Tunnel Addr](#)
- [Routing Table](#)
- [DHCP Status](#)
- [PPPoE Log](#)
- [Audit Ports](#)

Active TCP/UDP Ports

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	:::22	:::*	LISTEN
tcp	0	0	:::443	:::*	LISTEN
udp	0	0	0.0.0.0:67	0.0.0.0:*	
udp	0	0	:::22	:::*	


Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	4261	::ffff:192.168.1.1:443	::ffff:192.168.1.21:53085	ESTABLISHED
tcp	0	0	::ffff:192.168.2.114:22	::ffff:192.168.2.101:44206	ESTABLISHED

Audit Ports Screen

This screen shows the active TCP and UDP ports, for the purpose of auditing the system. Note, since the system is (IPv4/IPv6) dual-stack, results are shown using IPv6 nomenclature.

IPv4 Firewall



FT-6615


03-21-2025 14:11:10

MENU	System IPv4 Firewall Table																																																																																																																																																																																																																																																						
<ul style="list-style-type: none"> Administration LAN1 (private) LAN2 (internet) LAN3 (internet) LAN4 (internet) Tunnel Tools Status Interface Tunnel Log Tunnel Nodes Tunnel Addr Routing Table DHCP Status PPPoE Log Audit Ports IPv4 Firewall IPv6 Firewall FIPS Module Activate Changes Store Configuration 	<div style="margin-bottom: 10px;"> <p>Chain INPUT (policy DROP 46 packets, 8970 bytes)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>all</td> <td>-f</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>10</td> <td>840</td> <td>pingif</td> <td>icmp</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>icmp type 8</td> </tr> <tr> <td>74458</td> <td>43M</td> <td>ACCEPT</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>state RELATED,EST</td> </tr> <tr> <td>504</td> <td>43774</td> <td>tunnel</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>502</td> <td>43654</td> <td>manage</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmp</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>icmp type 255</td> </tr> <tr> <td>138</td> <td>4416</td> <td>ACCEPT</td> <td>2</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>2</td> <td>656</td> <td>ACCEPT</td> <td>udp</td> <td>--</td> <td>lan2</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>udp dpts:67:68</td> </tr> </tbody> </table> </div> <div style="margin-bottom: 10px;"> <p>Chain FORWARD (policy DROP 0 packets, 0 bytes)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> </div> <div style="margin-bottom: 10px;"> <p>Chain OUTPUT (policy ACCEPT 1689 packets, 441K bytes)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> </div> <div style="margin-bottom: 10px;"> <p>Chain manage (1 references)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>278</td> <td>31982</td> <td>RETURN</td> <td>!tcp</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>RETURN</td> <td>tcp</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>tcp dpt:!443</td> </tr> <tr> <td>224</td> <td>11672</td> <td>mngif</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>224</td> <td>11672</td> <td>mngaddr</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> </tbody> </table> </div> <div style="margin-bottom: 10px;"> <p>Chain mngaddr (1 references)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>224</td> <td>11672</td> <td>ACCEPT</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> </tbody> </table> </div> <div> <p>Chain mngif (1 references)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>DROP</td> <td>all</td> <td>--</td> <td>lan2</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>DROP</td> <td>all</td> <td>--</td> <td>lan3</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>DROP</td> <td>all</td> <td>--</td> <td>lan4</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> </tbody> </table> </div>							pkts	bytes	target	prot	opt	in	out	source	destination		0	0	ACCEPT	all	-f	*	*	0.0.0.0/0	0.0.0.0/0		10	840	pingif	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 8	74458	43M	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,EST	504	43774	tunnel	all	--	*	*	0.0.0.0/0	0.0.0.0/0		502	43654	manage	all	--	*	*	0.0.0.0/0	0.0.0.0/0		0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 255	138	4416	ACCEPT	2	--	*	*	0.0.0.0/0	0.0.0.0/0		2	656	ACCEPT	udp	--	lan2	*	0.0.0.0/0	0.0.0.0/0	udp dpts:67:68	pkts	bytes	target	prot	opt	in	out	source	destination												pkts	bytes	target	prot	opt	in	out	source	destination												pkts	bytes	target	prot	opt	in	out	source	destination		278	31982	RETURN	!tcp	--	*	*	0.0.0.0/0	0.0.0.0/0		0	0	RETURN	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:!443	224	11672	mngif	all	--	*	*	0.0.0.0/0	0.0.0.0/0		224	11672	mngaddr	all	--	*	*	0.0.0.0/0	0.0.0.0/0		pkts	bytes	target	prot	opt	in	out	source	destination		224	11672	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0		pkts	bytes	target	prot	opt	in	out	source	destination		0	0	DROP	all	--	lan2	*	0.0.0.0/0	0.0.0.0/0		0	0	DROP	all	--	lan3	*	0.0.0.0/0	0.0.0.0/0		0	0	DROP	all	--	lan4	*	0.0.0.0/0	0.0.0.0/0	
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																															
0	0	ACCEPT	all	-f	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
10	840	pingif	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 8																																																																																																																																																																																																																																														
74458	43M	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,EST																																																																																																																																																																																																																																														
504	43774	tunnel	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
502	43654	manage	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmp type 255																																																																																																																																																																																																																																														
138	4416	ACCEPT	2	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
2	656	ACCEPT	udp	--	lan2	*	0.0.0.0/0	0.0.0.0/0	udp dpts:67:68																																																																																																																																																																																																																																														
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																															
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																															
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																															
278	31982	RETURN	!tcp	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
0	0	RETURN	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:!443																																																																																																																																																																																																																																														
224	11672	mngif	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
224	11672	mngaddr	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																															
224	11672	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																															
0	0	DROP	all	--	lan2	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
0	0	DROP	all	--	lan3	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															
0	0	DROP	all	--	lan4	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																															

