ESP

Electronic Security Perimeter Appliance

User's Guide

9/21/2015
Revised 3/16/2016

Firmware Version 1.0x

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.

Version 1.x

RoHS

Some models of this product is available in RoHS versions.

This product is available in RoHS versions.

Table of Contents

Chapter 1

Introduction

This chapter provides an overview of the Electronic Security Perimeter Appliance's features and capabilities.

Congratulations on the purchase of your new Electronic Security Perimeter Appliance (ESP). This is an add-in device used as a front end to legacy equipment requiring modern security features.

The ESP provides encryption, authentication, and audit trail logging to protect against electronic security intrusions, meets new NERC-CIP requirements, new corporate security standards, and HIPPA regulations, etc.

Interfaces include three RS-232 serial ports (two implemented via USB) and three 10/100BaseT Ethernet ports. This allows a "lump in the cord" installation for Ethernet as well as RS-232 serial connections. Logging and authentication are provided either locally within the unit or via remote RADIUS and rsyslog servers.

This new appliance allows utilities to meet NERC-CIP Electronic Security Perimeter requirements without costly equipment replacement.

ESP Applications

In an **ethernet protection application,** the ESP is installed between the local ethernet network (typically connected to Eth3) and the equipment to be protected (typically connected to Eth1). It's then configured as a transparent firewall containing black-hole features, as a RADIUS enabled front-end authentication box, or as a SSH front end to the protected equipment's telnet port. Authentication and logging may be local or remote.

For a **serial protection application**, the ESP is installed between the equipment to be protected and the incoming serial line. It provides logging, authentication, and serial "firewalling" to protect the RS-232 serial interface.

In both of those typical installations, the ESP uses a remote RADIUS server for centralized authentication or an optional local authentication database. In all installations, the ESP can be configured for remote syslog logging of an audit trail or maintenance of a temporary local log.

The ESP can also be configured to allow **SSH access to the legacy equipment's serial interface via ethernet**. In many cases, this option will allow the removal of vulnerable telephone modem lines since more secure ethernet is often being installed in CIPS locations.

Features

Protocols

The ESP may be configured to handle any valid ethernet protocol.

Authentication Rules

User authentication is performed against either local user credentials, a remote Radius server, or some combination of the two based upon availability and timeout.

Extensive Filtering Rules

In addition to protocol filtering, the ESP will filter and log activity with user defined rules restricting source IP, protocol, destination IP, destination port, source IP, source port, ethernet frame type, ethernet protocol, source and destination MAC,

Upgradeable Firmware

Firmware upgrades may be installed using any web browser. Web access may be protected using certificates.

Serial Device Features

The connection to a serial device is either as a “lump in the cord” serial firewall or as a SSH to serial converter. The serial port allows various RS-232 control signals.

On-board Tools

Diagnostic tools such as extensive logging, traceroute, ping, and a simple packet sniffer are available to aid in network troubleshooting.

Audit Ports Feature

The ESP contains extensive reporting of IP connections and connection states.

Package Contents

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

- The ESP appliance
- Power Adapter
- This User’s Guide CDROM
- PC 9 pin DE-9 null modem connection cable

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

Software Requirements

No specific software is required for with the ESP other than a web browser using during configuration.

It supports IP and associated protocols such as UDP, ICMP, serial PPP, DHCP, SIP, multi-cast, and any protocol built upon IP**. It is configurable to pass (or block) any valid Ethernet protocol**. The initial IP address may be entered using any terminal or terminal emulation software on a PC, or the default may be used if appropriate for your network.

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

ESP Hardware

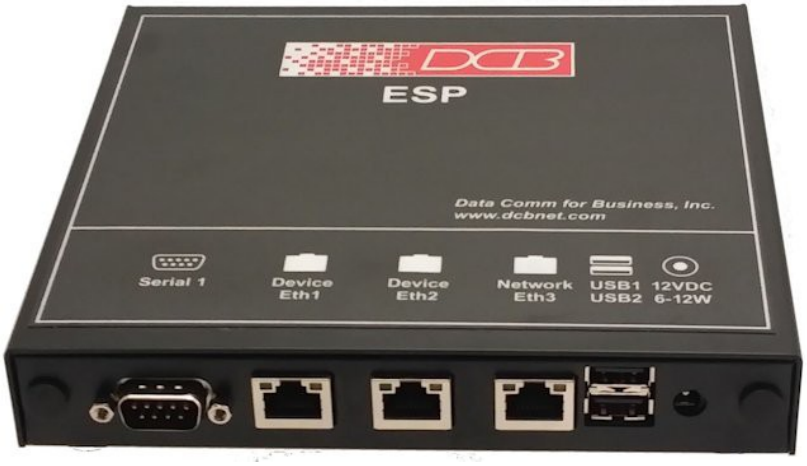
Introduction

The ESP bridge contains three gigabit ethernet ports and is often used with one port facing the local network and two ports facing the equipment to be protected. There are three serial ports, one implemented as RS-232 with a DE-9 interface and two implemented using USB interfaces.

The USB interfaces may use USB-to-RS-232 conversion cables. The serial ports may be connected directly to the equipment being protected or to incoming serial data sources. If needed, one serial interface that may be used in initial IP address configuration.

Configuration

If the default IP address is not appropriate for your LAN, connect a terminal to the serial port following the instructions in the configuration section of this manual. 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 administration and configuration of the tunnel.



ESP Hardware

LED Indicators

One set of indicators for each Ethernet Port

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

RS-232 Port

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

USB Ports

The two USB ports may be used as serial ports connecting to either the protected equipment or incoming lines. DCB USB to RS-232 conversion cables are available.

Chapter 2

Installation

This Chapter details the installation process for the ESP.

Overview

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

Quick Start

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

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 ESP's IP address

If the ESP’s default address (192.168.0.1) is appropriate for your network, skip to step 2, “Connect the Ethernet Cable”.   If thie address isn't appropriate, it may be more convenient to temporarily configure a PC to 192.168..x and skip to step 2 below.

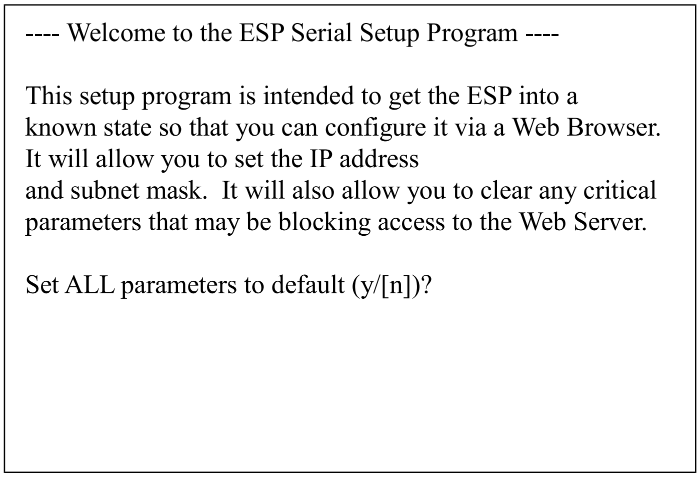
1. Connect a terminal or PC running terminal emulation program (Hyperterm, Procomm, etc) to the serial port.
2. Start the terminal emulation program using 9600 bps, 8-bits, No parity, No flow control.
3. Power up the ESP.

```
Welcome to the  ESP V 1.0
To start the Serial Setup Program, login with
the name: setup
ESP login:
```

Log in Screen

4. TheESP will reboot pausing at a log in screen. **For initial setup, enter the log in 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".



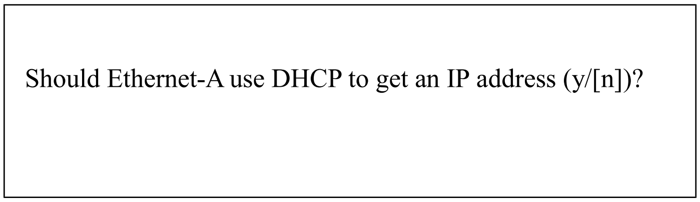
```
---- Welcome to the ESP Serial Setup Program ----

This setup program is intended to get the ESP into a
known state so that you can configure it via a Web Browser.
It will allow you to set the IP address
and subnet mask.  It will also allow you to clear any critical
parameters that may be blocking access to the Web Server.

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

Default Screen

6.You are then asked if you wish to use a DHCP client. If you want the ESP to pick up a DHCP address from a local DHCP server connected to LAN-1, answer "y", otherwise answer "n". DHCP is not recommended.



```
Should Ethernet-A 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 and subnet mask. Enter the values for the LAN-1 interface.

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

```
Saving Configuration. Do not cycle power...
Erasing flash sector 0x10fc0000
Storing file [config.tar.gz], size 1541 bytes
Store complete
Setup complete.
After rebooting the system, you will be able to configure
the unit from a Web Browser.  Use the URL
http://11.22.33.44 .


press <enter> to reboot system...
```

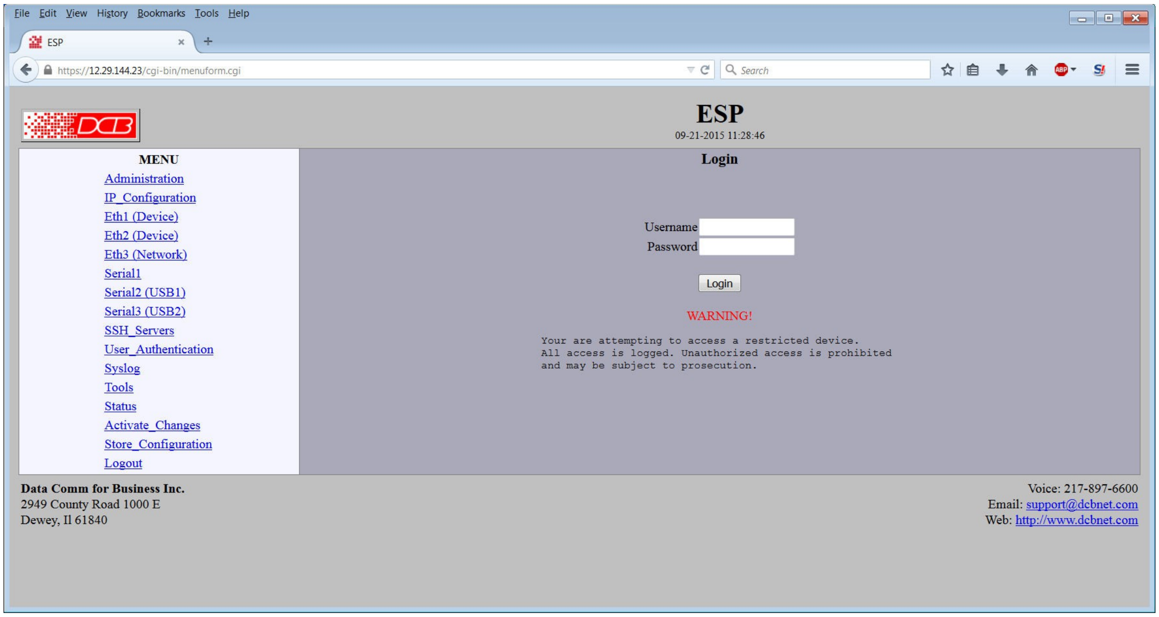
9. The bridge will now reboot.

