LLEA

Encrypted Ethernet Layer II Tunnel

User's Guide

Revised 07/23/2020

Firmware Version 1.x

Certifications

FCC Statement

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

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

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

RoHS

Some models of this product is available in RoHS versions.

TABLE OF CONTENTS

Chapter 1
Introduction

This chapter provides an overview of the EtherSeries LLEA Layer Two Tunnel's features and capabilities.

Congratulations on the purchase of your LLEA high performance layer two encrypter. This is a simple, easily configured tunneling device containing two ethernet interfaces that provides lilnk layer 2 encrypterion performance above 900 Mbps using gigabit ethernet interfaces. It contains a FIPS 140-2 Level 1 validated encryption module.

LLEA provides layer 2 security by allowing two layer-2 network segments to be securely bridged across an insecure network segment at high speed as a layer 2 tunnel. They are used in pairs to create a point-to-point layer 2 tunnel between the two layer-2 segments. Network traffic that traverses the the insecure network segment is protected against eavesdropping and tampering by the layer 2 tunnel. In addition, the ***LLEA*** devices protect the network segments from malicious packet injection with layer 2 encryption and authentication.

AES encryption and HMAC-SHA1 for data integrity are used in the ***LLEA***. The Diffie-Hellman algorithm is used for session key establishment. Encryption keys are changed every 6-hours or 2 billion packet, whichever comes first. All cryptographic operations are provided by an embedded FIPS 140-2 Level 1 validated cryptographic module.

The original Ethernet packets are completely encapsulates by ***LLEA*** for transport across the insecure network segment. To minimize the overhead of encapsulation and encryption, the ***LLEA*** will coalesce packets where possible for high performance on gigabit ethernet encryption links. This reduces the number of small packets that traverse the insecure network often improving the throughput of a slower network link.

This link layer encrypter can transport both standard Ethernet packets and 802.1q tagged VLAN packets. Since packets are encapsulated when transported across the insecure network segment, this has the effect of tunneling 802.1q across a network segment that may not support it while providing 802.1q encryption. Inter-site VLAN encryption has a side benefect... the packets that traverse the insecure network segment will always appear as standard Ethernet packets.

LLEA requires very little configuration. In fact, it is possible to deploy a pair with no configuration at all. Just place them in-line and turn them on. Typical configuration consists of setting an IP address, a shared secret, and selecting the encryption level. Configuration is web based with a click-for-help hyperlink on every configuration item.

This is a layer 2 FIPS 140-2 compliant product using a validated encryption module. Due to the encryption employed in these products, they are export controlled items and are regulated by the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce. They may not be exported or shipped for re-export to restricted countries in Country Group E:1. They are shippable to most other countries with proper licensing. Please contact us if you are considering exporting these.

LLEA Applications

LLEA provides a high speed encrypted tunnel between two LAN segments. It allows secure connections between those LAN segments using any unencrypted layer two ethernet connection such as point-to-point microwave, fiber WAN connections, MAN, or other layer two ethernet paths.

Other Features

Protocols

The encrypter uses raw, layer two ethernet packets to connect to its remote peer. It encrypts and passes all valid ethernet protocols, including but not limited to IP, TCP/IP, UDP,IP, multicast IP, etc.

Easily Configured

The LLEA may be installed with virtually no configuration, however minimal configuration is recommended to provide a management interface and maximum security. Default encryption configuration is AES-128, which many users change to AES-256 for compliance with agency regulations.

802.1q VLAN

The encrypter passes 802.1Q VLAN tagged packets.

Upgradeable Firmware

Firmware upgrades may be installed using any web browser.

FIPS-140 Validation

This is a layer 2 FIPS 140-2 compliant product using a validated encryption module. Due to the encryption employed in these products, they are export controlled items and are regulated by the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce. They may not be exported or shipped for re-export to restricted countries in Country Group E:1. The *LLEA* uses an embedded FIPS 140-2 validated cryptographic module (Certificate #1747) running on a Linux x86 platform per FIPS 140-2 Implementation Guidance section G.5 guidelines

Package Contents

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

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

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

Software Requirements

The layer two tunnel encrypted bridge supports any protocol built upon raw Ethernet**. As a layer two encrypter, it bridges any valid Ethernet protocol**. The initial IP address may be entered using any terminal or terminal emulation software on a PC through the serial port, or the default may be used if appropriate for your network..

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

LLEA Hardware

Introduction

The LLEA Ethernet Tunnel contains two 10/100/1000BaseT Ethernet ports (Fiber interfaces optional) and two USB ports. It is designed for operation with a direct point to point raw ethernet connection. The ***LLEA*** uses an embedded FIPS 140-2 validated cryptographic module (Certificate #1747) running on a Linux x86 platform per FIPS 140-2 Implementation Guidance section G.5 guidelines

Configuration

This model contains a serial interface to be used in initial setup (if needed) and two USB interfaces (used only if browser certificates are enabled). IF the default IP address of 192.168.0.100 is not appropriate for your LAN and you can not temporarily re-configure a PC to that subnet, connect a terminal to the serial port following the instructions in the configuration section. The setup port is always active on this model**.** Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are used for full configuration.

LLEA Front

LED Indicators

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

USB Connectors

There are two USB connectors. They are interchangeable, and only the first one that senses a USB device connection is activated. The USB interface is used to transfer x509 security certificates (if used) for secure communications with certificate-based web browser authentication.

RS-232 Connector

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

Ethernet Connectors

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

Chapter 2
Installation

This Chapter details the installation process for the Layer two encrypted tunnel.

Overview

The unit is normally configured using a web browser directed to its address. If the default address of 192.168.0.100 is appropriate for your local network, then plug it in and simply direct your web browser to the management web browser interface (using https without using a proxy) and continue with configuration. If this address is not appropriate for your network, the IP address must be configured using the initial terminal method below, or you may temporarily re-configure a PC to the 192.168.0.x subnet.

The CDROM contains a Configuration Worksheet document and more detailed step-by-step

Quick Start

Quick start instructions are in the following chapter and in a separate document provided with the unit. Installation is an easy process, but you are must have an 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 this or any other network hardware.

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 LLEA's IP address

If the default address (192.168.0.100) 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 unit.
2. Start the terminal emulation program using 9600 bps, 8-bits, No parity, No flow control.
3. Power up the unit.

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

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

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

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

8. These values will now be compressed and saved the configuration to flash memory. Do not cycle power during this time or the unit may be rendered inoperable.

9. The encrypter will now reboot.

The entire dialog is listed below:

-------- LLEA Setup Program --------

Welcome to Setup. This setup will establish the LLEA 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: 192.168.0.100

SM: 255.255.255.0

GW:

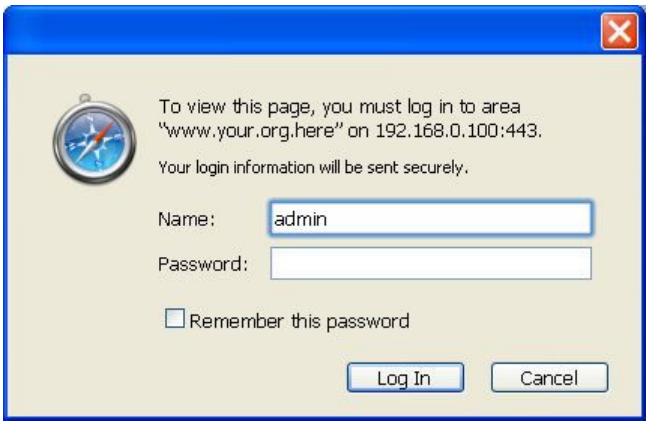
Set ALL parameters to default (y/[n])? y
Should LAN1 use DHCP to get an IP address (y/[n])? n
LAN1 IP Address is currently: 192.168.0.100 Enter new IP Address, or blank for no change:
LAN1 Subnet Mask is currently: 255.255.255.0Enter new IP Subnet Mask, or blank for no change:
LAN1 Gateway Address is currently: Enter new IP Subnet Mask, or blank for no change:
Will LAN1 be connected to an 802.1Q tagged VLAN trunk(y/[n])?
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://192.168.0.100
rebooting system
-----

2. Connect the Ethernet Cable

Connect a LAN cable from your hub or switch to Ethernet Port LAN1 (the leftmost ethernet connection). Reboot the unit with a power cycle. The management web server interface will now be available to any web browser on the same LAN segment. If your web browser does not receive a response, verify that you do not have a proxy server configured in the browser and are using https instead of http for a secure connection. If so, properly configure the browser to bypass the proxy server for this URL. The default address is 192.168.0.100. 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://192.168.0.100 if using the default address) into your web browser. The login screen below should be displayed.

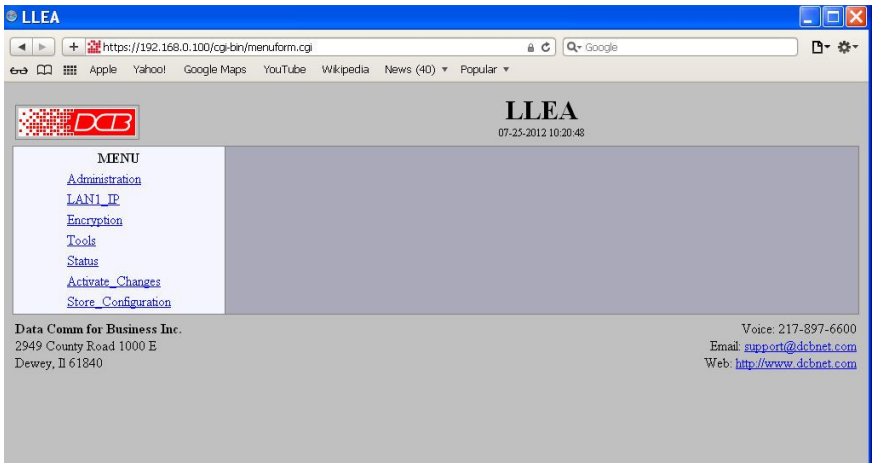


Login Screen

Since the LLEA uses a self-signed security certificate, your web browser may warn you that the security certificate is untrusted. You may ignore this warning, and if desired, later create x509 certificates on the LLEA and install companion certificates on your workstation.