IPv4 Firewall Screen

This screen shows the active IPv4 firewall, for the purpose of auditing the system.

IPv6 Firewall




FT-6615
03-21-2025 14:07:08

MENU	System IPv6 Firewall Table																																																																																																																																																																																																																																																																
Administration LAN1 (private) LAN2 (internet) LAN3 (internet) LAN4 (internet) Tunnel Tools Status Interface Tunnel Log Tunnel Nodes Tunnel Addr Routing Table DHCP Status PPPoE Log Audit Ports IPv4 Firewall IPv6 Firewall FIPS Module Activate Changes Store Configuration	<p>Chain INPUT (policy DROP 0 packets, 0 bytes)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>DROP</td> <td>all</td> <td>*</td> <td>*</td> <td>*</td> <td>::ffff:0.0.0.0/96</td> <td>::/0</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>all</td> <td>*</td> <td>*</td> <td>*</td> <td>:::1</td> <td>:::1</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>icmpv6_in</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>all</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>state RELATED,EST</td> </tr> <tr> <td>0</td> <td>0</td> <td>tunnel</td> <td>all</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td></td> </tr> <tr> <td>0</td> <td>0</td> <td>manage</td> <td>all</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td></td> </tr> </tbody> </table> <p>Chain FORWARD (policy DROP 0 packets, 0 bytes)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>20</td> <td>1524</td> <td>icmpv6_out</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td></td> </tr> </tbody> </table> <p>Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 2</td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 3</td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 4</td> </tr> <tr> <td>0</td> <td>0</td> <td>pingif</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>DROP</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>pingif</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>DROP</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> <tr> <td>0</td> <td>0</td> <td>DROP</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> </tbody> </table> <p>Chain icmpv6_in (1 references)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th></th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>icmpv6</td> <td>*</td> <td>*</td> <td>*</td> <td>::/0</td> <td>::/0</td> <td>ipv6-icmpdtype 1</td> </tr> </tbody> </table>							pkts	bytes	target	prot	opt	in	out	source	destination		0	0	DROP	all	*	*	*	::ffff:0.0.0.0/96	::/0		0	0	ACCEPT	all	*	*	*	:::1	:::1		0	0	icmpv6_in	icmpv6	*	*	*	::/0	::/0		0	0	ACCEPT	all	*	*	*	::/0	::/0	state RELATED,EST	0	0	tunnel	all	*	*	*	::/0	::/0		0	0	manage	all	*	*	*	::/0	::/0		pkts	bytes	target	prot	opt	in	out	source	destination		20	1524	icmpv6_out	icmpv6	*	*	*	::/0	::/0		pkts	bytes	target	prot	opt	in	out	source	destination		0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 2	0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 3	0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 4	0	0	pingif	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	DROP	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	pingif	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	DROP	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	0	0	DROP	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1	pkts	bytes	target	prot	opt	in	out	source	destination		0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																																									
0	0	DROP	all	*	*	*	::ffff:0.0.0.0/96	::/0																																																																																																																																																																																																																																																									
0	0	ACCEPT	all	*	*	*	:::1	:::1																																																																																																																																																																																																																																																									
0	0	icmpv6_in	icmpv6	*	*	*	::/0	::/0																																																																																																																																																																																																																																																									
0	0	ACCEPT	all	*	*	*	::/0	::/0	state RELATED,EST																																																																																																																																																																																																																																																								
0	0	tunnel	all	*	*	*	::/0	::/0																																																																																																																																																																																																																																																									
0	0	manage	all	*	*	*	::/0	::/0																																																																																																																																																																																																																																																									
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																																									
20	1524	icmpv6_out	icmpv6	*	*	*	::/0	::/0																																																																																																																																																																																																																																																									
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																																									
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 2																																																																																																																																																																																																																																																								
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 3																																																																																																																																																																																																																																																								
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 4																																																																																																																																																																																																																																																								
0	0	pingif	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	DROP	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	pingif	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	DROP	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
0	0	DROP	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																																																																																																																																																																																									
0	0	ACCEPT	icmpv6	*	*	*	::/0	::/0	ipv6-icmpdtype 1																																																																																																																																																																																																																																																								