2. Connect the Ethernet Cable

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

3. Verify the IP Address Configuration

Enter the URL from step 1 (or https://192.168.0.1 if using the default address) into your web browser. Note that it uses HTTPS: and not HTTP: . The login screen below should be displayed.



ESP

09-21-2015 11:28:46

Login

Username

Password

WARNING!

```
Your are attempting to access a restricted device.
All access is logged. Unauthorized access is prohibited
and may be subject to prosecution.
```

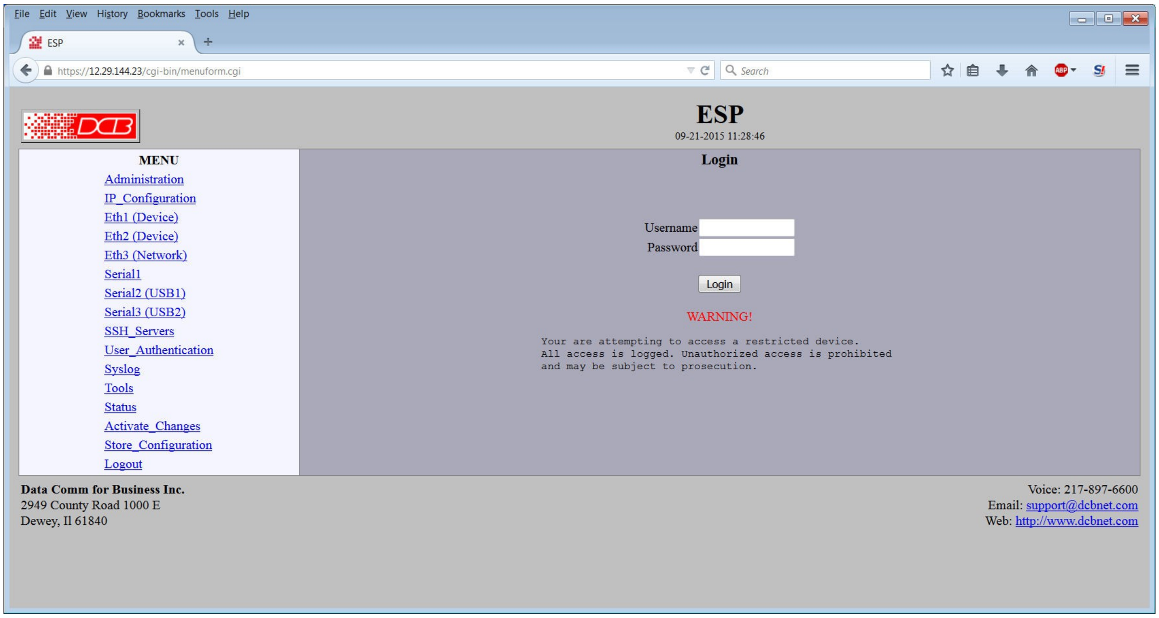
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Login Screen

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

4. Enter Configuration Values



ESP

09-21-2015 11:28:46

WARNING!

```
Your are attempting to access a restricted device.
All access is logged. Unauthorized access is prohibited
and may be subject to prosecution.
```

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Initial Main Menu

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

5. Minimum Configuration

The minimum configuration items required for basic operation are determined by your application. There are several quick-start examples detailing the most commonly used topologies.

Chapter 3

The Configuration Process

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

Overview

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

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 ESP 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 form memory when the ESP was last booted WITH any changes made by using the configuration screens. This configuration is NOT the configuration running the hardware at present.
3. The ***stored*** configuration. This is the configuration that was last written to non-volatile RAM. The next time the ESP restarts, it will start running this configuration.

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

Using the Configuration Flexibility

When the ESP 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 or the *stored* 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 ESP 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 ESP. However, upon the next reset or power cycle, the ESP will begin using the stored configuration.

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

Configuration Process Examples

Example 1:

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

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

Example 2:.

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

This method allows one to configure the ESP on a network 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 ESP is reset, it will begin using the new configuration. This method is useful when you are configuring an ESP to use a new LAN address range while it is on the old LAN.

Example 3:

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

It is useful to transfer an existing ESP 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 ESP (192.168.0.x subnet), then a new, out-of-the-box ESP is easily configured using this method. Start the ESP, transfer a stored configuration file, and store it. When the hardware is restarted, it will have the proper configuration. This process uses the Administration **Config File** screen.

Saved Configuration Files

The saved configuration file is a simply formatted encrypted text file.

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

Chapter 4

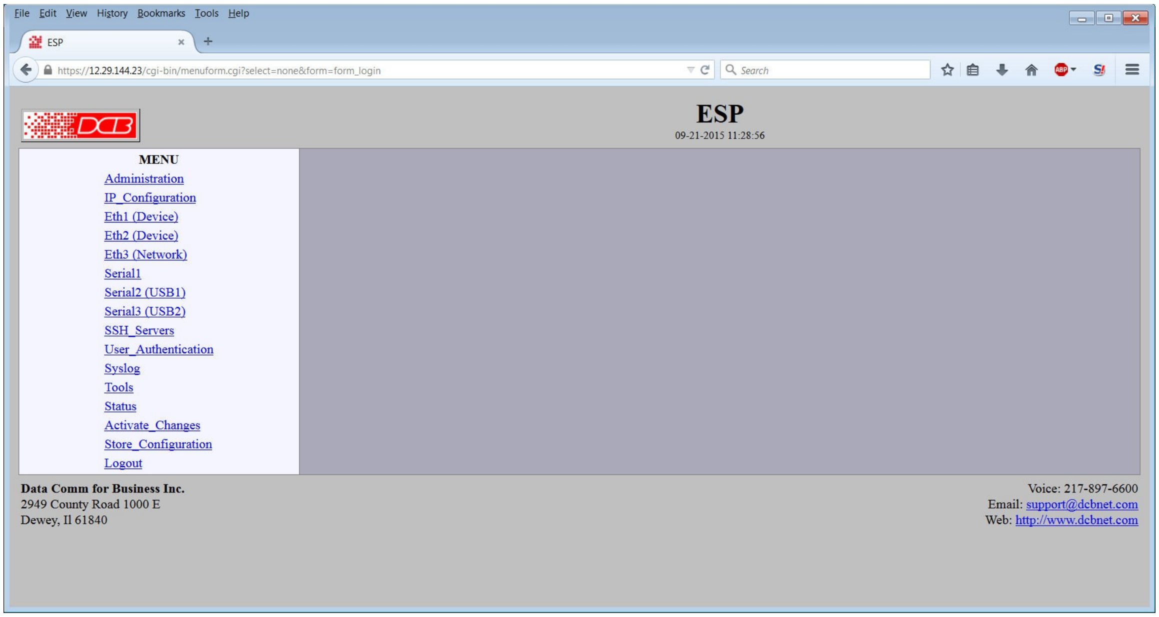
Configuration

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

The ESP 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, security, or routing. Familiarity with IP and related information is required before you can configure any ethernet product.

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

Configuration screens are available to all valid IP addresses unless “Web Firewall Rules” have been activated. This default operation may be changed during configuration, but it is highly recommended that configuration be locked to only appropriate workstations.



ESP

09-21-2015 11:28:56

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

ESP Main Screen

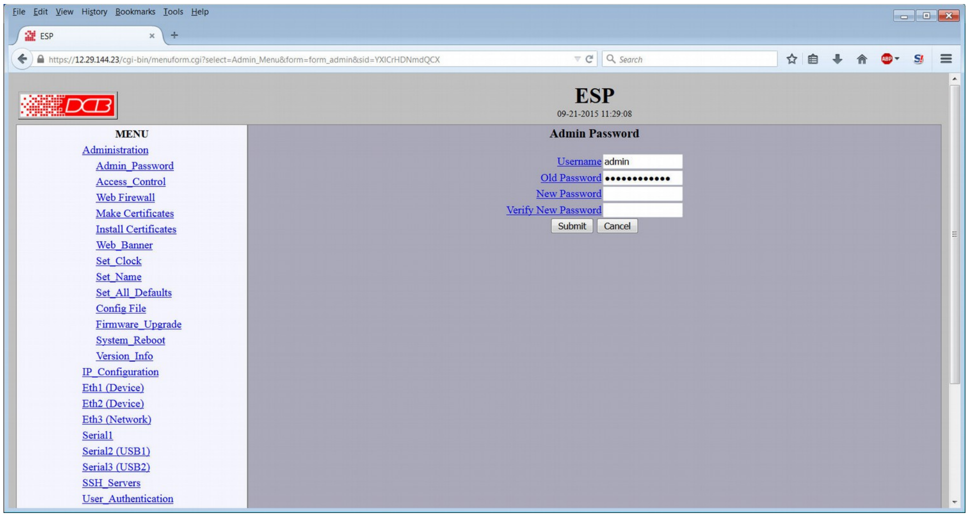
From this index, click on a menu keyword to open the appropriate screen. In this manual, screens are discussed in the order shown on the index screen.

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



ESP

09-21-2015 11:29:08

Admin Password

Username admin
Old Password ••••••••••••
New Password
Verify New Password

Admin Password Screen

Access to the ESP's configuration web server is protected by HTTP Basic Authentication and uses the secure web server HTTPS. 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. Advanced users may wish to use the x509 certificate requirement method as well to lock down the configuration capability even tighter. That method is detailed elsewhere. In addition, requiring Radius authentication may also be configured under the Access Control screen.

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

Fields

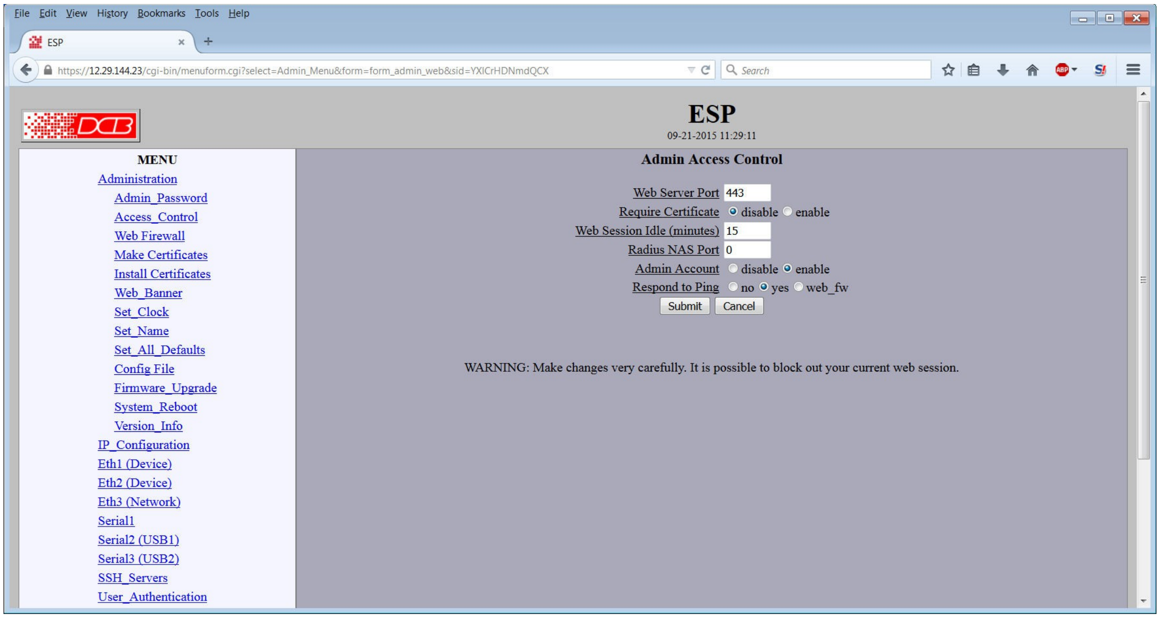
- User Name
  This field may be a string of 0 to 15 printable characters. Do not use space or control characters. If you leave this field blank, you will need to enter a blank username during authentication. **This field should not be blank.**
- Old Password
  In order to change the username and password,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

Admin Access Control



ESP
09-21-2015 11:29:11

Admin Access Control

Web Server Port 443
Require Certificate ● disable ○ enable
Web Session Idle (minutes) 15
Radius NAS Port 0
Admin Account ○ disable ● enable
Respond to Ping ○ no ● yes ○ web_fw

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 UT's internal configuration web server.