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

4. Enter Configuration Values



Initial Main Menu

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

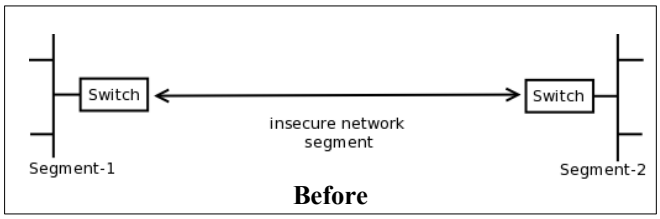
5. Minimum Configuration

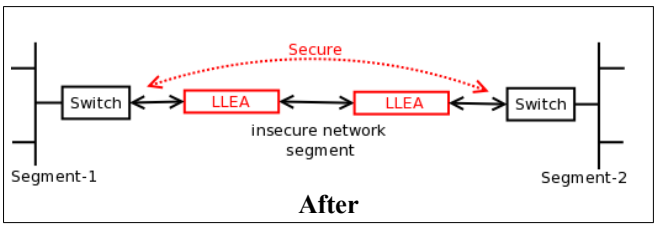
The minimum configuration items required for basic LAN-to-LAN encrypted bridging connection are detailed in the ***LLEA Quick Setup Guide***. This information is duplicated below.

LLEA Quick Setup Guide

Thank you for your purchase of the **LLEA** Link Layer Encryption Appliance. This quick setup guide will walk you through the minimum steps necessary to configure the device in a typical application.

The **LLEA** devices are used in pairs to secure a layer-2 Ethernet segment. An example application is shown below. The insecure network segment could consist of a simple wire or include additional devices such as hubs, switches and wireless bridges. The only requirement is that the insecure network segment must reside in the same broadcast domain. No layer-3 devices, such as a router, may be in the path.

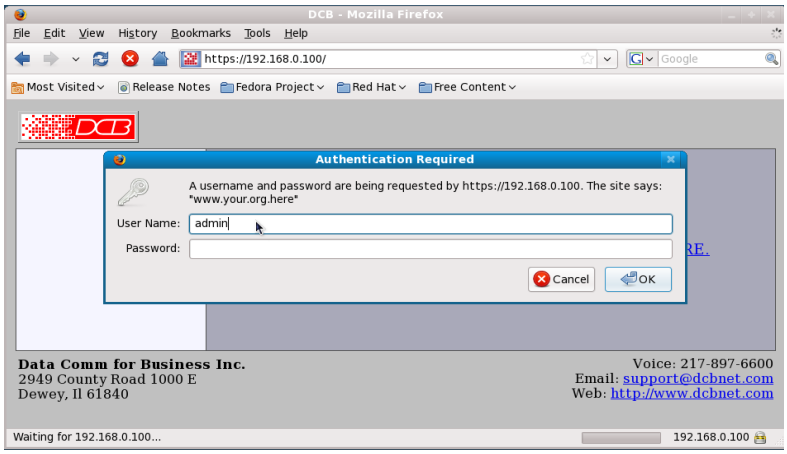




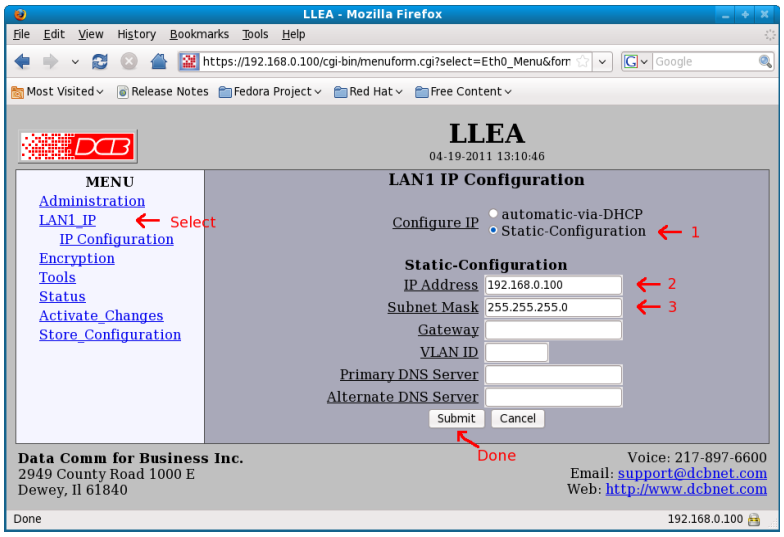
The **LLEA** is configured through the LAN1 Ethernet interface using a web browser. It has a default IP address of 192.168.0.100 and a subnet mask of 255.255.255.0. If this address is not compatible with your PC, temporarily configure your PC with an address on the 192.168.0.x subnet. For example, use the address 192.168.0.99.

Start your web browser and enter https://192.168.0.100 as the web address. Please notice the "s" in https. When you first connect to the **LLEA**, you will receive a security warning. This is because the device uses a self-signed certificate. Please choose to "continue to this website" or to "add an exception". If you are using Firefox, it will also be necessary to "get the certificate" and to "confirm security exception".

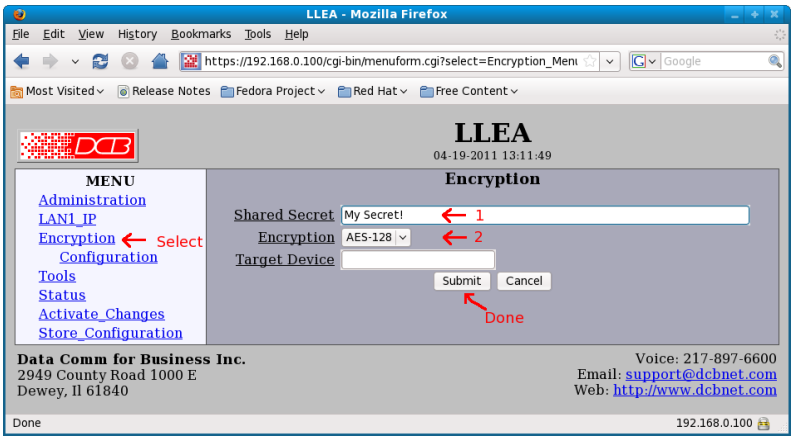
When prompted, enter ***admin*** as the User Name. Leave the Password field blank.



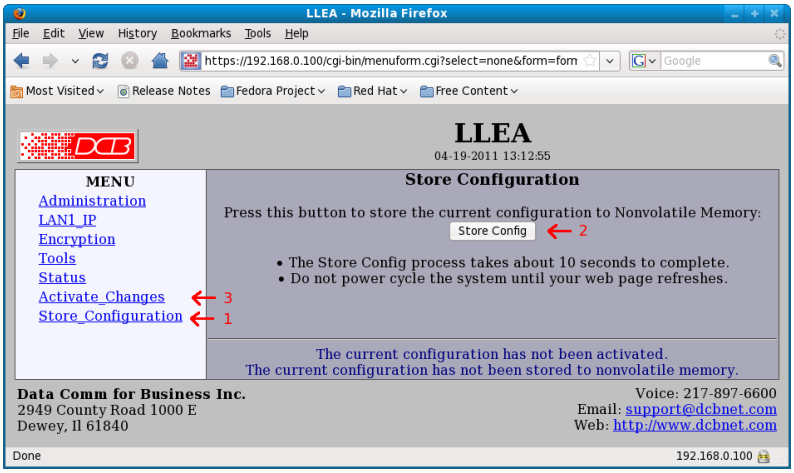
Go to the ***LAN1_IP*** configuration page. Select the ***Static Configuration*** button and configure the ***IP Address*** and ***Subnet Mask***. The other items on this page are optional. If you know the correct values, go ahead and enter them. However, they are not required in a minimal configuration. Press the ***Submit*** button when done.



Next, go to the ***Encryption*** configuration page. Enter a ***Shared Secret*** and choose an ***Encryption*** method. The shared secret can any combination of letters, numbers, spaces, and most symbols. It is case sensitive. Remember your settings. When you set up the second **LLEA**, you will need to enter the same values. The other items on this page are optional and not needed in a typical configuration. Press the ***Submit*** button when done.

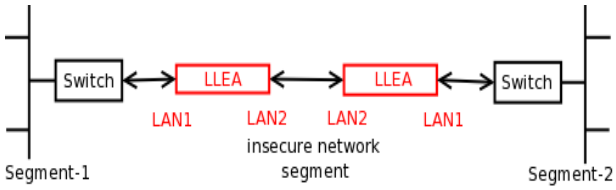


Finally, store and activate your changes. To store, select ***Store Configuration*** and confirm the operation by pressing the ***Store Config*** button. To activate, select ***Activate Changes***. Once you active the changes, the new IP address will take effect. To access the device again, you will need to enter the new IP address in the web browser address field.



Repeat the above operations for the second **LLEA**. Make sure to use a unique IP address, but use the same Shared Secret and Encryption method.

The **LLEA**s are ready to deploy. Attach the LAN-2 Ethernet interfaces to the insecure network segment and the LAN-1 Ethernet interfaces to the secure network segments as shown below.