IPv6 Firewall Screen

This screen shows the active IPv6 firewall, for the purpose of auditing the system. The IPv6 firewall is always active, even if IPv6 mode is not enabled on any of the interfaces.

FIPS Module Status



FT-6615

03-21-2025 13:58:50

MENU	FIPS Module Status
<ul style="list-style-type: none"> Administration LAN1 (private) LAN2 (internet) LAN3 (internet) LAN4 (internet) Tunnel Tools Status Interface Tunnel Log Tunnel Nodes Tunnel Addr Routing Table DHCP Status PPPoE Log Audit Ports IPv4 Firewall IPv6 Firewall FIPS Module Activate Changes Store Configuration 	<pre> HMAC : (Module_Integrity) : Pass SHA1 : (KAT_Digest) : Pass SHA2 : (KAT_Digest) : Pass SHA3 : (KAT_Digest) : Pass TDES : (KAT_Cipher) : Pass AES_GCM : (KAT_Cipher) : Pass AES_ECB_Decrypt : (KAT_Cipher) : Pass RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass Pass ECDSA : (PCT_Signature) : Pass ECDSA : (PCT_Signature) : Pass DSA : (PCT_Signature) : Pass TLS13_KDF_EXTRACT : (KAT_KDF) : Pass TLS13_KDF_EXPAND : (KAT_KDF) : Pass TLS12_PRF : (KAT_KDF) : Pass PBKDF2 : (KAT_KDF) : Pass SSHKDF : (KAT_KDF) : Pass KBKDF : (KAT_KDF) : Pass HKDF : (KAT_KDF) : Pass SSKDF : (KAT_KDF) : Pass X963KDF : (KAT_KDF) : Pass X942KDF : (KAT_KDF) : Pass HASH : (DRBG) : Pass CTR : (DRBG) : Pass HMAC : (DRBG) : Pass DH : (KAT_KA) : Pass ECDH : (KAT_KA) : Pass RSA_Encrypt : (KAT_AsymmetricCipher) : Pass RSA_Decrypt : (KAT_AsymmetricCipher) : Pass RSA_Decrypt : (KAT_AsymmetricCipher) : Pass INSTALL PASSED ##### FIPS install successful. FIPS encryption module enabled. </pre>

FIPS Module Status Screen

The screen shows the results of the self-test run by the FIPS module during boot-up. Please note that because the system uses a multi-cored processor and is running the tests in parallel, the results strings may intermix as seen above for the RSA and RNG tests. This is not an error.

FT-Soft Tunnel Configuration

The screenshot shows the 'Tunnel Configuration' dialog box. It includes the following fields and controls:

- Virtual Interface:** A list box containing 'Ethernet 6' and 'Ethernet 7'.
- Server IP:** A text box containing '192.168.2.114'.
- Port:** A text box containing '22'.
- Backup Server IP:** An empty text box.
- Backup Server Port:** A text box containing '22'.
- Generate Local Key:** A button.
- Idle Disconnect Time:** A text box containing '45'.
- Send Keep-Alive:** A text box containing '15'.
- UDP Transport:** A checked checkbox.
- Send Buffer:** A list box containing '8192'.
- Minimum TLS Version:** Radio buttons for 'TLS-v1.0', 'TLS-v1.2', and 'TLS-v1.3' (selected).
- Allow not yet valid certificates:** An unchecked checkbox.
- Allow expired certificates:** An unchecked checkbox.
- Connect:** A button.
- Exit:** A button.