Fields

- Web Server Port
  This is the TCP Port to use for the internal Secure 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 UT's web interface and attempt to break in. A different port may be needed to accommodate other local firewalling.

  If you change the web server port number to any value other that 443, remember that you will have to include the port number in your URL. For example, https://192.168.0.1:7995 .
- Require Certificate
  This option allows selection between two different methods of authenticating web access. HTTPS Basic is the method built into web servers and web browsers. A user name and password is required to

access each web page. Once the user has entered the credentials into the web browser, the web browser will cache the information and automatically provide them to the web server during that session. A disadvantage of HTTP Basic Authentication is that it has no mechanism to re-authenticate a user after a period of time. This creates a security risk if the user fails to close their web browser. Enabling tThis option enables certificate based authentication of web browsers attempting to connect to the ESP's internal web server. The browser must present the appropriate certificate, otherwise access will be denied. See the section on making and installing certificates if you wish to use the certificate method.

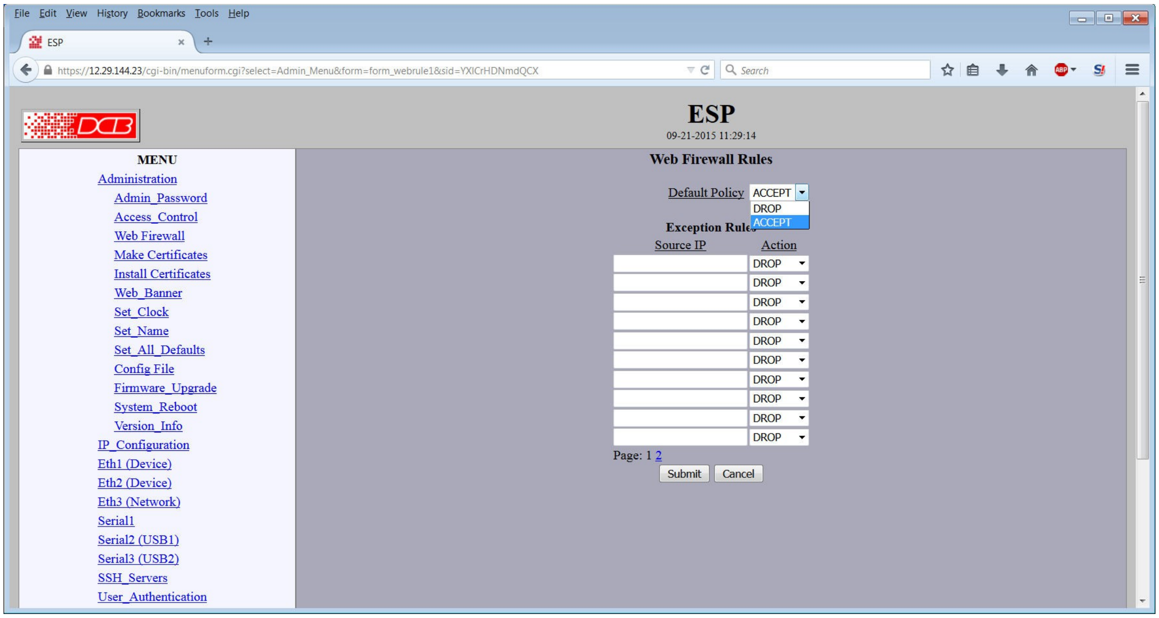
- Web Session Idle Timeout
  Once a web session has been idle for the configured time-out period, the user will need to re-authenticate with the web server. The time is specified in minutes and may range from 5 minutes to 120 minutes. There is no option to disable the timer.
- Radius NAS Port
  A Radius NAS Port is an identifier used by a radius server to identify a resource. In this instance, it is the identifier for the ESP's web server. So, for example if the Radius NAS Port is set to 100 and user Bob attempts to log into the ESP's web server, a request will be set to the Radius server asking if user Bob has permission to access NAS Port 100.
- Admin Account
  This options enables/disables the special Admin User Account. When disabled, any administrative access to the ESP's web interface must be authenticated through a radius server or the local user database.

  Before enabling this option, please thoroughly test your configuration to insure you can still manage the ESP. If locked out, the only recourse is to reset the ESP to defaults.
- Respond to Ping
  This item allows you to block ping requests to the ESP. Ping is a valuable tool for diagnosing network problems, but can also become a security problem. Disabling ping causes the ESP to not respond to ping requests. It has no effect on the passing of ping request and responses from other network nodes.

Notes

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

Web Firewall



ESP

09-21-2015 11:29:14

Web Firewall Rules

Default Policy: ACCEPT (options: DROP, ACCEPT)

Exception Rules

Source IP	Action
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP

Web Firewall Screen

The Web Firewall allows you to control which hosts or networks have access to the ESP's web server. As HTTPS request packets are received, each packet is compared against the Web Firewall rules, and the specified action taken if the rule matches.

Entries are made by specifying a Source IP and optional mask. For example, if you want to allow the host 192.168.10.16 access, you would enter:

```
Source IP: 192.168.10.16     Action: ALLOW
```

If you wanted to allow access to all hosts in the subnet 192.168.10.0 to 192.168.10.255, you would enter:

```
Source IP: 192.168.10.0/24   Action: ALLOW
```

The firewall rules are applied in the order displayed. This feature can be used to build more complex rules. For example, if you wanted to allow access to all hosts in a subnet, except for host .13, you could order two rules as follows:

```
Source IP: 192.168.10.13     Action: DROP
Source IP: 192.168.10.0/24   Action: ALLOW
```

Fields

- Default Policy The *Default Policy* configures the action to take if the incoming packets doesn't match any of the exception rules. The two actions are to *ACCEPT* the packet, or *DROP* the packet.
- Source IP This field specifies the Source IP address and optional subnet mask. It is specified as an *address/mask* where the */mask* part is optional and may be in the dotted format or bit count format. For example:

```
192.168.0.1
192.168.0.0/255.255.255.0
192.168.0.0/24
```

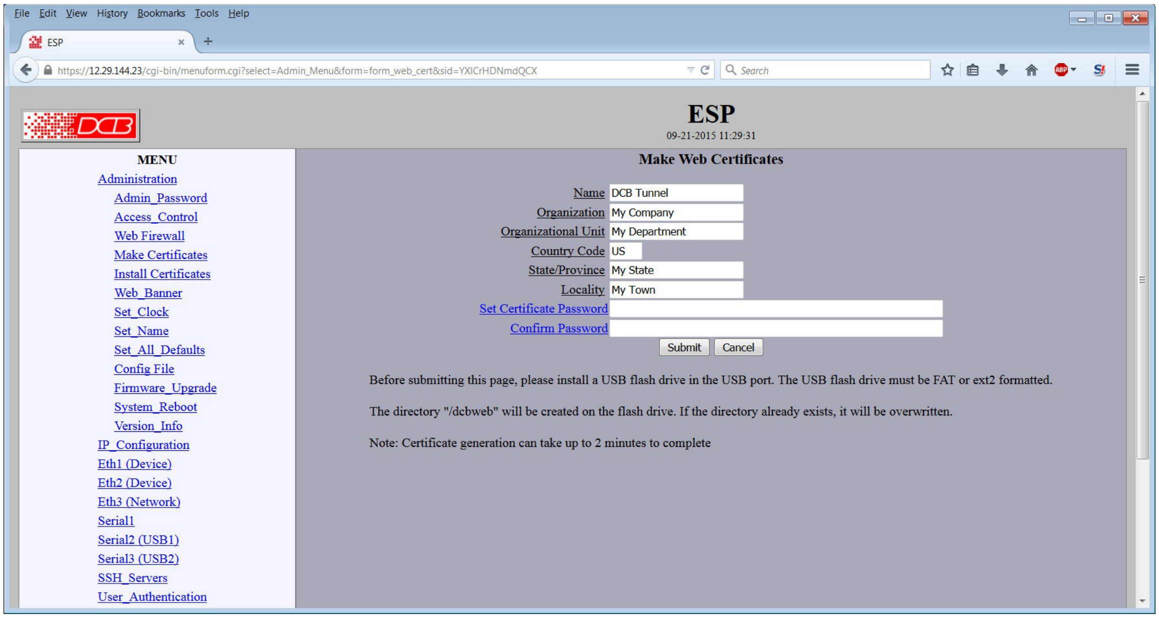
If the Source IP field is blank, the action is ignored.

- Action This field selects the action to take if an incoming packet matches the given Source IP address. The two actions are to *ACCEPT* the packet, or *DROP* the packet.

Notes

It is good practice to test your configuration before permanently storing it.

Make Certificates



ESP

09-21-2015 11:29:31

Make Web Certificates

Name DCB Tunnel

Organization My Company

Organizational Unit My Department

Country Code US

State/Province My State

Locality My Town

Set Certificate Password

Confirm 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 "/dcbweb" will be created on the flash drive. If the directory already exists, it will be overwritten.