Troubleshooting

If you are unable connect to the **LLEA** using the web browser, check the following:

- Verify that you are plugged into the LAN1 interface and that it is showing a valid link indication (LAN1 LEDs illuminated).
- Verify that your PC and the ***LLEA***are connected on the same LAN. To be sure, plug a cable directly between your PC and the **LLEA**.
- Verify that your PC is configured with an IP address on the same subnet as the **LLEA**. On Windows you can do this by opening a command prompt and running the command "ipconfig". Your Local Area Connection should show an address on the 192.168.0.x network with a subnet mask of 255.255.255.0.
- Verify that your Web Browser is not configured to use a proxy. For Internet Explorer, open "Tools Internet Options". Select the "Connections" tab. Press the "LAN settings" button. Uncheck "Use a proxy" or check "bypass proxy for local addresses". For Firefox, open "Edit – Preferences". Select the "Network" tab. Press the "Settings" button. Make sure "No Proxy" is selected.
- If you are still unable to connect, the **LLEA** may not be configured to the default address. You can check the IP address and/or reset it using the **LLEA**'s serial port or by attaching a PS2 keyboard and VGA monitor. If you use the serial port, configure your terminal emulator for 9600 baud, 8-bits, 1-stop, no parity, and no flow control. You will need to use a null modem cable.

Free technical support is available by phone during central time zone office hours at 217-897-6600. Please call out technicians if you have any problems installing the ***LLEA.***

---- End of Quick Setup Guide ---

Chapter 3
The Configuration Process

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

Overview

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

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

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

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

Using the Configuration Flexibility

When starting from a power-off condition, an active configuration loads from 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 hardware 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. However, upon the next reset or power cycle, the unit will begin using the stored configuration.

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

Configuration Process Examples

Example 1:

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

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

Example 2:.

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

This method allows one to configure the unit remotely while using the link in a manner 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 hardware is reset (which may be performed remotely), it will begin using the new configuration. This method is useful when you are configuring to use a new LAN address range while it is on the old LAN. It's also used when the tunneled link connection is the management path, and the new configuration will not allow that connection.

Example 3:

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

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

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

Saved Configuration Files

The saved configuration file is a encrypted binary file. It is saved using a unique password, and that password must be used to retrieve the saved configuration. The file may be archived for future use.

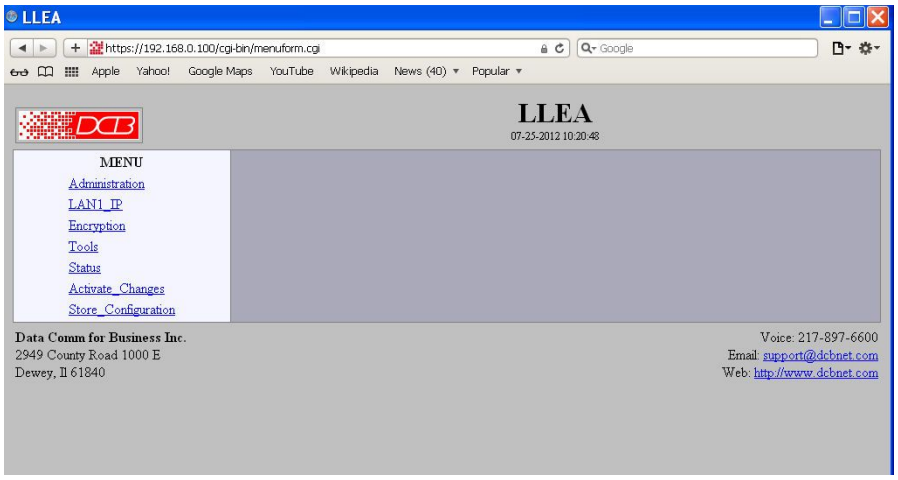
Chapter 4
Configuration

This Chapter describes configuration screens and some configuration hints for the LLEA

Overview

The LLEA is configured using forms displayed on a web browser. In this chapter, we illustrate all entry forms, and describe their use.

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.



LLEA Main Screen

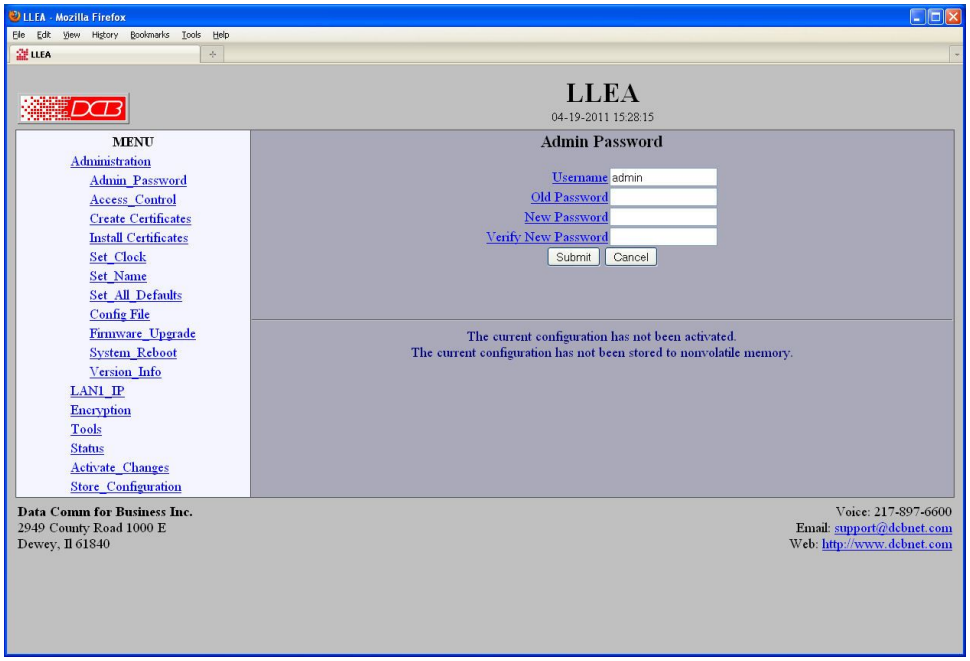
From this index, click on a menu keyword to open the appropriate screen. In this manual, screens are discussed in the order shown on the index screen.

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

Administration

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

Admin Password



Admin Password Screen

Access to the configuration web server is protected by HTTP Basic Authentication and uses the secure web server. This is a simple methodology where the web server will require a web browser to provide a username and password for each page requested. The Web Browser will typically ask the user to enter the username and password once, then will remember it for the duration that the Web Browser is running. For all LLEA models in default configuration, use https: (instead of http:) when addressing the web browser screens.

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

Fields

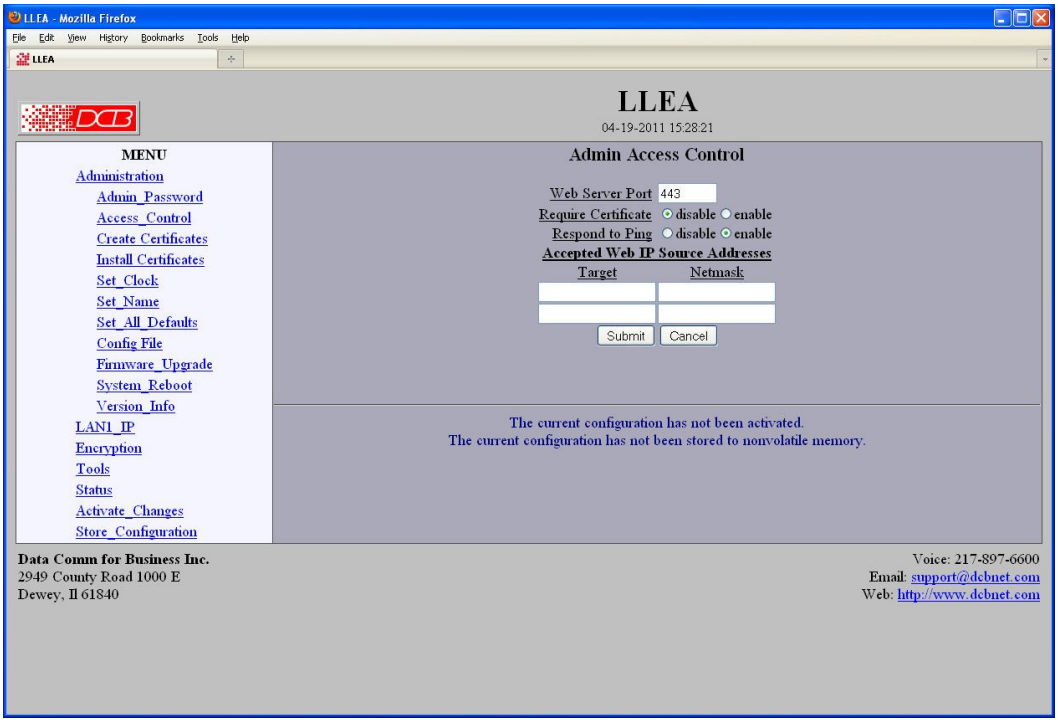
- User Name
  This field may be a string of 0 to 15 printable characters. Do not use space or control characters. If you leave this field blank, you will need to enter a blank username during authentication.
- Old Password
  In order to change the username and password, you must know the old password.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

- New Password
  When changing the username and password, this field provides the new password. It may be a string of 0 to 15 characters. If you leave this field blank, you will need to enter a blank password during authentication.
- Verify New Password
  Retype the password to verify that it was correctly entered.