FT-Soft Tunnel Configuration

Fields

- **Virtual Interface** - The name of the virtual interface. Usually there is only one virtual interface. If your system has multiple instances of the virtual interface, select the name of the interface to use for this instance. If this list-box is empty, it indicates the virtual Ethernet driver is not properly installed.
- **Server IP** - The Public (untrusted) IP address or hostname of the FT server device. This is the FT server that FT-Soft is connecting to.
- **Port** - The TCP port that the FT server is listening to for connections. This must match the FT server configuration.
- **Backup Server IP** - The Public (untrusted) IP address or hostname of a backup FT server device. It may also be the secondary untrusted IP address of the primary server. If FT-Soft is unable to connect to the primary server IP, it will attempt to connect to the backup server. While connected to the backup server IP, it will periodically attempt to reconnect to the primary server IP. Re-connection attempts are randomized between 5 and 10 minutes.
- **Backup Server Port** - The TCP port that the backup FT server is listening to for connections.
- **Idle Disconnect Time** - The amount of time, in seconds, where if FT-Soft does not receive any data packets from the FT Server, FT-Soft will close the current connection and try to establish a new connection. Valid range is 0 - 86400. The value 0 disables the feature.
- **Send Keep-Alive** - The amount of time, in seconds, where FT-Soft will send keep-alive packets to the FT Server device. These packets are sent when there is no data packets to send. The purpose is to prevent the FT server from closing the connection due to its own Idle Disconnect configuration. Valid range is 0 - 86400. The value 0 disables the feature.
- **UDP Transport** - When this box is checked and if the FT server allows it, once authentication is performed over the TCP connection, both FT-Soft and the FT server will switch to a UDP transport instead of the TCP transport. UDP is often a better transport for Ethernet data,

especially when carrying audio or video streams where the recovery mechanism in TCP will interfere with timely delivery of real-time data.

- Send Buffer – This option only applies to the TCP Transport. It sets the upper limit for data stored in the local system TCP buffer. The value is in bytes and may range between 0 and 262144. Choosing 0 disables the feature and causes the system default buffers size to be used.
- Minimum TLS Version – Select the minimum allowed TLS version to use for the connection to the server. TLS v1.0 is no longer permitted.
- Allow not yet valid certificates – X.509 certificates carry a date stamp and validity period. This option will allow the FT-Soft to accept a certificate that is not yet valid when checked against the system's internal clock.
- Allow expired certificates – X.509 certificates carry a date stamp and validity period. This option will allow FT-Soft to accept a certificate that has expired when checked against the system's internal clock.
- Generate Local Key – This button will open a dialog where the user may generate the FT client's local key. This process is similar to generating a local key on the FT hardware boxes.

Notes

- FT-Soft must be running “as an Administrator” in order to modify the FT-Soft configuration. This is because the configuration files are write protected. Once the configuration is set, FT-Soft may be run normally.
- Windows 10 Updates have been know to cause the Virtual Ethernet Adapter to disappear from the system or to lose it's static configuration. If this happens, it may be necessary to remove and reinstall FT-Soft. This is not due to a problem with the FT-Soft. The same problem has been reported for all network adapters.
- Do not disable Idle Disconnect Time or Send Keep-Alive unless you really know what you are doing. The Idle Disconnect mechanism is how FT-Soft recovers from network errors. If you are experiencing excessive Idle-Disconnect errors, it is usually due to problem with your Internet connection.
- When configuring the Virtual Ethernet Adapter, do not set a gateway address. Doing so will override your local gateway causing your PC to lose it's Internet connection. This in-turn will cause FT-Soft to lose the connection to the Server.

FT-Soft Generate Local Key

The screenshot shows a window titled "Generate Local Key" with a close button in the top right corner. The window contains the following fields and controls:

- Name:** A text input field with a help icon (?) to its right.
- Certificate Lifetime:** A text input field containing "3650" followed by "days".
- Optional:** A section header above two text input fields: "Local Password" and "Verify Local Password".
- Certificate Authority (CA) Key:** A section header above a "Find CA" button, a list box, and a "CA Password" text input field. A note next to the list box reads: "Insert USB drive with CA key and press Find CA button to locate the drive."
- Buttons:** "Generate" and "Cancel" buttons at the bottom center.

FT-Soft Generate Local Key

Fields

- **Name** – This is an arbitrary name given to the client. It will show up in the server’s log when the client connects.
- **Certificate Lifetime** – This field sets the time period that the key will be valid. Please make sure the computer’s date and time are correct before generating the local key.
- **Local Password/Verify Local Password** – This is an optional feature. The local key can be password protected, meaning that the key file will be stored on the system in an encrypted format. The user will need to enter this password each time they run FT-Soft. If no password is set, the key file will not be encrypted.
- **Certificate Authority (CA) Key** – In order to generate a local key, you must have the Certificate Authority (CA) USB flash drive generated by your FT server. Insert the USB flash drive into an available port on your PC and press the Find CA. Button. FT-Soft will search the available drives looking for the CA. If found, it will be displayed in the list-box. Highlight the drive letter before proceeding.
- **CA Password** – Enter the password used to protect the Certificate Authority. This password was set when the CA was initially generated.