Note: Certificate generation can take up to 2 minutes to complete

Make Certificates Screen

The ESP's 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 your ESP'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 ESP's USB ports. Separate steps are required to install the certificates into the ESP's web server and your computer's web browser. For more information, see *Installing Web Certificates*

Four files 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
```

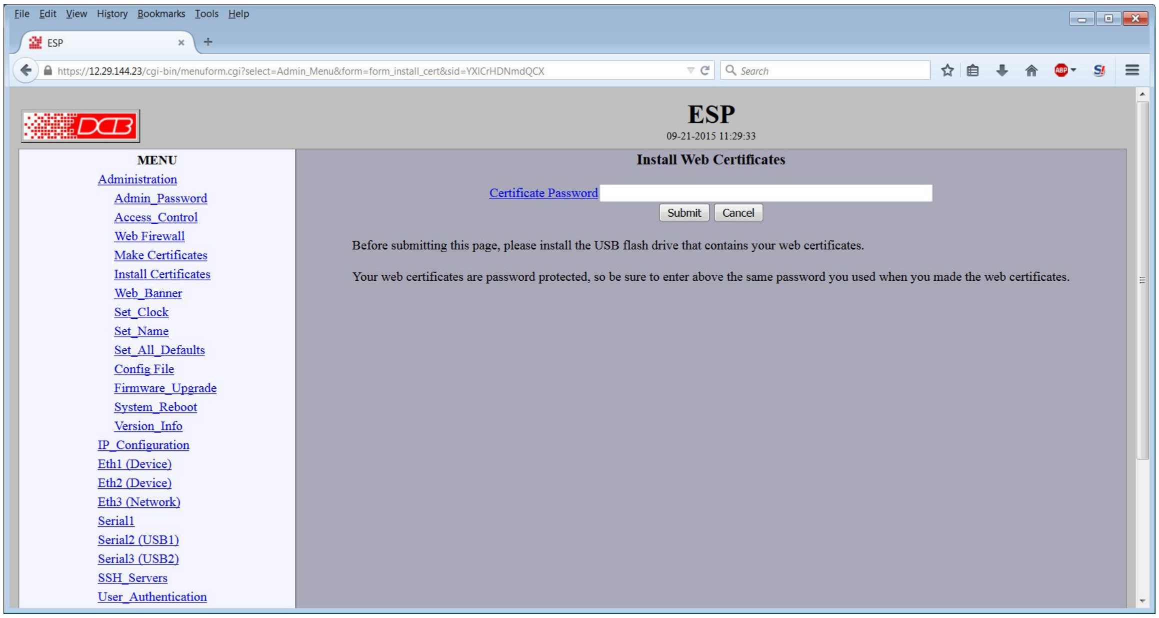
Fields

- 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/ProvinceThe 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.
- Confirm Password Re-enter the password for confirmation.

Notes

Install Certificates



ESP

09-21-2015 11:29:33

Install Web Certificates

Certificate Password

Before submitting this page, please install the USB flash drive that contains your web certificates.

Your web certificates are password protected, so be sure to enter above the same password you used when you made the web certificates.

Install Certificates Screen

This form will allow you to install two x509 certificates into the ESP'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 one of the ESP's USB ports. 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 ESP's web server will refuse to communicate with your web browser. You will need to import the certificate files from the USB Flash Drive into your web browser. The actual method depends upon your browser and version, but the method for Internet Explorer and Firefox is described below.

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

```
- Click on the "View Certificates" button.

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

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

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

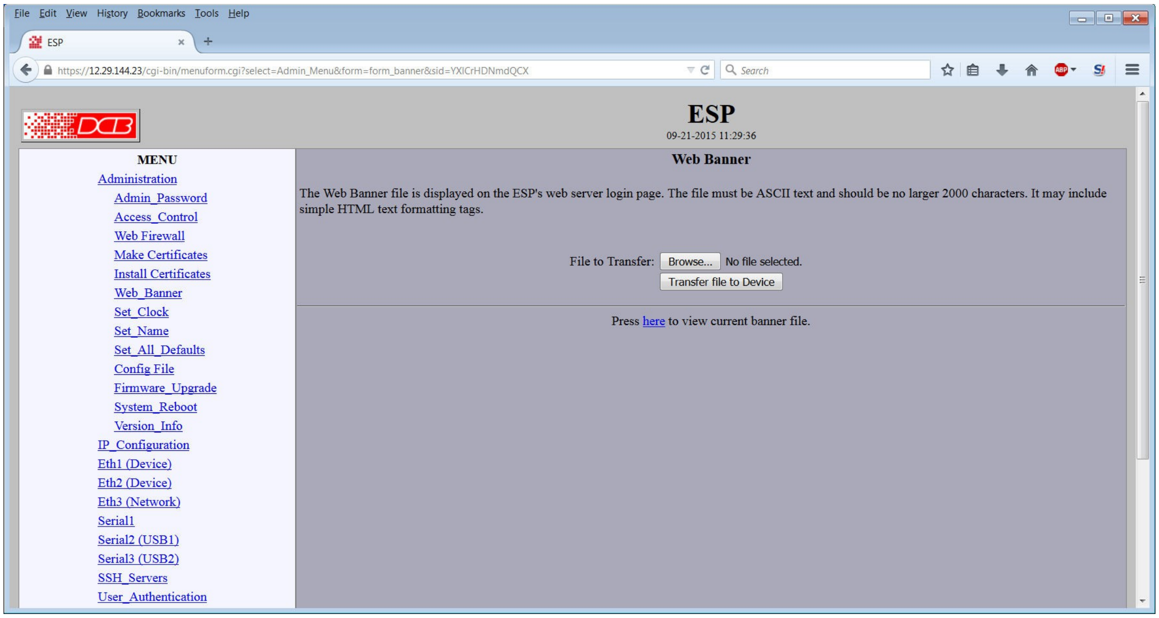
- Certificate Password The password to use to decrypt the private key stored in the certificate files. This must be the same password used when the certificates files were generated.

Notes

- Before submitting this page, please install the USB flash drive that contains your web certificates.

  Web certificates are password protected, so be sure to enter above the same password you used when creating the web certificates.

Web Banner



ESP

09-21-2015 11:29:36

Web Banner

The Web Banner file is displayed on the ESP's web server login page. The file must be ASCII text and should be no larger 2000 characters. It may include simple HTML text formatting tags.

File to Transfer: Browse... No file selected.

Press here to view current banner file.

Web Banner Screen

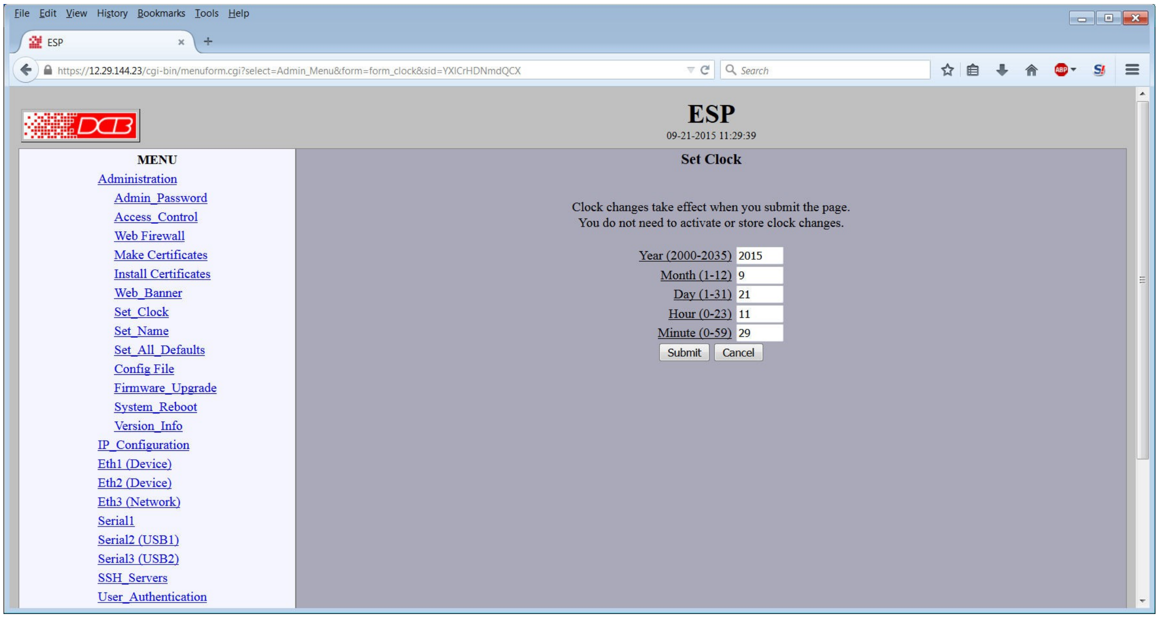
This form allows you to set the upload a custom banner screen. The Web Banner file is displayed on the ESP's web server login page. The file must be ASCII text and should be no larger 2000 characters. It may include simple HTML text formatting tags.

Fields

- File to Transfer Browse   Browse your local workstation for a file to transfer.
- Transfer file to Device   Click this button to actually upload the selected file.
- Press Here to view the current banner file Click "here" to display the current ESP banner.

Notes

Set Clock



ESP

09-21-2015 11:29:39

Set Clock

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

Year (2000-2035)	2015
Month (1-12)	9
Day (1-31)	21
Hour (0-23)	11
Minute (0-59)	29

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. Note: The clock can be automatically updated using NTP, found on the **tools/NTP page**. Also, the NTP timezone configuration will apply to the clock even if NTP is disabled.

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.

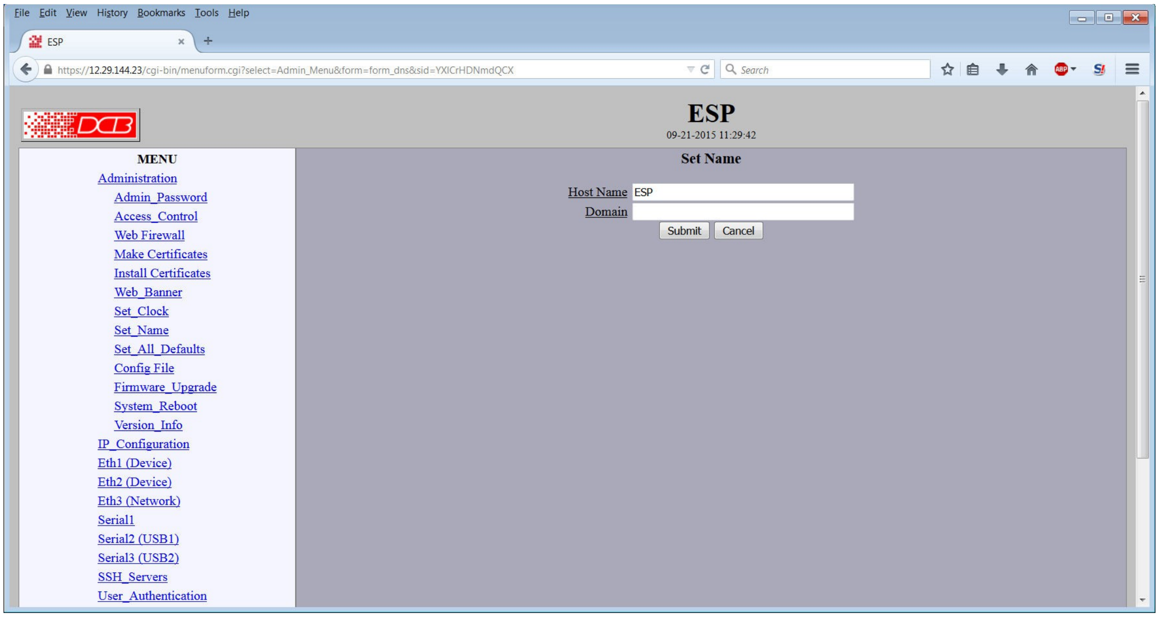
Hour   Hour of the day in the range 0 to 23.

Minute Minutes in the range 0 to 59.