Notes

- If you forget your username or password, you can use the Serial Port Setup to erase the current settings and return the unit to factory defaults. **There is no way to retrieve a forgotten password!**
- Security Note: HTTP Basic Authentication may be easily hacked if the attacker has the ability to sniff network packets. For this reason HTTPS: secure sockets layer methods should be used. Otherwise, the username is transmitted in the clear and the password is transmitted in an obfuscated but possibly recoverable format.

Admin Access Control



Administrative Access Control Screen

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

Fields

- Web Server Port
  This is the TCP Port to use for the internal Web Server. Typically it is set to port 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 web interface and attempt to break in. A different port may be needed to accommodate local firewalling.

If you change the web server port number to port 443, remember that you will have to include the port number in your URL. For example, https://192.168.0.1:7995 OR https://192.168.0.1:7995 .

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

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

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

- Accepted Web IP Source Address
  This table allows you to control what hosts or networks have access to the web server. If empty, any host may access the unit.

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

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

  Target: 192.168.10.0 Netmask: 255.255.255.0

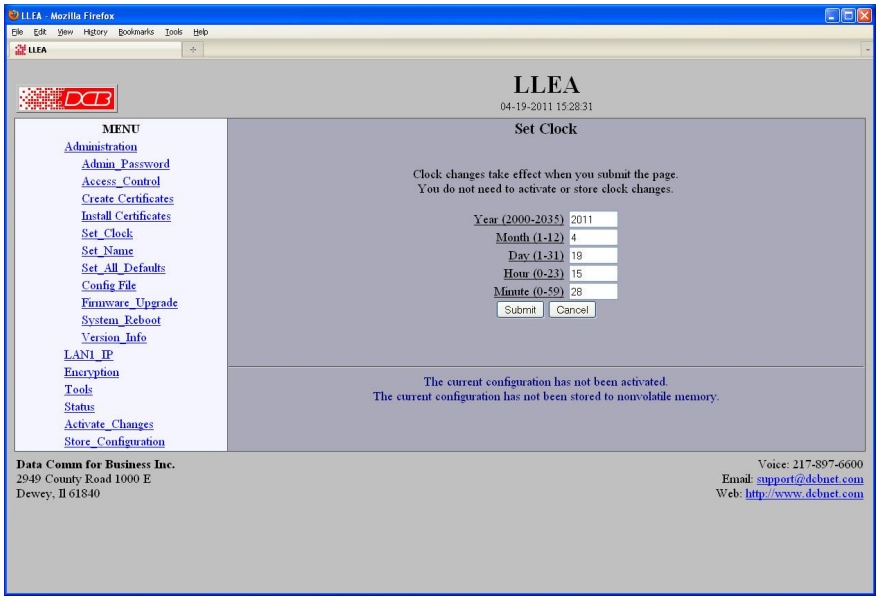
- Target
  Host or Network address.

- Netmask
  If blank or set to 255.255.255.255, target is assumed to be a host address. Otherwise, target is treated as a network address.

Notes

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

Set Clock



Set Clock Screen

This form allows you to set the real time clock. The setting will take effect as soon as you submit the page, you do not need to activate or store the changes.

Fields

Year Year in the range 2000 to 2035.

Month Numeric value of month in the range 1 to 12.

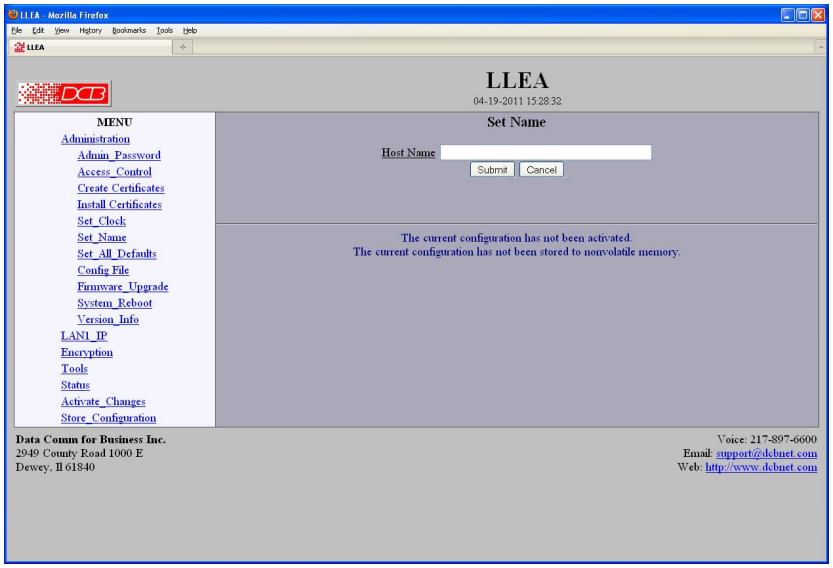
Day Day of month in the range 1 to 31.

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

Minute Minutes in the range 0 to 59.

Notes

Set Name



Set Name Screen

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

Fields

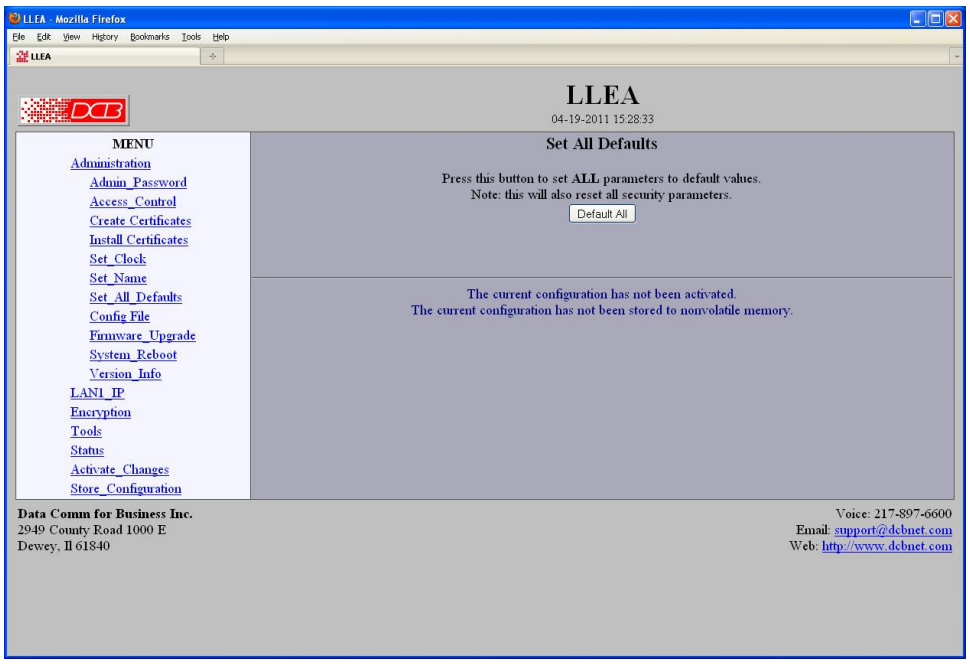
Host Name

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

Notes

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

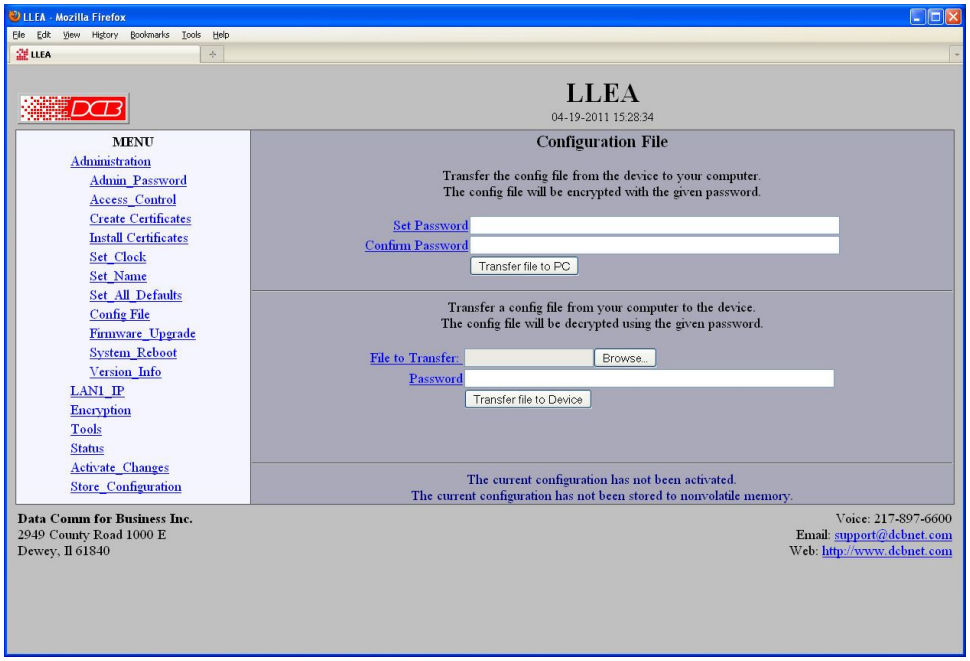
Set All Defaults



Set All Defaults Screen

This form will allow you to set all configuration values to their default value. Before you "Activate Changes", you should configure the interface that you are using to access the unit. Otherwise, the unit will be configured with the IP address of 192.168.0.100.

Configuration File



Configuration File Screen

This form will allow you to copy the LLEA internal configuration to a file on your PC. You can also use the form to transfer a configuration file from your PC to this or another LLEA.