Notes

- You must run FT-Soft “as an Administrator” in order to save a new local key. If you are not running as an administrator, the key generation will proceed as normal, but will fail when it tries to save the new key.
- Clock mismatch is often the cause of certificate errors. While the clock on a PC is usually correct, the clock on the FT hardware may have been incorrect at the time the CA was generated. This is especially a problem if the time-zone has not been set on the FT hardware. Clock mismatch will self-correct if the difference is small. However, if there is a large discrepancy, it may be necessary to regenerate the CA and re-key your server and clients.
- If the Find CA button does not locate the USB flash drive, please verify the correct drive was installed and that the system has finished installing the device. Some USB flash drives take a few minutes to fully install.

- The USB flash drive containing the CA does **not** need to remain in the system after key generation is complete. The USB flash drive should be removed and stored in a safe place.

Chapter 5

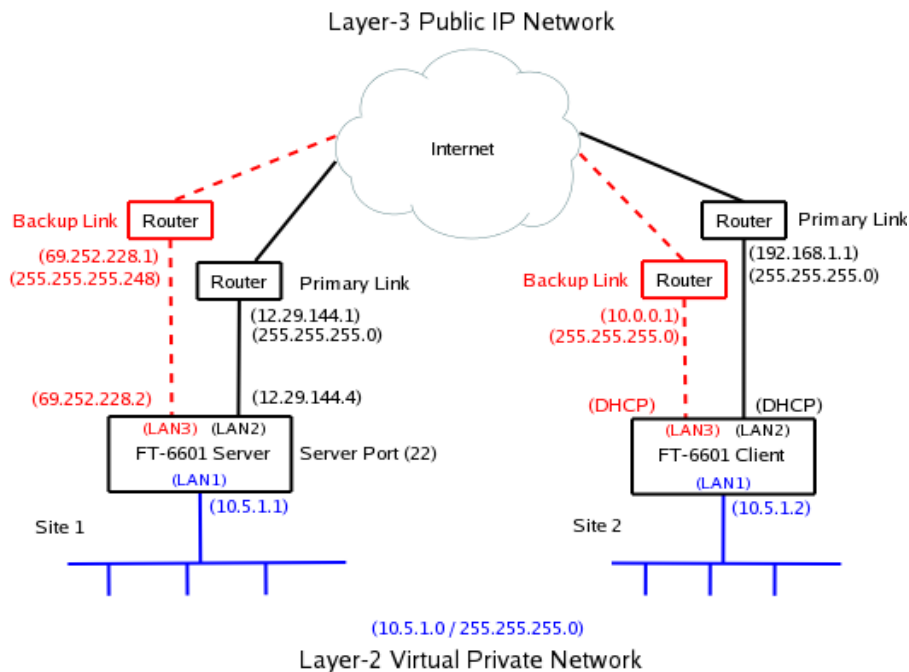
Quick-Start Guide

This Chapter explains how to configure the FT-66xx for use.

Overview

This quick-start guide will walk you through the minimum steps necessary to setup a pair of FTs 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 device except where noted.

The FTs use 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-66xx 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-66xx 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 1.2 or 1.3 protocol.

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-66xx. 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-66xx'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 gives you a chance 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 your 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: Set the Clock

It is important to set the FT-66xx clock prior to generating the security keys. These keys contain time-stamps, and large clock discrepancies can result in certificate errors. Navigate to [Administration – Set Clock](#) to manually set the time. Optionally, navigate to [Tools – NTP](#) and configure NTP. If relying on an NTP server to obtain the time, please verify that the time is successfully set prior to generating any keys.

Step 9: Tunnel – Generate CA Key

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

A USB flash drive was included with your FT-66xx. Insert the USB flash drive into one of the USB ports on the FT-66xx. 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 can be 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 10: Tunnel – Generate Local Key

This step will be performed for each FT device. As a reminder, make sure the FT’s clock has been set before proceeding.

Insert the USB flash drive, containing your CA Key, into one of the USB ports on the FT-66xx. 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-66xx could be named “Home Office Server” and the client FT-66xx 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-66xx devices to your server.

Step 11: Tunnel – Mode

Navigate to the [Tunnel – Mode form](#) and select whether the FT-66xx is operating as the server or the client.

Step 12: 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 13: Tunnel – Configuration (Client)