Notes

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

Set Name



ESP

09-21-2015 11:29:42

Set Name

Host Name: ESP

Domain:

Set Name Screen

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

Fields

Host Name

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

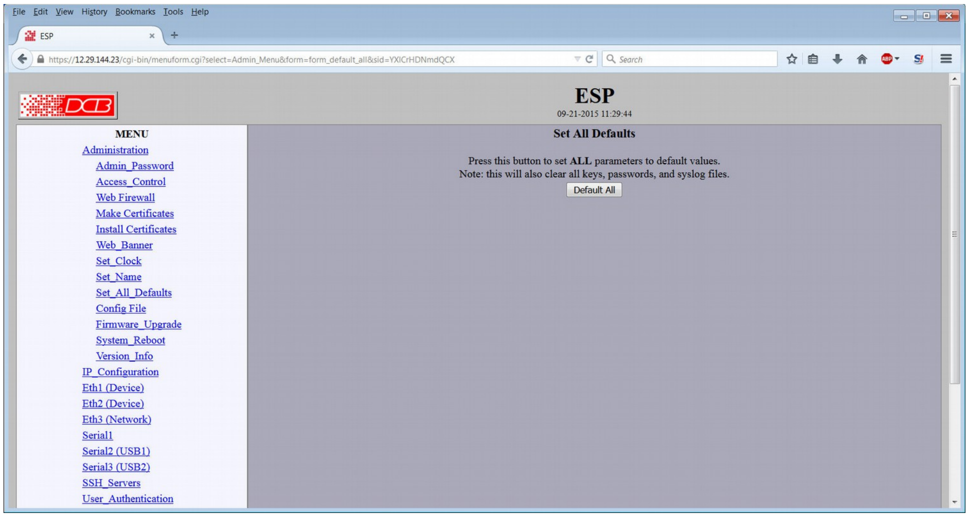
Domain

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

Notes

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

Set All Defaults



ESP

09-21-2015 11:29:44

Set All Defaults

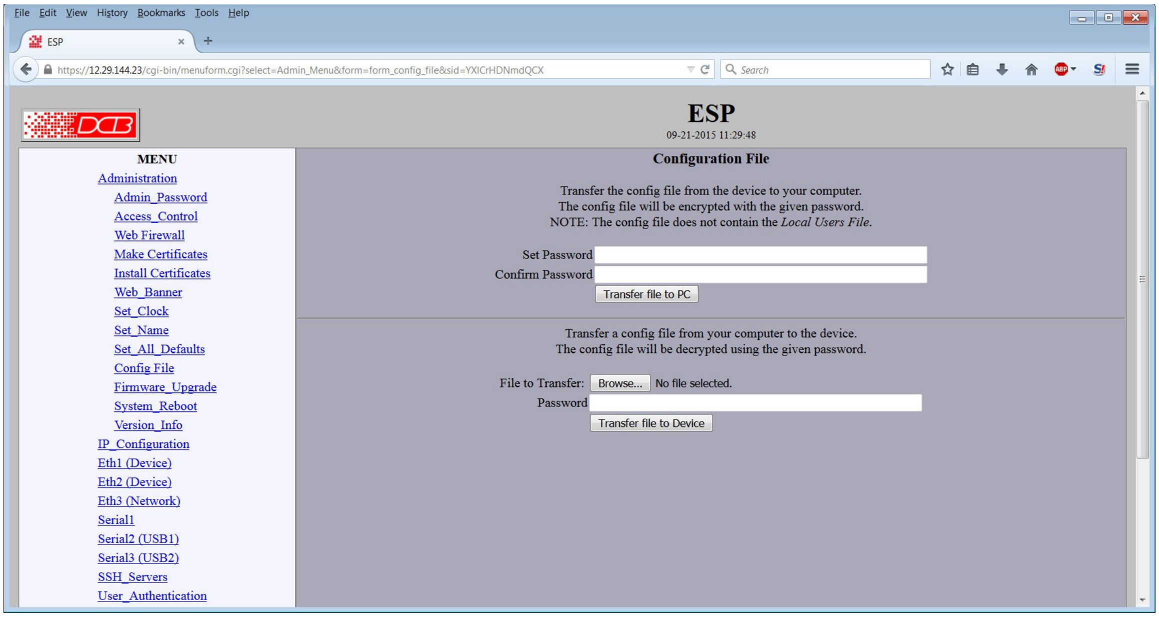
Press this button to set **ALL** parameters to default values.
Note: this will also clear all keys, passwords, and syslog files.

Set All Defaults Screen

Clicking on this button will set ALL configuration values back to factory default values. Note that this clears ALL keys, passwords, and syslog files.

Clicking this button will require you to completely reconfigure the ESP!

Configuration File



ESP

09-21-2015 11:29:48

Configuration File

Transfer the config file from the device to your computer.
The config file will be encrypted with the given password.
NOTE: The config file does not contain the *Local Users File*.

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 ESP configuration to a file on your PC. You can also use the form to transfer a configuration file from your PC to the bridge.

Fields

Transfer a Configuration file to the PC

- Set Password. The configuration file you save will be encrypted on the PC. **This password will be required to retrieve the file later.**
- Confirm Password Verify the password entered above.
- Transfer File to PC (action) Click this button to copy the configuration file to an encrypted file on the PC.

Retrieve a configuration file from the PC

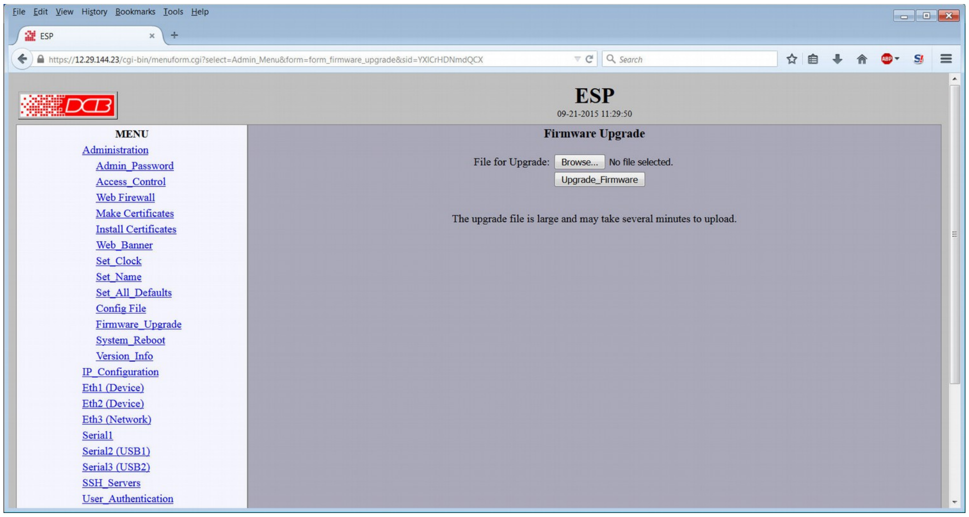
Transfers the current bridge configuration file to this PC.

- File to Transfer The Click the Browse button to select a file to be transferred.
- Password the password used to encrypt the file when it was saved.
- Transfer File to Device (action) Click this button to copy the configuration file into the pending configuration of the ESB.

Notes

- The configuration file is an encrypted, specially formatted binary file.
- You may save multiple configuration files on the PC by using different names for them.
- After transferring a configuration file to the ESP, 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 ESP will immediately begin using the new configuration. If the changes are stored, the ESP 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 ESP using its new configuration. Otherwise, it may be necessary to return to the old stored configuration with a reset.

Firmware Upgrade



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 ESP. The firmware will be saved to non-volatile memory, replacing the current firmware.

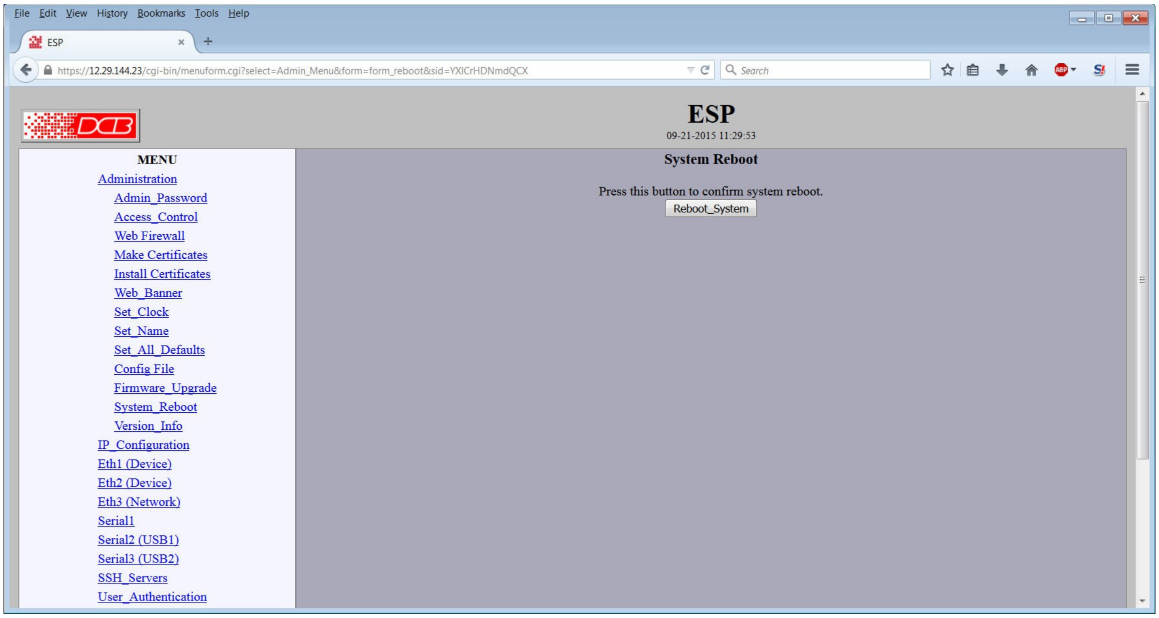
Fields

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



ESP

09-21-2015 11:29:53

System Reboot

Press this button to confirm system reboot.

System Reboot Screen

This form will allow you to reboot the ESP. If you have configuration changes that have not been saved to non-volatile memory, they will be lost. This is a way to revert back to your previously stored configuration.