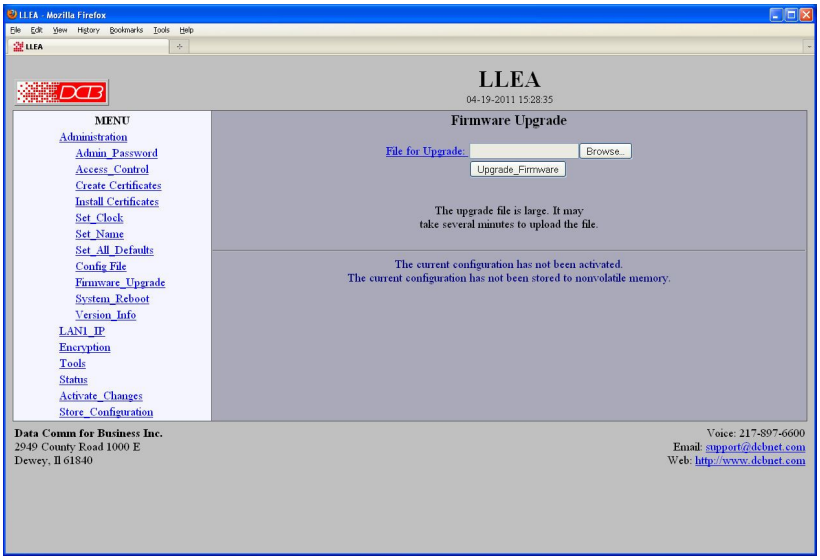
Fields

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

Notes

- The configuration file is an encrypted binary file. You must know the password to unencrypt the file later.
- You may save multiple configuration files on the PC by using different names for them.
- After transferring a configuration file to the current or new hardware, you may either activate the changes (with the activate screen), or store the changes (with the store configuration screen). If you activate the changes, the unit will immediately begin using the new configuration. If the changes are stored, the unit 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 unit using its new configuration. Otherwise, it may be necessary to return to the old stored configuration with a reset.

Firmware Upgrade



Firmware Upgrade Screen

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

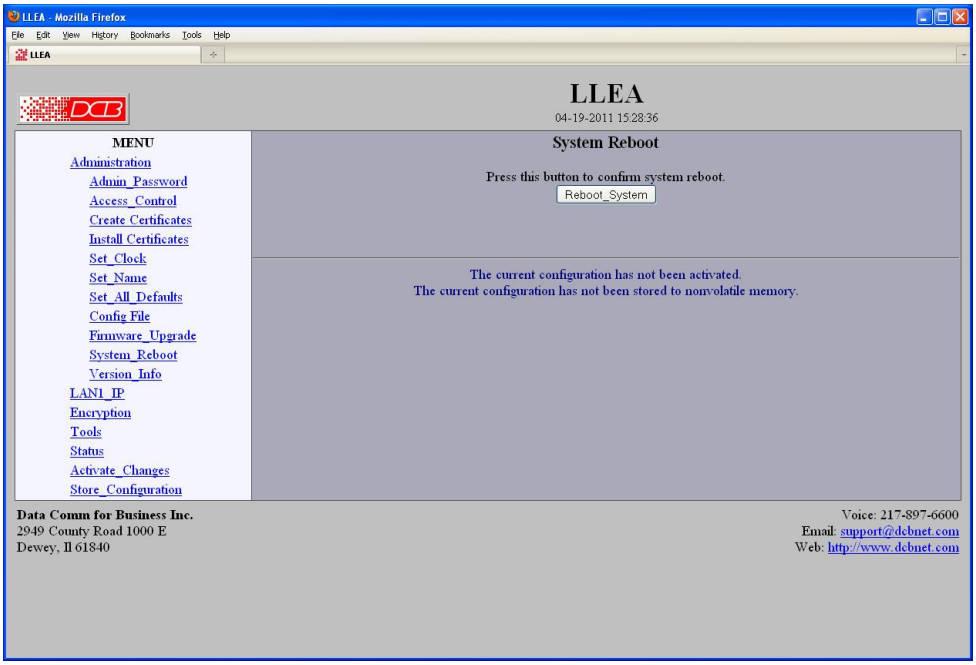
Fields

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

Notes

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

System Reboot



System Reboot Screen

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

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

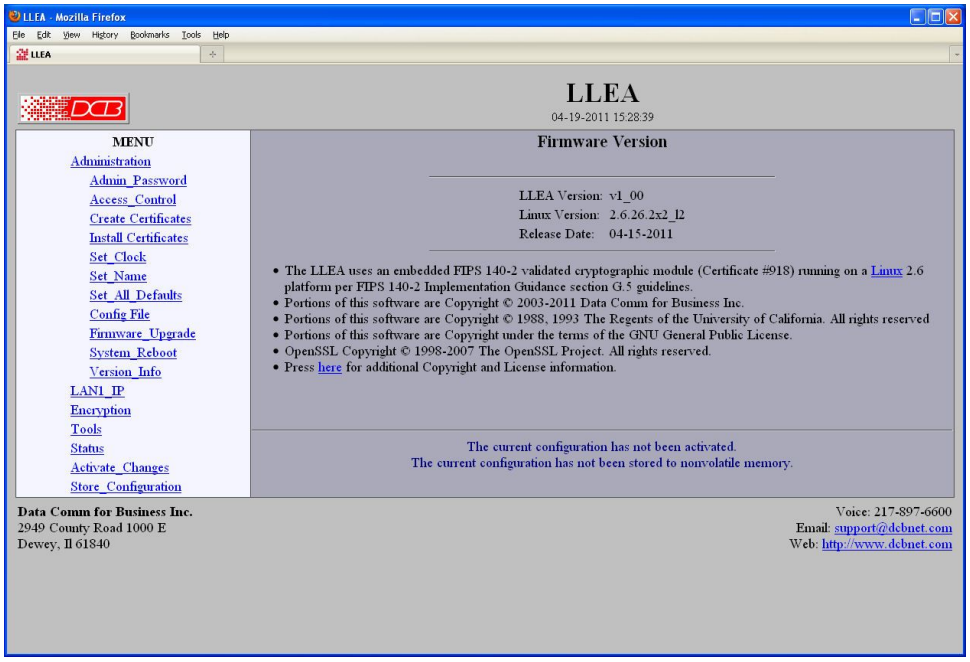
Fields

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

Notes

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

Version Information Screen

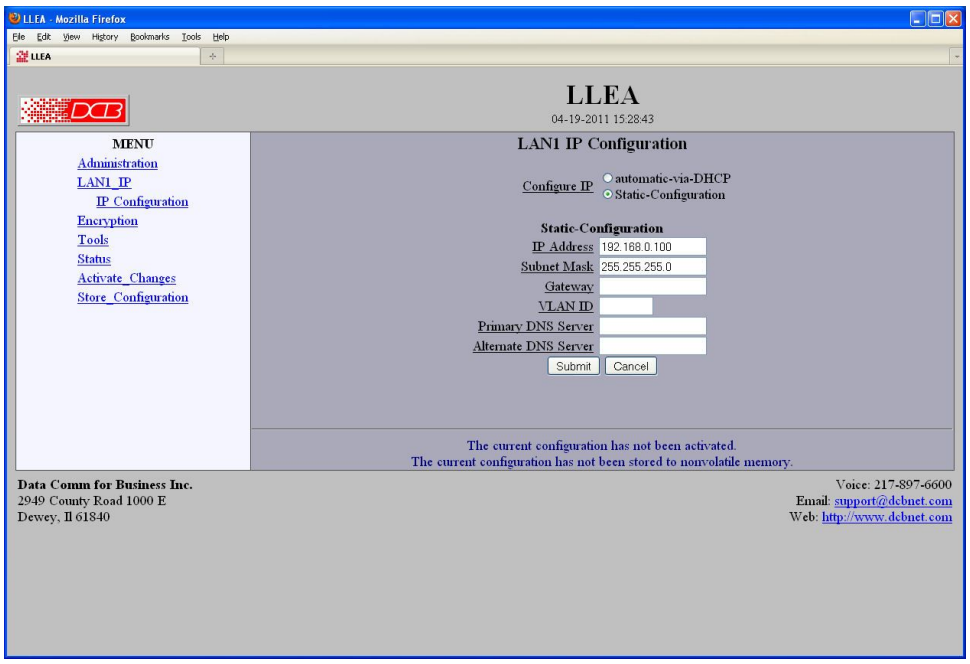


Version Information Screen

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

1.

LAN 1 IP Configuration



Lan 1 IP Configuration Screen

The LLEA contains two ethernet interfaces. LAN 1 (the leftmost interface) is used for the "local" trusted LAN. LAN 2 is the untrusted, interface connecting to the companion LLEA. LAN 1 is always a local, secure side of the tunnel. This screen is used to configure IP parameters for LAN 1.

Fields

- Configure IP
  Select DHCP or a static configuration. If DHCP is selected, the static-configuration is ignored.
- IP Address
  An IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. The default value is 192.168.0.100.
  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.