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

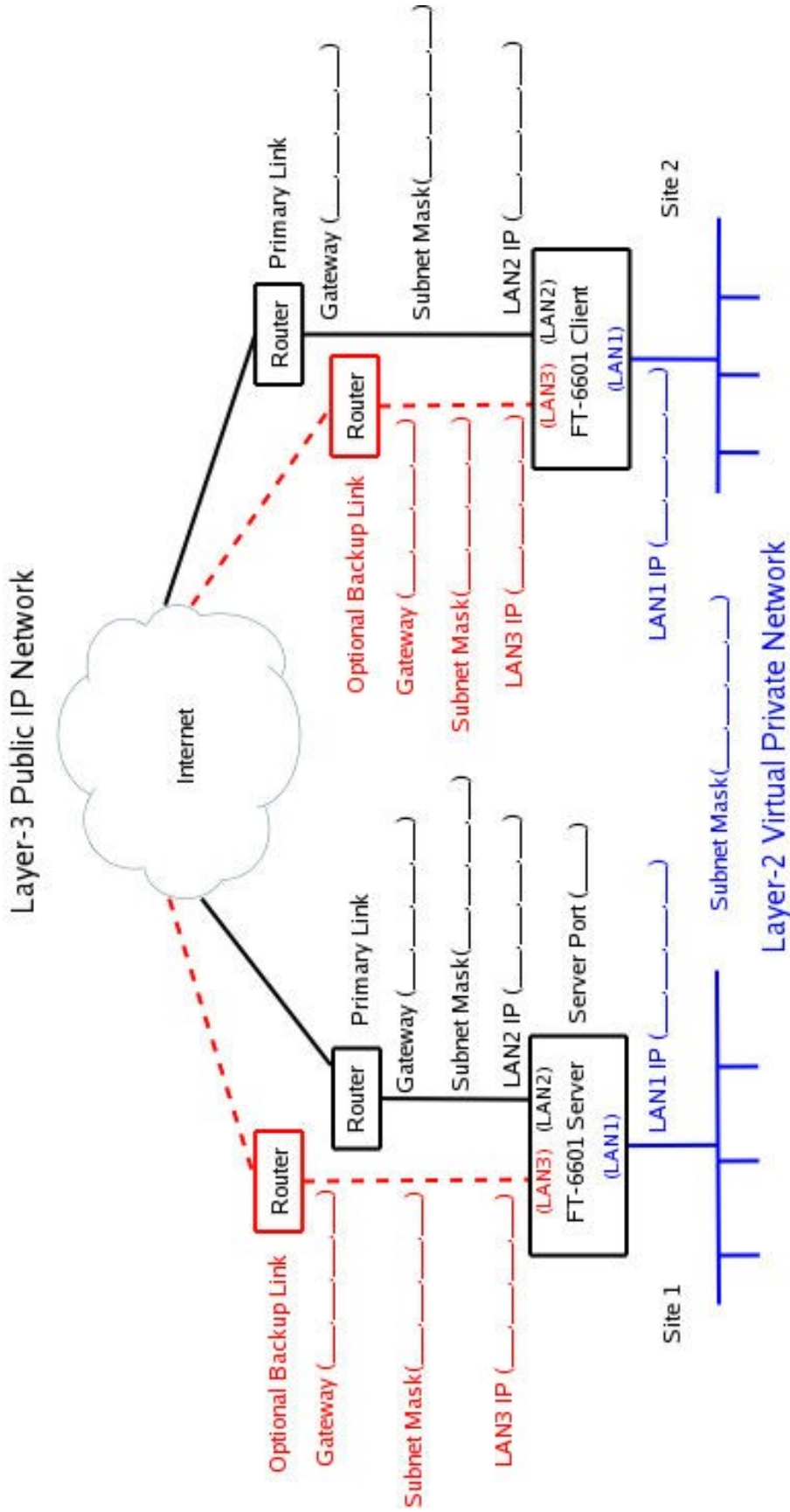
Navigate to the [Tunnel – Configuration form](#). Set the “Connect to Server” field to the Server's LAN2 IP address. Referring to example setup, this would be the 12.29.144.4 address. Set the “port” field to the same port number set in the previous step. Set the “via interface” to LAN2.

If you have a backup Internet connection on LAN3, you can also set the fail-over fields. In our example configuration this would 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 14: 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.



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 FT Series 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, 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. LAN1 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.

Certificate Errors

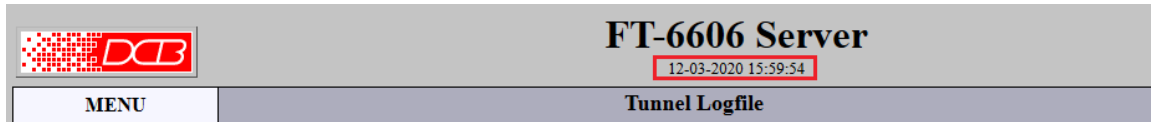
Firmware and software released in December 2020 added some logging feature to help resolve certificate errors. These features are described below.

A common problem when generating the CA and local keys is a discrepancy in each system local clock. A mismatch can result in certificate that won’t be valid until some time in the future. When this occurs, one or both systems will reject the certificate and not allow the connection.