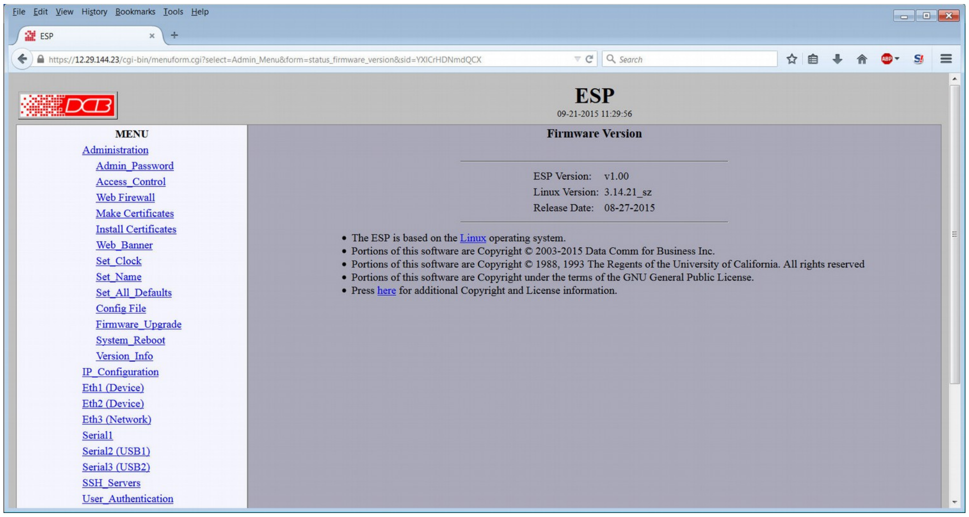
Fields

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

Notes

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

Version Information Screen



ESP

09-21-2015 11:29:56

Firmware Version

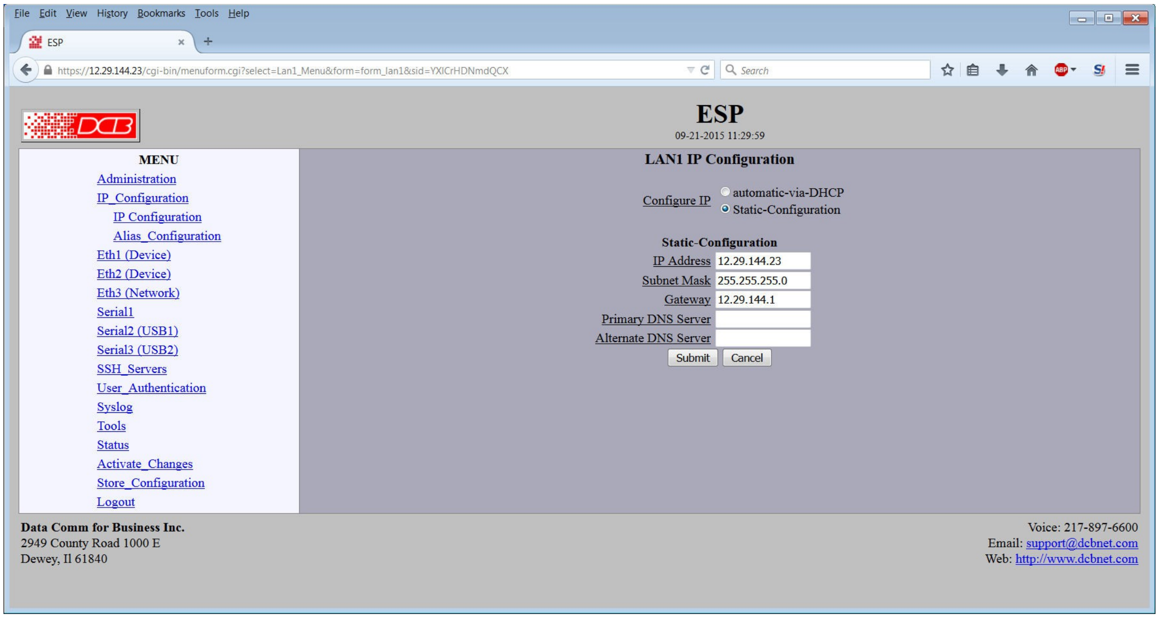
ESP Version: v1.00
Linux Version: 3.14.21_sz
Release Date: 08-27-2015

- The ESP is based on the Linux operating system.
- Portions of this software are Copyright © 2003-2015 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.
- 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.

IP Configuration



https://12.29.144.23/cgi-bin/menuform.cgi?select=Lan1_Menu&form=form_lan1&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:29:59

LAN1 IP Configuration

Configure IP ○ automatic-via-DHCP ● Static-Configuration

Static-Configuration

IP Address	12.29.144.23
Subnet Mask	255.255.255.0
Gateway	12.29.144.1
Primary DNS Server	
Alternate DNS Server	

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

IP Configuration Screen

This screen configures the IP address used to communicate with the ESP itself.

Fields

- Configure IP (Automatic via DHCP or Static-Configuration)
  The interface can be configured automatically using DHCP or statically. If you choose to use DCHP, there must be a DHCP server running on the network segment and you need to know what IP address will be assigned in order to communicate with the ESP.
- IP Addresses 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.

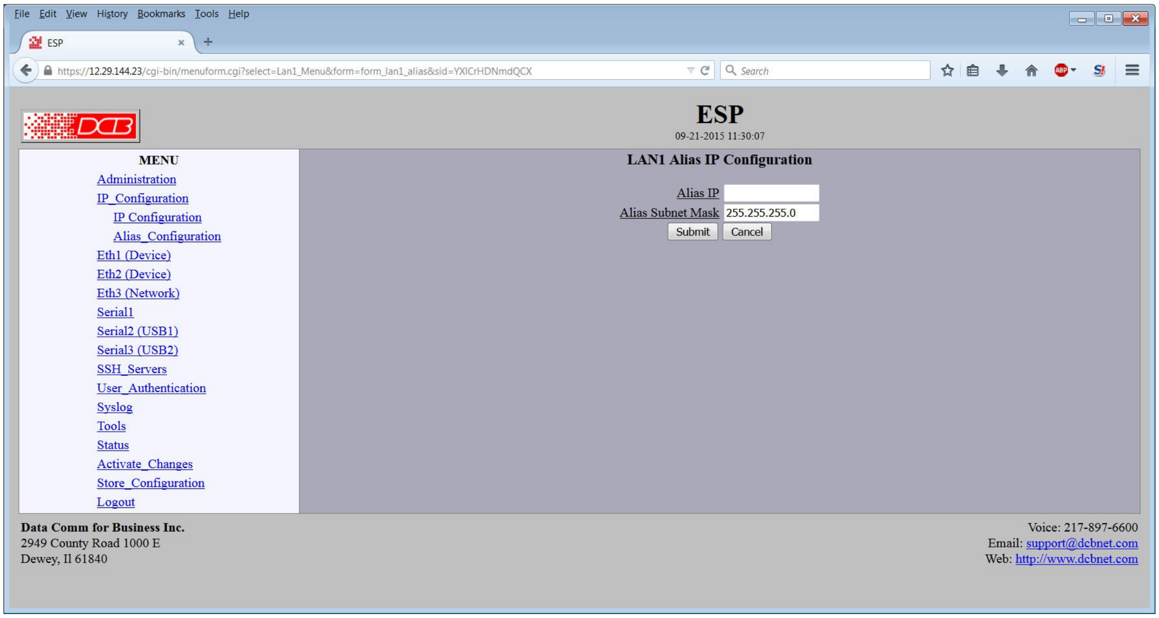
  This field is not used if configuring automatic-via-DHCP. The IP address will be assigned by the DHCP server.
- Subnet Mask A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, 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 configuring automatic-via-DHCP. 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.
- Primary DNS Server The IP address of the primary DNS server. Setting the DNS server is optional and only necessary when using hostnames.

- Secondary DNS Server The IP address of the secondary DNS server. Setting the DNS server is optional and only necessary when using hostnames.

Notes:

Alias Configuration



https://12.29.144.23/cgi-bin/menuform.cgi?select=Lan1_Menu&form=form_lan1_alias&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:30:07

LAN1 Alias IP Configuration

Alias IP

Alias Subnet Mask 255.255.255.0

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Alias Configuration Screen

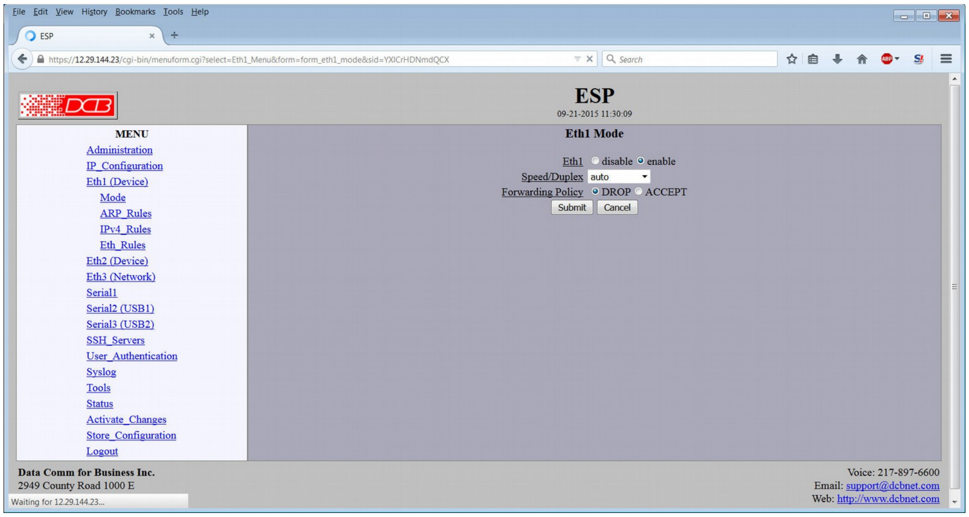
This screen configures an alias IP address for the ESP. An Alias IP address is a secondary IP address given to an interface. This is an optional field and is rarely used.

Fields

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

Notes:

Eth1 Mode



https://12.29.144.23/cgi-bin/menuform.cgi?select=Eth1_Menu&form=form_eth1_mode&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:30:09

Eth1 Mode

Eth1 ○ disable ● enable

Speed/Duplex auto

Forwarding Policy ● DROP ○ ACCEPT

Data Comm for Business Inc.
2949 County Road 1000 E

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Waiting for 12.29.144.23...

Ethernet 1 Mode Screen

The ESP contains three independent ethernet interfaces. Ethernet interfaces one and two are connected to devices to be protected. Ethernet interface three is connected to the incoming network.

Fields

- Enable / Disable
  Each ethernet interface may be individually enabled or disabled.

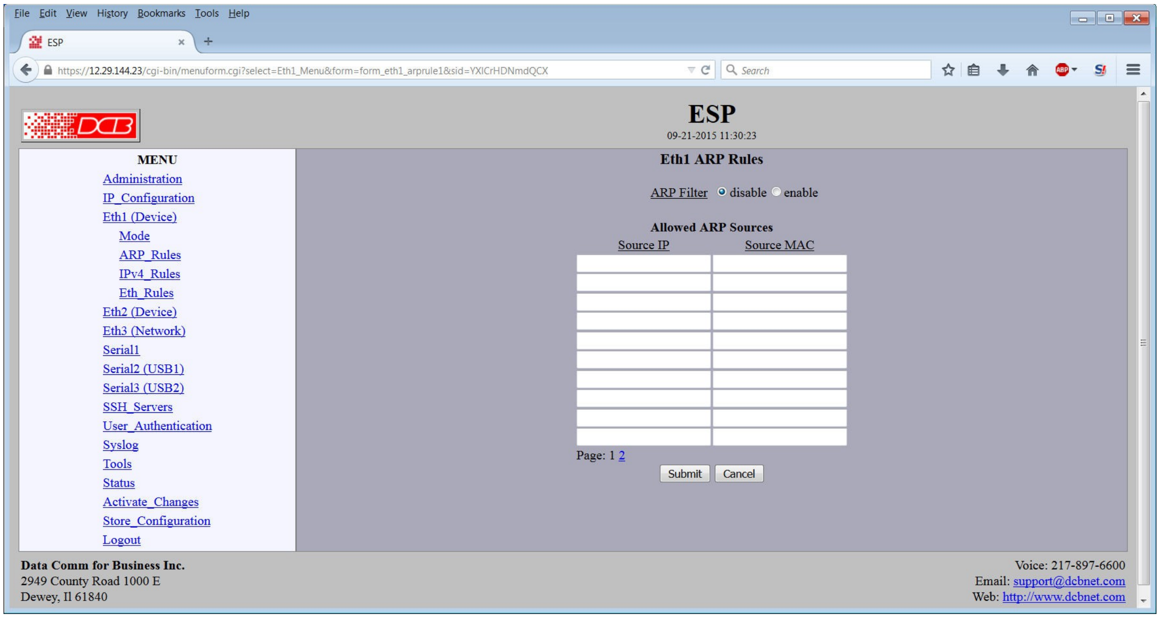
- Speed/Duplex
  This field allows Nway auto-negotiation to be disabled and to force the ethernet speed and duplex to a fixed setting.