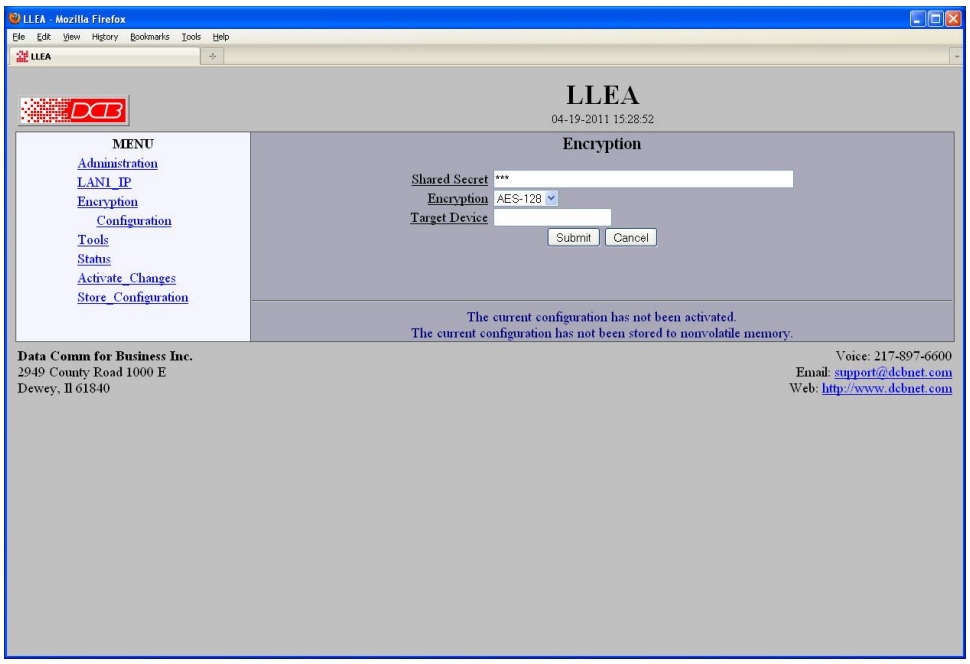
- VLAN ID
  If the Ethernet interface is attached to an 802.1Q trunk, you must specify a VLAN ID number for the interface. The IP address will be then be bound to this VLAN. This will allow you to access the LLEA's web server through the 802.1Q trunk from the specified VLAN. Valid range is 0 - 4095. Leave blank to disable.

  Note: *Static-configuration* must be used on LAN 1 if it is configured for an 802.1Q VLAN.

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

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

Encryption



Encryption Configuration Screen

Fields

Shared Secret
The Shared Secret is used for authentication. Both devices must be configured with the same shared secret. This secret phrase is used to generate the AES key used to cypher the communications. The secret phrase may be up to 52 characters in length. Do not use a quote or backslash character in the phrase. Best security requires a long, random shared secret.

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

Target Device

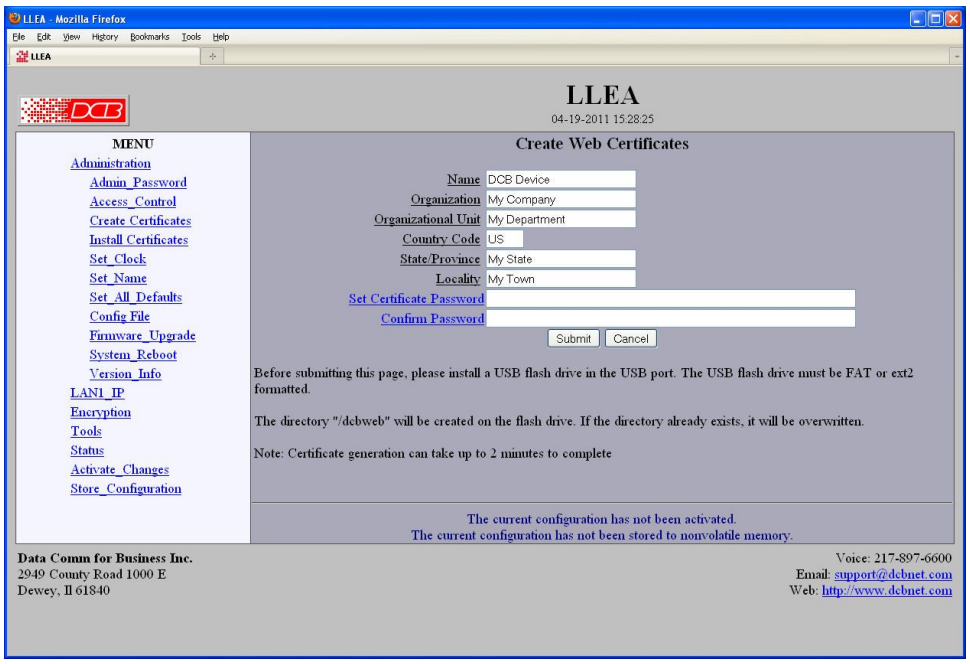
If this field is blank, the device will try to automatically detect and associate with a peer device. If you enter an Ethernet Address (MAC), the device will only associate with the specified device. This is necessary if you will be running more than 1 pair of encryption devices on a single network segment.

When entering the Ethernet MAC Address, use the LAN2 address of the peer device.

Notes

•

Create Web Certificates



Create Web Certificates

This form will allow you to create two x509 certificates into the secure web server. One certificate is used to identify the web server. The second is used to verify the identity of the web browser.

The internal secure web server operates using the SSL protocol. SSL allows for the use of x509 certificates to identify and authenticate web servers and web browsers. You may use this form to generate a pair of x509 certificates. One to identify the device's web server and the other to identify your computer's web browser.

This form only generates the certificates, writing them to a USB Flash Drive inserted into one of the USB ports on the device. Separate steps are required to install the certificates into the device's web server and your computer's web browser. For more information, see installing web certificates.

Four file will be written to the directory:

```
dcbweb/
   wbrowser.p12 - browser certificate file in PKCS12 format
   wbrowser.pem - browser certificate file in PEM format
   wserver.pem  - server certificate file in PEM format
   wserver.key  - server private key file
```

Note: Certificate generation may take several minutes to complete.

Fields

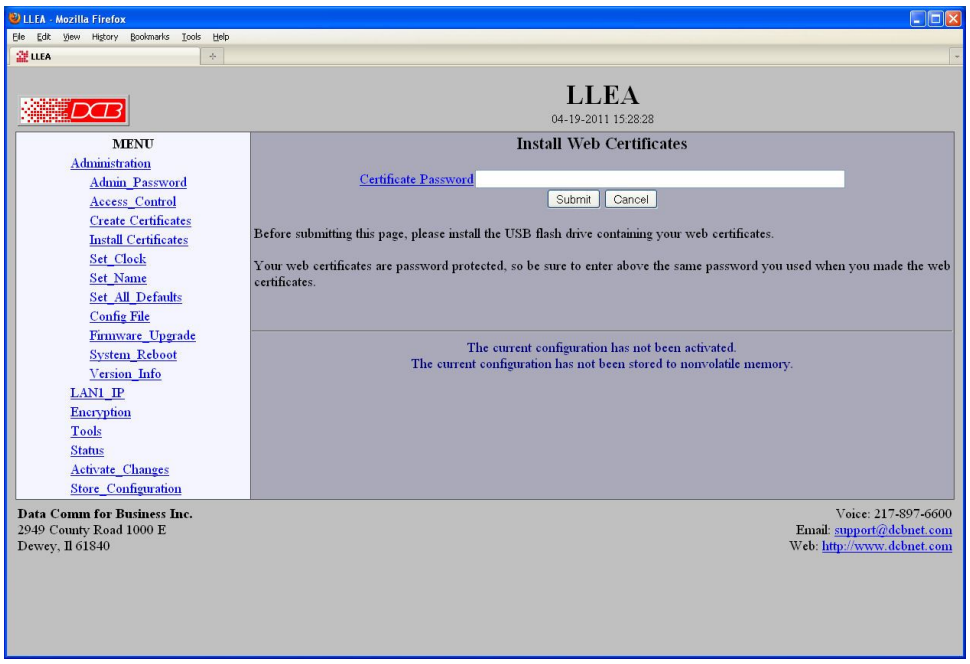
- Name
  The common name given to the certificate. The supplied name will be appended with the word "Server" for the server certificate and the word "Browser" for the browser certificate. Name may be 1 to 64 characters in length, limit to alph-numeric characters.
- Organization
  The organizational name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

Notes

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

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

Install Web Certificates



Install Web Certificates

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

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

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

Browser Certificate
- Make sure the "Your Certificates" tab is selected.
- Press the "Import" button.
- You will be prompted for your Master Password.  The Master
  password is for protecting your web browser's certificates.
```

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

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

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

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

- Insert the USB Flash Drive into your computer.
- For Firefox 1 and 2:
  Go to "Edit/Preferences/Advanced/Security".
- For Firefox 3
  Go to "Tools/Options/Advanced/Encryption".
- For Internet Explorer:
  Go to "Tools/Options/Privacy".
- Click on the "View Certificates" button.

Browser Certificate
- Make sure the "Your Certificates" tab is selected.
- Press the "Import" button.
- You will be prompted for your Master Password. The Master password is for protecting your web browser's certificates. If this is the first time you have imported a certificate,

```
  you will be asked to create a password.
- Select the file "dcbweb/wbrowser.p12" from the USB drive.
- You will be prompted for the password used encrypt the
  certificate.  Enter the same password you used when you
  generated the certificates.