The firmware will now display the validity period for both the CA and the local key. When having problems, compare the validity period to the time as shown by the local clock. Keep in mind that if the unit is configured for a specific time-zone, you will need to account for the time-zone offset. The validity period is always shown in GMT (UTC) time. The local clock will be in local time.

```
12-01-2020 16:11:05 ---Tunnel Started---
12-01-2020 16:11:05 OpenSSL FIPS mode enabled
12-01-2020 16:11:05 TLS v1.2 mode
12-01-2020 16:11:05 CA Certificate
12-01-2020 16:11:05   Name: AnotherTestCA
12-01-2020 16:11:05   Serial No: 9966B6F0A8BFEB83
12-01-2020 16:11:05   Valid from Nov 23 16:00:49 2020 GMT to Nov 18 16:00:49 2040 GMT
12-01-2020 16:11:05 My Local Certificate
12-01-2020 16:11:05   Name: FT-6606 Server
12-01-2020 16:11:05   Serial No: 01
12-01-2020 16:11:05   Valid from Nov 23 16:01:16 2020 GMT to Dec  3 16:01:16 2020 GMT
```

Check the local clock on both of your systems. If the current time is not within the validity period, then you need to either regenerate the certificates or correct the time on the systems so that they are within the validity period. Again, don't forget about any time-zone adjustment. The timezone is set in Tools-NTP.



Another common problem is encountered when deploying a new unit on an existing system. Users that manage multiple FT installations will mistakenly use the wrong CA key on the new system. You can confirm that the correct CA has been used by verifying the CA serial numbers. If the new unit is displaying a CA serial number that differs from the older units in the system, then the incorrect CA key was used.

```
12-01-2020 16:11:05 ---Tunnel Started---
12-01-2020 16:11:05 OpenSSL FIPS mode enabled
12-01-2020 16:11:05 TLS v1.2 mode
12-01-2020 16:11:05 CA Certificate
12-01-2020 16:11:05   Name: AnotherTestCA
12-01-2020 16:11:05   Serial No: 9966B6F0A8BFEB83
12-01-2020 16:11:05   Valid from Nov 23 16:00:49 2020 GMT to Nov 18 16:00:49 2040 GMT
```

If a running system suddenly starts having certificate errors, please verify that the real-time clock in the unit is still functioning properly. Also keep in mind that if it has been running for many years, the certificates may have expired.

FT firmware prior to v2.06 has a known date calculation bug. Using this firmware to generate a CA after 2018 will result in an invalid CA. It is recommended that firmware be upgraded.

Appendix A

Specifications

FT-6602 Bridge Specifications

- LAN 1 Interface: 10/100 BaseT, Autosense
- LAN 2 Interface: 10/100 BaseT, Autosense
- LAN 3 Interface: 10/100 BaseT, Autosense
- OS: Linux
- 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 25 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 +50C
- Dimensions 6 ¼ x 6 x 1 inches

FT-6606 Bridge Specifications

- LAN 1 Interface: 10/100/1000 BaseT, Autosense
- LAN 2 Interface: 10/100/1000 BaseT, Autosense
- LAN 3 Interface: 10/100/1000 BaseT, Autosense
- OS: Linux
- Power: 12 VDC, 6 to 10 watts depending on CPU load.
- Supplied with 100-240 VAC external supply. Optional power supplies available.
- Stand alone package
- Throughput: approximately 40Mbps
- Supports 25 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 0C to +40C
- Dimensions 6 5/8" x 6 1/4" x 1 1/4"
- Shipping weight: five pounds

FT-6615 Bridge Specifications

- Four LAN Interfaces: 10/100/1000BaseTx, Autosense, one trusted and three untrusted interfaces
- Serial Port: RS-232 port
- Sustained throughput: 125 Mbps @ packet size 1470
- Sustained packet rate: 11,145 packet-per-second @ packet size 1470
- Bridge/Tunnel supports 4096 MAC address table entries
- Power: 12 VDC, 2.5A, 30 watts.
- Standard power supply adapter: 100-240 VAC 50/60 HZ
- Indicators: LAN Activity, LAN status (two per interface), power, SSD activity
- Default LAN 1 IP address: 192.168.0.1
- Default LAN 2/3/4 IP addresses: DHCP Client
- In server mode, supports 25 simultaneous clients
- Browser Management port: 443 (HTTPS)
- Operational Temperature: -10 to +50 C
- Humidity: 0 – 95% relative humidity, non-condensing
- Dimensions 4.5” x 4.2” x 1.7”
- Device weight: 1.25 pounds
- Shipping weight: 4 pounds
- Approvals: UL (Power Supply), FCC Part 15 Class B, CE, RoHS
- Export: ECCN 5A002, License exception ENC