- Forwarding Policy (Drop or Accept)
  This field sets the packet forwarding policy for the port. When set to *DROP* all packets will be dropped unless the packet matches an IPv4 Rule or an Ethernet Rule that accepts the packet. When set to *ACCEPT* all packets will be accepted unless the packet matches an IPv4 Rule or an Ethernet Rule that drops the packet.

  The best practice is to set the forwarding policy to DROP on the device ports, then to define the minimum set of IPv4 and Eth rules accepting packets needed by the device.

Notes:

Eth1 ARP Rules



ESP

09-21-2015 11:30:23

Eth1 ARP Rules

ARP Filter ● disable ○ enable

Allowed ARP Sources

Source IP	Source MAC

Page: 1 2

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Ethernet 1 ARP Rules Screen

Address Resolution Protocol (ARP) is one of the IP protocols. It is used to map a logical IP address to a physical Ethernet address, also called a MAC address, of a device. Since all IP devices must support ARP, ARP is frequently abused. It provides a convenient mechanism to map a subnet, and with ARP spoofing, can to used to insert a rogue device in the middle of a communication path.

The ESP can be configured to filter ARP packets as they egress (output) a port. This simple feature can be used to greatly limit the visibility of a device on the subnet. In addition, by configuring filter rules to include both the IP and MAC address, ARP spoofing becomes difficult to perform.

The scope of ARP is limited to a subnet. Devices outside the subnet cannot directly generate an ARP request. In this case, communication is via a gateway router, and any ARP requests will come from the gateway router.

Fields

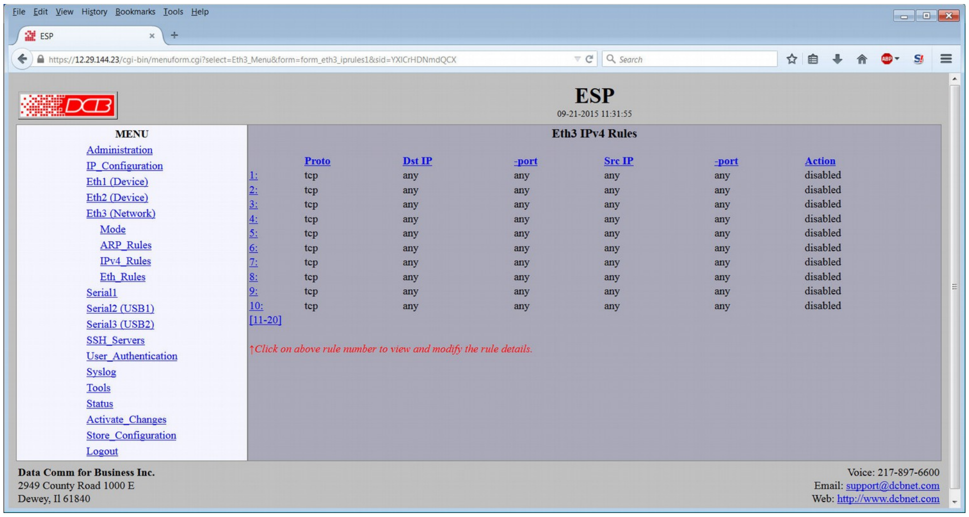
- ARP Filter Enable / Disable
  Enable/Disable ARP filtering on the specified port. When enabled, only ARP messages that match a rule will egress out this port.

- Source IP
  Source IP address of the device generating the ARP packet. If blank, any IP is allowed, provided the MAC matches.

- Source MAP
  Source MAC (Ethernet) address of the device generating the ARP packet. If blank, any MAC is allowed, provided the IP matches.

Notes:

Eth1 IPv4 Rules



File Edit View History Bookmarks Tools Help
ESP
https://12.29.144.23/cgi-bin/menuform.cgi?select=Eth3_Menu&form=form_eth3_iprules1&sid=YXICrHDNmdQCX
Search

ESP

09-21-2015 11:31:55

MENU
Administration
IP_Configuration
Eth1 (Device)
Eth2 (Device)
Eth3 (Network)
Mode
ARP_Rules
IPv4_Rules
Eth_Rules
Serial1
Serial2 (USB1)
Serial3 (USB2)
SSH_Servers
User_Authentication
Syslog
Tools
Status
Activate_Changes
Store_Configuration
Logout

Eth3 IPv4 Rules

	Proto	Dst IP	-port	Src IP	-port	Action
1:	tcp	any	any	any	any	disabled
2:	tcp	any	any	any	any	disabled
3:	tcp	any	any	any	any	disabled
4:	tcp	any	any	any	any	disabled
5:	tcp	any	any	any	any	disabled
6:	tcp	any	any	any	any	disabled
7:	tcp	any	any	any	any	disabled
8:	tcp	any	any	any	any	disabled
9:	tcp	any	any	any	any	disabled
10:	tcp	any	any	any	any	disabled
[11-20]						

↑Click on above rule number to view and modify the rule details.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Ethernet 1 IPv4 Rules Screen

The ESP can act as a transparent firewall, monitoring IPv4 frames and selecting which frames are allowed to pass. The decision to ALLOW or DROP a frame occurs on output, just before a frame is to egress an Ethernet port. The frame is tested against the rules, and if it matches the criteria, the specified action is taken. In addition, the event can be logged to a remote syslog server.

The IPv4 rules are applied in the listed order. Once a packet is either ALLOWED or DROPPED it will not be tested against any following rules.

Fields

- Rule Number

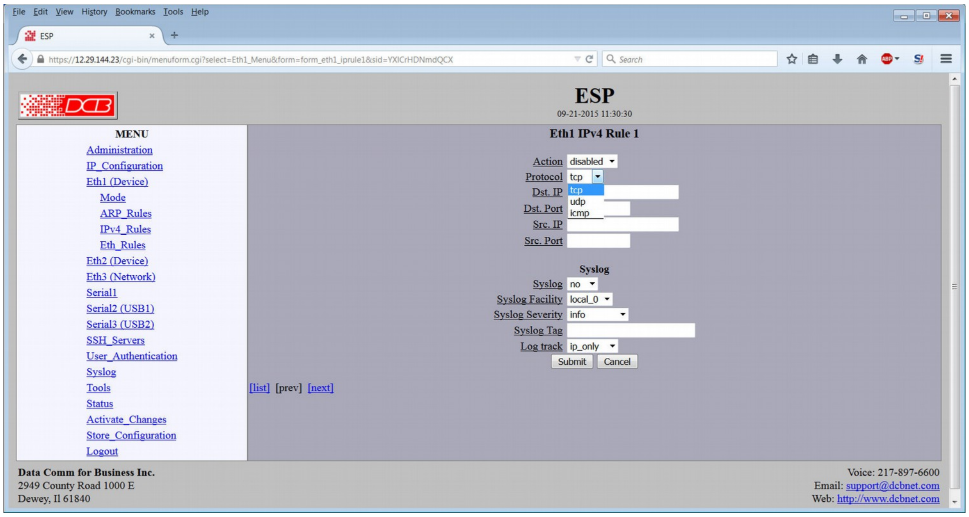
  There are 20 IPv4 handling rules, summarized in two screens of ten each. The rule number displayed on this screen is a link to the detailed rule configuration screens.

- Display Fields

  This summary screen displays overview information for the 20 IPv4 rules. Protocol, Destination IP, Destination Port, Source IP, Source Port, and action are displayed for each rule.

Notes:

Eth1 IPv4 Rule # 1 – 20 Details



ESP

09-21-2015 11:30:30

Eth1 IPv4 Rule 1

Action: disabled
Protocol: tcp (tcp, udp, icmp)
Dst. IP:
Dst. Port:
Src. IP:
Src. Port:

Syslog

Syslog: no
Syslog Facility: local_0
Syslog Severity: info
Syslog Tag:
Log track: ip_only

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Ethernet 1 IPv4 Rules Detail Configuration Screen

The ESP can act as a transparent firewall, monitoring IPv4 frames and selecting which frames are allowed to pass. The decision to ALLOW or DROP a frame occurs on output, just before a frame is to egress an Ethernet port. The frame is tested against the rules, and if it matches the criteria, the specified action is taken. In addition, the event can be logged to a remote syslog server.

There may be up to 20 IPv4 rules. The rules are applied in the listed order. Once a packet is either ALLOWED or DROPPED it will not be tested against any following IPv4 rules.

Fields

- Action
  This field specifies the action to take if a packet meets the criteria. The action can be to *DROP* the packet or to *ACCEPT* the packet. If the rule is *disabled* it is ignored and no action will be taken.
- Protocols
  This selects the IPv4 protocol of the frame. The options are *TCP*, *UDP*, or *ICMP*.
- Destination IP
  This field specifies the Destination IP address and optional subnet mask. It is specified as an *address/mask* where the */mask* part is optional and may be in the dotted format or bit count format. For example:

  ```
  192.168.0.1
  192.168.0.0/255.255.255.0
  192.168.0.0/24
  ```

  If the Destination IP field is blank, any address is considered a match.

- Destination Port
  This field specified the Destination port. This field is ignored if the IPv4 Protocol is set to ICMP. ICMP frames to not have a destination port component.

- Source IP
  This field specifies the Source IP address and optional subnet mask. See the Destination IP address above for examples.
- Source Port
  This field specifies the Source port. This field is ignored if the IPv4 Protocol is set to ICMP. ICMP frames to not have a source port component.
- Syslog
  When a IPv4 frame matches a rule, the event can be logged.
- Syslog Facility
  The Syslog Facility Code is an identifier used by a remote syslog server to catogorize an event. The code choosen is arbitrary and typically used to identify a resource. yslog Severity
- Syslog Severity

  The Syslog Severity Code is an identifier used by a remote syslog server to catogorize the severity of an event. The code choosen is arbitrary and typically used to trigger a specific action by the syslog server. For example, a *critical* event may cause a syslog server to send an email alert.
- Syslog Msg

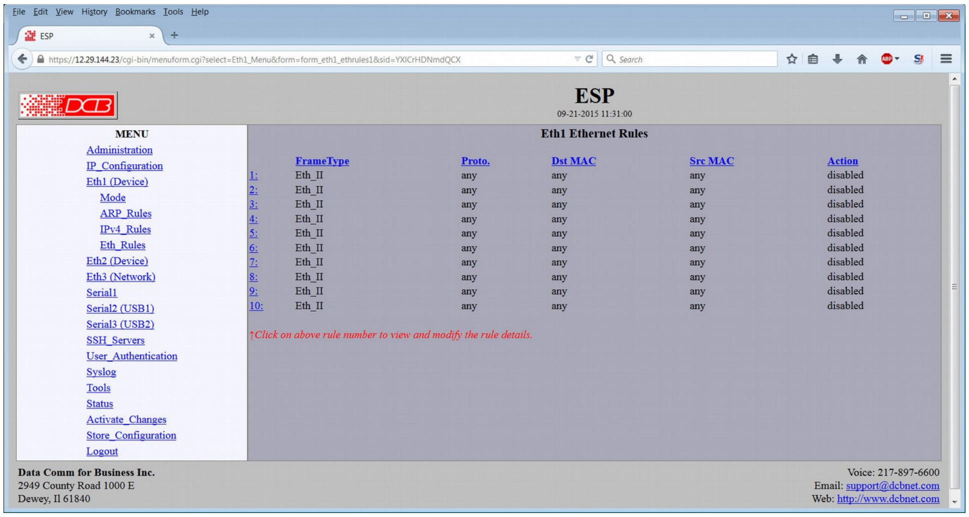
  The Syslog Msg is a small identifier string that will be included in the body of a syslog message. The identifier may be up to 28 characters in length and consist of letters, digits, and the underscore character.
- Syslog Track

  This option selects how the event is tracked. Generating a syslog message for every IPv4 packet that matches the rule could potentially generate a large number of syslog messages. To minimize this, the ESP tracks the event and only sends periodic messages. In addition, the ESP can track the event with more or less detail. *Ip_only* is the least detail. The ESP will only track events by the source and destination address. *Src_port* and *dst_port* is the next level of detail and tracks the event by the IP addresses and by the source port or destination port. *Src+dst* is the maximum level and tracks the packet by all four fields, source IP, source port, destination IP, and destination port.