Server Certificate (Internet Explorer and Firefox 1 and 2)
- Select the "Web Sites" tab.
- Press the "Import" button.
- Select the file "dcbweb/wserver.pem" from the USB drive.
- After import, highlight the server's certificate.
- Press the "Edit" button.
- Select "Trust the authenticity of this certificate"
- Press "OK"

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

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

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

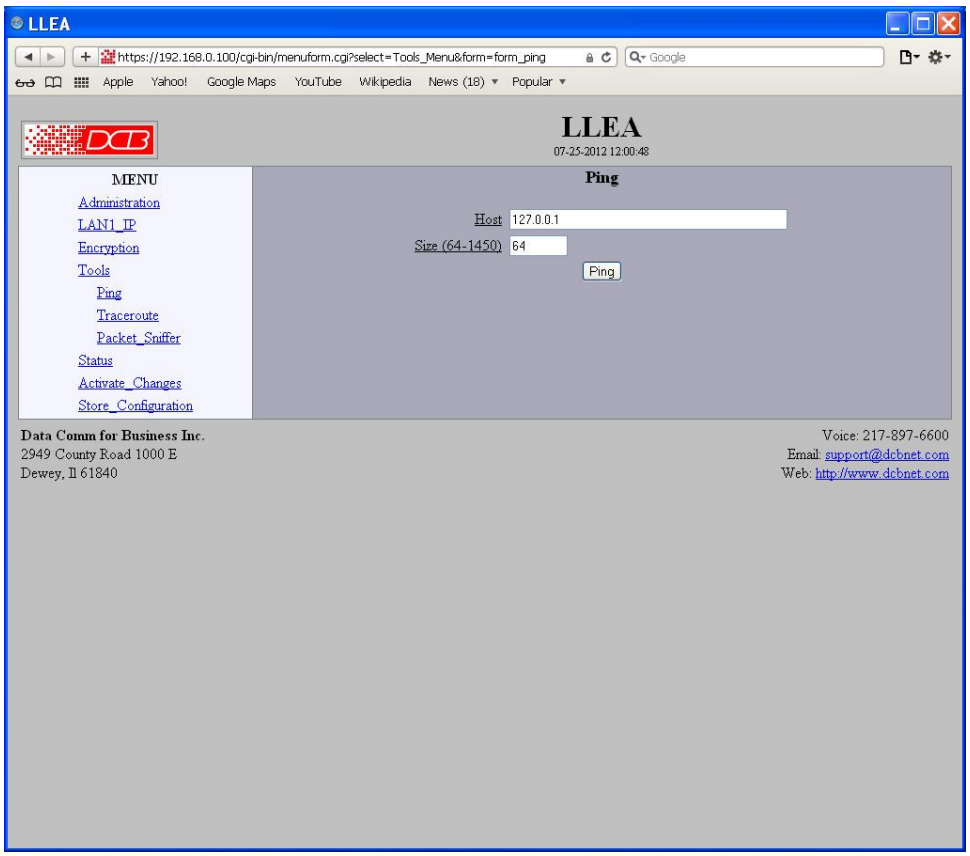
Fields

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

Notes

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

Ping Screen



Ping Screen

Ping will send four ICMP echo requests to the specified host. It will wait approximately 16 seconds for a response. This tool is useful for local network troubleshooting.

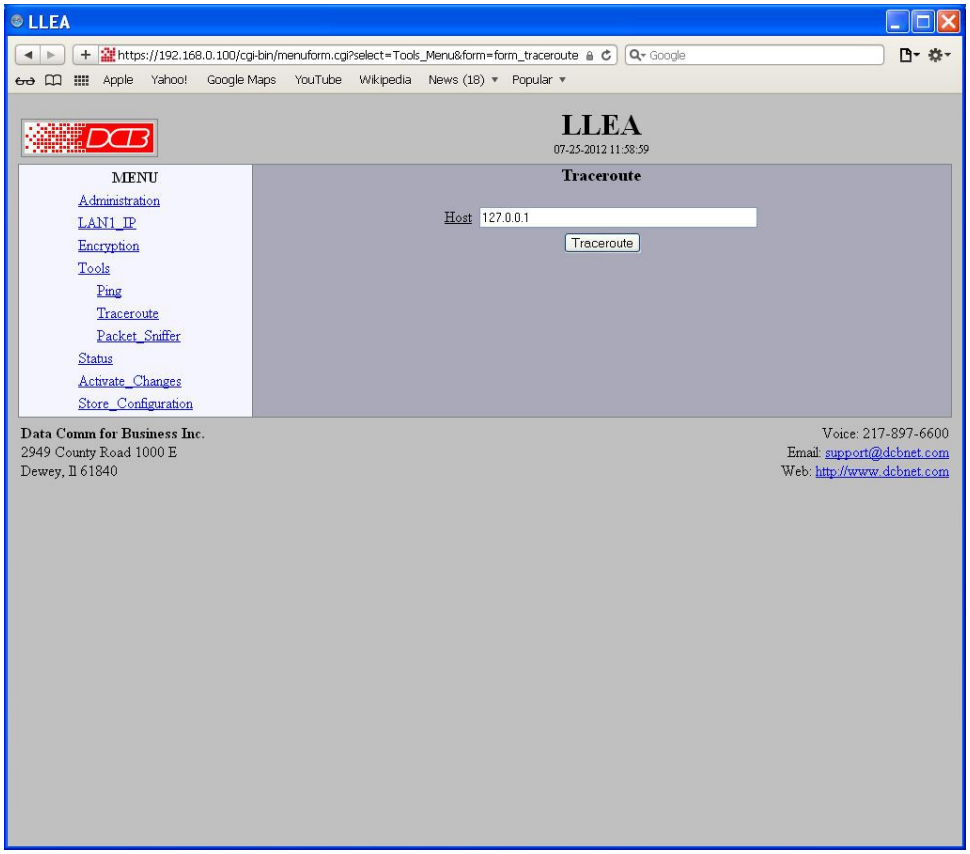
Fields

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

Notes

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

Traceroute Screen



Traceroute Screen

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

Fields

Host

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

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

Notes

Packet Sniffer Screen

Packet Sniffer Screen

The Packet Sniffer allows you to take a snapshot of the network traffic passing through an interface. It captures only the packet headers. No other packet data is retrieved.