FT-6632 Bridge Specifications

- LAN1 Interface: 10/100/1000BaseT, Autosense
- LAN2 Interface: 10/100/1000BaseT, Autosense
- RS-232 interface for initial setup
- 4 – USB interfaces.
- CPU: 8th/9th Intel Xeon, 4 cores, 3.5Ghz.
- OS: Linux
- Power: 120 VAC or 240 VAC, 200 Watts Maximum
- Rack-mount: 1U high
- Throughput: approximately 600Mbps
- Supports 50 simultaneous client FTs
- LED: (Over-temperature warning, LAN Activity, LAN Status (two per interface), Power)
- Default IP address: 192.168.0.1
- Internal Certificate Authority and key generation
- Browser Management port: 443 SSL
- Operational Temperature 10C to +35C
- Dimensions: 1.7” high, 17.2” width, 9.8” depth
- Shipping weight approximately 12 pounds.
- Export: This device may not be exported.

FT-Soft Specifications

- Emulates FT Client device.
- OS: Windows 10/11.
- 32-bit application compatible with both 32-bit and 64-bit systems.
- Virtual Ethernet adapter is NDIS 6.0 Miniport driver.
- Install package supplied on CD.
- License key require per virtual Ethernet adapter.
- Install size approximately 10MB.
- Runtime memory usage approximately 4MB.
- Single-threaded application.
- Performance depends on host system hardware and OS version.

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

FT		PC
1,6	——	4
2	——	3
3	——	2
4	——	1,6
5	——	5
7	——	8
8	——	7

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.

FT-6615 Serial (COM) Port

The FT-6615 serial port is implemented on an RJ45 connector. An adapter is provided to convert from the RJ45 connector to a DE9 female, suitable for direct connection to a PC COM port.

RJ45	DE9	DTE Signal Name	Signal Direction to/from FT-6615
Pin 1	Pin 8	RTS	Output
Pin 2	Pin 6	DTR	Output
Pin 3	Pin 2	TXD	Output
Pin 4	Pin 5	GND	
Pin 5	Pin 5	GND	
Pin 6	Pin 3	RXD	Input
Pin 7	Pin 4	DSR	Input
Pin 8	Pin 7	CTS	Input

The above cable is widely available, often described as a router console management cable.

Bridge to hub or Ethernet switch

Use any commercially available 10/100/1000 BaseT cable. If using 100 or 1000 BaseT, 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 operating system is Linux, available from <http://www.kernel.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

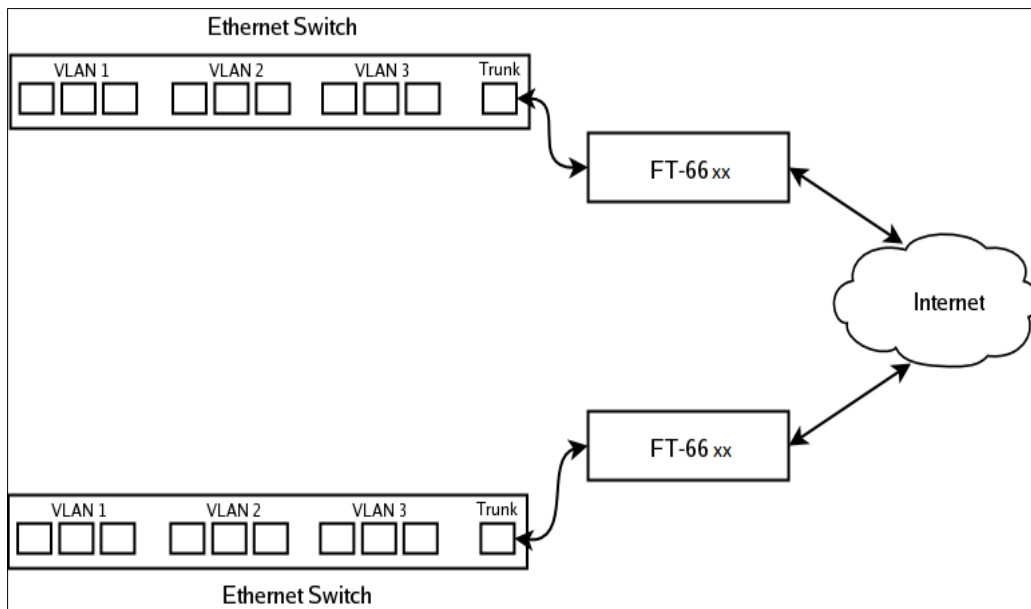
Appendix C

802.1Q VLAN Tagging

The FT Series products supports bridging of 802.1Q VLAN packets.

Introduction

The FT series products support bridging 802.1Q Tagged Ethernet. An application for this is shown below where two 802.1Q VLAN switches are being tunneled across the Internet.



VLAN Configuration Differences

The default configuration for the 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.

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.