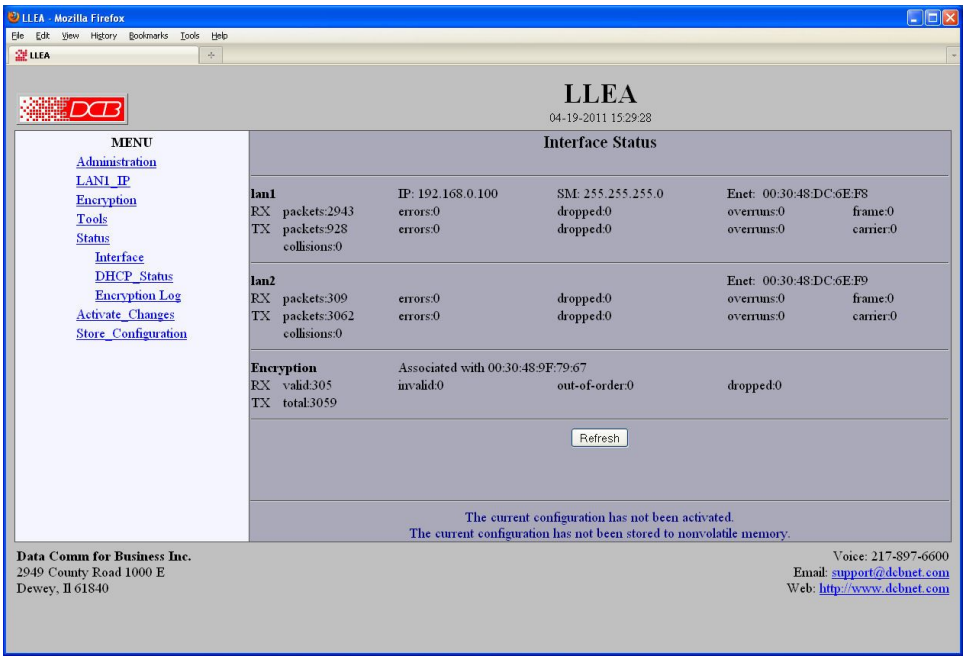
Fields

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

Notes

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

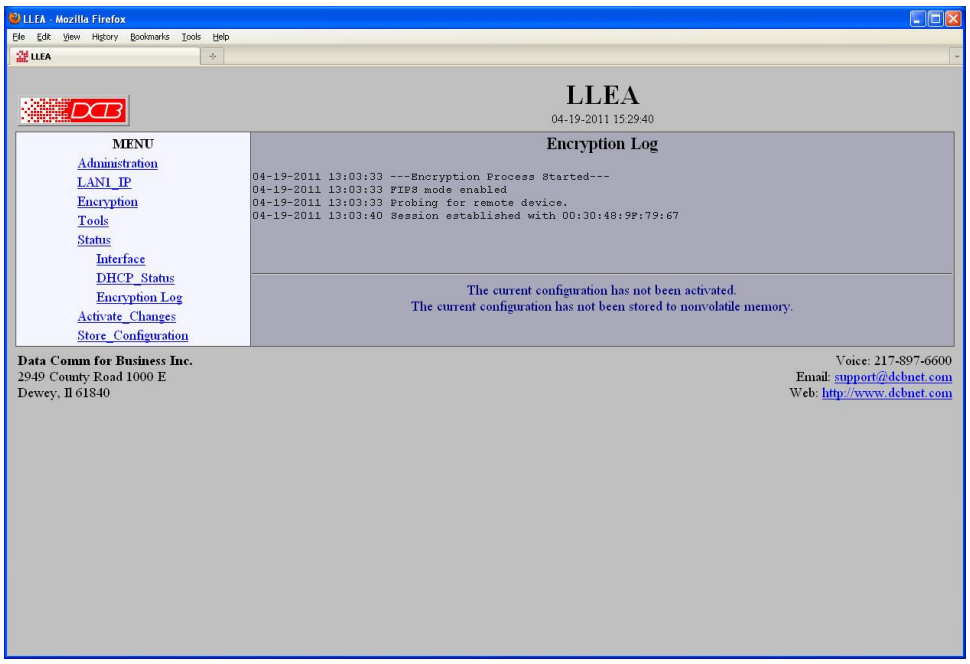
Interface Status Screen



Status Screen

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

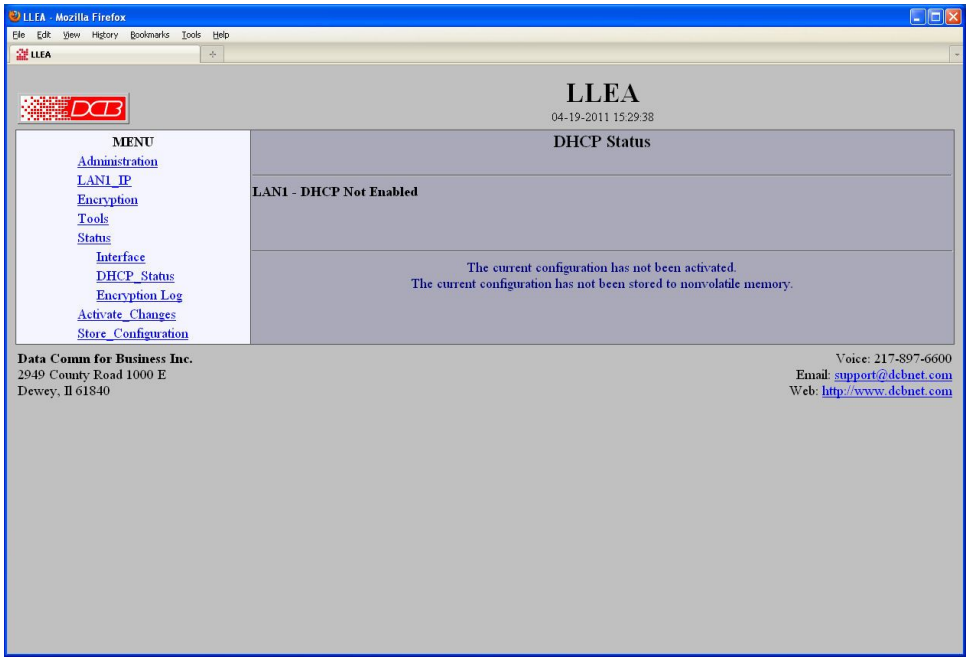
Encryption Log Screen



Encryption Log Screen

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

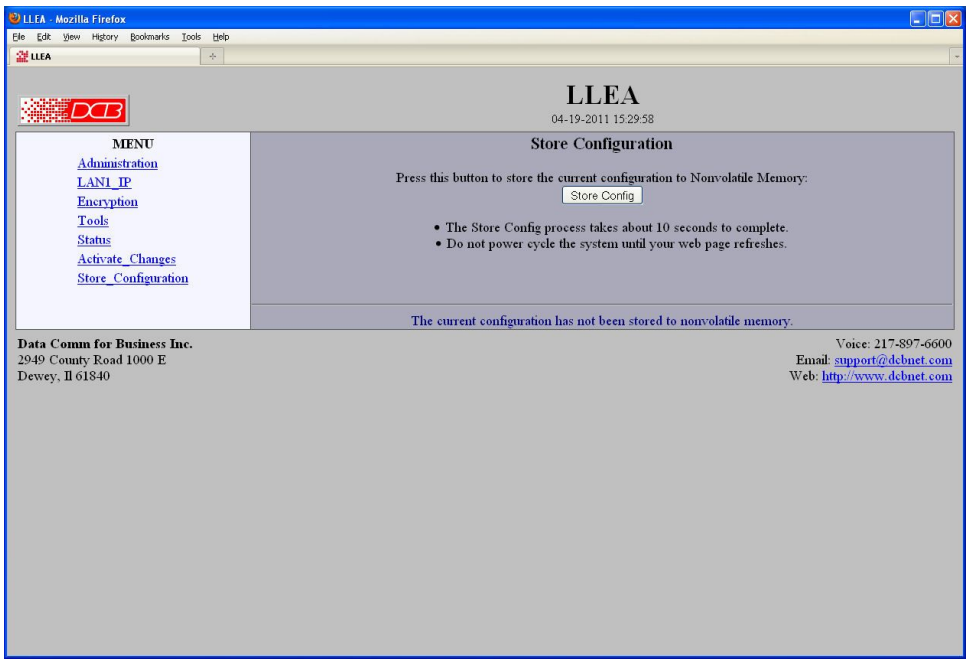
DHCP Status Screen



DHCP Status Screen

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

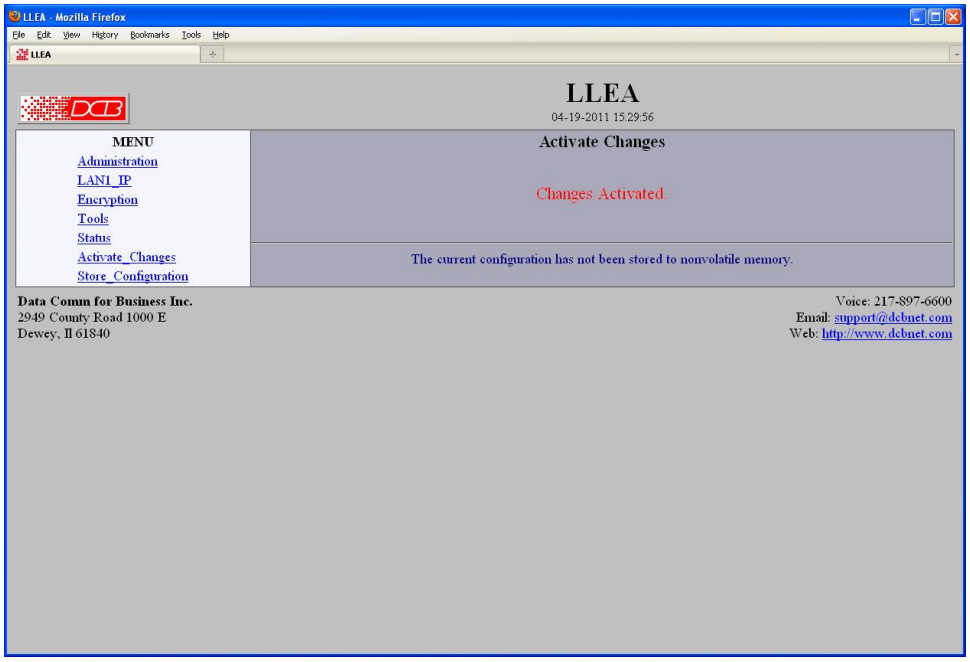
Store Configuration Screen



Store Configuration Screen

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

Activate Configuration Screen



Activate Configuration Screen

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

Chapter 5
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 LLEA still does not function properly, please contact your dealer for further advice. Our contact information is at the bottom right corner of all configuration screens.

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 LLEA is connected. If it is off, make sure the network cable between the encrypter 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 unit correctly ie. https:// instead of http:// for some models .
- Start troubleshooting from a known state. Power the unit and switches OFF and ON to reboot.
- Is a proper IP address configured in the unit and PC?
- "Ping" the unit 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 unit (e.g. `ping 192.168.0.100`). 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 encrypter have compatible IP addresses.**
- It may be that your "ARP table" contains invalid entries. You can clear the "ARP table" by rebooting, or, on Windows, by typing the following command at the command prompt or *Run* dialog box.: `ARP * -d` **. This is a common problem with test-bench setups.**
- Check that you are using the proper Ethernet connections. The leftmost port, LAN 1 is the local port, the rightmost port, LAN2 is connected only to the remote LLEA. Both ports should not be on the same lan segment for proper operation.
- 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 LLEA end of the cable to verify program operation and the proper COM: port.
- The most common problems causing this symptom are incorrect RS-232 wiring or the Windows Hyperterm program not operating correctly.

***P*:** How to set the unit back to factory defaults?
S: If you know the IP address, you may browse to the Administration screen – Set All Defaults. If the IP address is unknown, use the serial connection setup method (Chapter 2), and answer Yes when asked if you wish to reset the unit to factory defaults. The factory default IP adderss for the trusted side ethernet port (Port A) is 192.168.0.100 .

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

Checking Encrypter Operation

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

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

If any one PC on one side of the tunnel can communicate with any single PC or server on the other side of the link, then the en crypter 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 Layer 2 bridge, not a router. All IP addresses on the trusted side of ALL bridges in the system should be in the same IP subnet address range if there are no external routers.

Appendix A

Specifications

LLEA Link Layer Encrypter Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense X2
- USB Interface: USB for certificate transfer
- Serial Port (1) RS-232 port for initial IP address setup if needed
- OS: linux
- CPU: Quad Core 32 bit or higher performance processor
- Memory: 2Gig or more RAM
- Throughput: Greater than 900 Mbps with AES,
- Operates in pairs as a layer two bridge
- Power: 120 VAC ~260 watts
- LED: Over-temperature warning, LAN Activity, LAN status (two per interface), Power
- Default LAN 1 IP address: 192.168.0.100
- Default LAN 2 IP addresses: No IP address, used for layer two ethernet link to companion LLEA
- Browser Management port: 443 (HTTPS)
- Operational Temperature: Office environment
- Dimensions 1U high rack chassis

Cables

Commonly used cable connections:

Bridge to hub or ethernet switch

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

Bridge to PC crossover ethernet cable

A crossover cable may be constructed to allow the LLEA ethernet port to directly connect to a PC or equivalent without using a hub.

Use the following pinout to build an ethernet crossover cable:

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

Appendix B

Open Source Software Information

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

Introduction

Some models were designed and programmed with Open Source Linux software in mind. DCB supports the Open Source software effort and is appreciative of the contribution many open source developers have made to the community

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

Obtaining the Source Code

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

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