  For most protocols, *dst* tracking is the appropriate choice.
- List
  Display the IPv4 Rules Summary page
- Prev
  Display the previous rule's detail page
- Next
  Display the next rule's detail page

Notes:

Eth1 Ethernet Rules



File Edit View History Bookmarks Tools Help
ESP
https://12.29.144.23/cgi-bin/menuform.cgi?select=Eth1_Menu&form=form_eth1_ethrules1&sid=YXICrHDNmdQCX
Search

ESP

09-21-2015 11:31:00

Eth1 Ethernet Rules

	FrameType	Proto.	Dst MAC	Src MAC	Action
1:	Eth_II	any	any	any	disabled
2:	Eth_II	any	any	any	disabled
3:	Eth_II	any	any	any	disabled
4:	Eth_II	any	any	any	disabled
5:	Eth_II	any	any	any	disabled
6:	Eth_II	any	any	any	disabled
7:	Eth_II	any	any	any	disabled
8:	Eth_II	any	any	any	disabled
9:	Eth_II	any	any	any	disabled
10:	Eth_II	any	any	any	disabled

↑Click on above rule number to view and modify the rule details.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Ethernet 1 Ethernet Rules Screen

The ESP can act as a transparent firewall, monitoring Ethernet frames and selecting which frames are allowed to pass. The decision to ALLOW or DROP a frame occurs on output, just before a frame is to egress an Ethernet port. The frame is tested against the rules, and if it matches the criteria, the specified action is taken. In addition, the event can be logged to a remote syslog server.

The Ethernet rules are applied in the listed order. Once a packet is either ALLOWED or DROPPED it will not be tested against any following rules.

The Ethernet rules are applied after the IPv4 rules. If a packet is ALLOWED or DROPPED by an IPv4 rule, then the packet will not be tested against any of the Ethernet rules.

Note: The need to filter at the raw Ethernet level should be rare and for most applications all filtering can be done at the IPv4 level. Designing a set of Ethernet rules for an application would require an advanced understanding protocols in use by the target devices.

Fields

- Rule Number

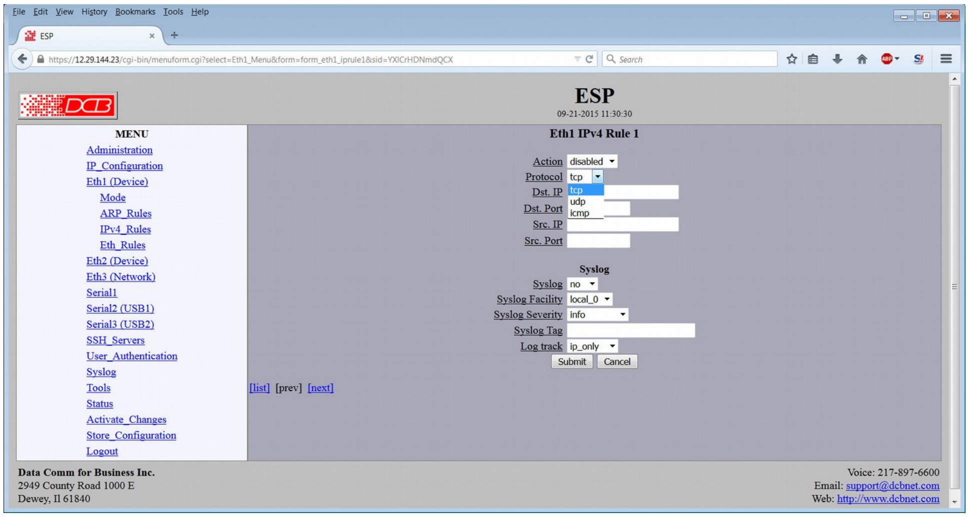
  There are 10 ethernet handling rules. The rule number displayed on this screen is a link to the detailed rule configuration screens.

- Display Fields

  This summary screen displays overview information for the 10 ethernet rules. Frame Type, Protocol, Destination MAC Address, Source MAC Address, and Action are displayed for each rule.

Notes:

Eth1 Ethernet Rule # 1 – 10 Details



ESP

09-21-2015 11:30:30

Eth1 IPv4 Rule 1

Action: disabled
Protocol: tcp
Dst. IP:
Dst. Port:
Src. IP:
Src. Port:

Syslog

Syslog: no
Syslog Facility: local_0
Syslog Severity: info
Syslog Tag:
Log track: ip_only

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Eth1 Ethernet Rules Detail Configuration Screen

The ESP can act as a transparent firewall, monitoring Ethernet frames and selecting which frames are allowed to pass. The decision to ALLOW or DROP a frame occurs on output, just before a frame is to egress an Ethernet port. The frame is tested against the rules, and if it matches the criteria, the specified action is taken. In addition, the event can be logged to a remote syslog server.

The Ethernet rules are applied in the listed order. Once a packet is either ALLOWED or DROPPED it will not be tested against any following rules.

The Ethernet rules are applied after the IPv4 rules. If a packet is ALLOWED or DROPPED by an IPv4 rule, then the packet will not be tested against any of the Ethernet rules.

Note: The need to filter at the raw Ethernet level should be rare and for most applications all filtering can be done at the IPv4 level. Designing a set of Ethernet rules for an application would require an advanced understanding protocols in use by the target devices.

Fields

- Action
  This field specifies the action to take if a packet meets the criteria. The action can be to *DROP* the packet or to *ACCEPT* the packet. If the rule is *disabled* it is ignored and no action will be taken.

- Frame Type
  This field selectes the Ethernet frame type. The choices are *Ethernet II* or *802.3*.

- Protocol
  This field selects the Ethernet Protocol. The Ethernet protocol is specified as a hexadecimal number greater than 0x600.

- Destination MAC address
  This field specifies the destination MAC address. The MAC address is specified as an address with an optional mask. Below are some examples:

```
00:09:AA:01:23:45                         {single host}
00:09:AA:00:00:00/ff:ff:ff:00:00:00       {hosts with OUI 00:09:AA}
01:00:00:00:00:00/01:00:00:00:00:00       {all multicast}
```

- Source MAC Address
  This field specifies the source MAC address. The MAC address is specified as an address with an optional mask. Below are some examples:

```
00:09:AA:01:23:45                           {single host}
00:09:AA:00:00:00/ff:ff:ff:00:00:00         {hosts with OUI 00:09:AA}
01:00:00:00:00:00/01:00:00:00:00:00         {all multicast}
```

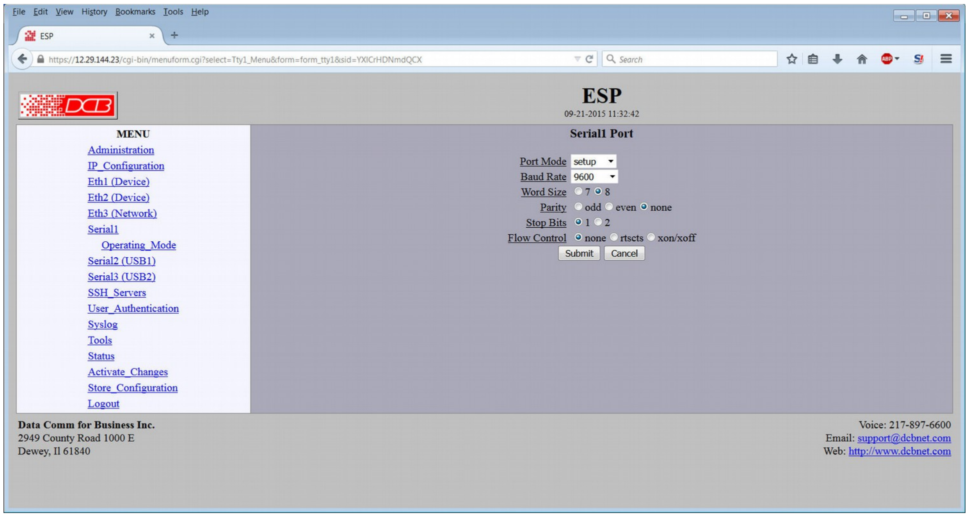
- Syslog
  When a frame matches a rule, the event can be logged.
- Syslog Facility
  The Syslog Facility Code is an identifier used by a remote syslog server to catogorize an event. The code chosen is arbitrary and typically used to identify a resource.
- Syslog Severity

  The Syslog Severity Code is an identifier used by a remote syslog server to categorize the severity of an event. The code chosen is arbitrary and typically used to trigger a specific action by the syslog server. For example, a *critical* event may cause a syslog server to send an email alert.
- Syslog Msg

  The Syslog Msg is a small identifier string that will be included in the body of a syslog message. The identifier may be up to 28 characters in length and consist of letters, digits, and the underscore character.

Notes:

Serial 1 Configuration



https://12.29.144.23/cgi-bin/menuform.cgi?select=Tty1_Menu&form=form_tty1&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:32:42

Serial1 Port

Port Mode: setup
Baud Rate: 9600
Word Size: ○ 7 ● 8
Parity: ○ odd ○ even ● none
Stop Bits: ● 1 ○ 2
Flow Control: ● none ○ rtscts ○ xon/xoff

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Serial 1 Configuration Screen

The ESB contains three serial ports. This screen is used to configure the individual serial port operating mode and parameters. Serial1 is factory defaulted to the “setup” mode. Other modes are *device, user*, and *disable*. See the other manual chapters for details about each mode. The port should be disabled if not in use.

Setup Mode is a special configuration mode which allows the the ESP to be reset to defaults or to allow the IP configuration to be changed. Setup Mode is the default mode for all serial ports and is enabled when the configuration reset sequence is performed on the device. During initial configuration, it is best to have at least one serial port configured for Setup Mode. However, for best security, Setup Mode should be disabled once a working configuration has been established.

Fields

- Port Mode

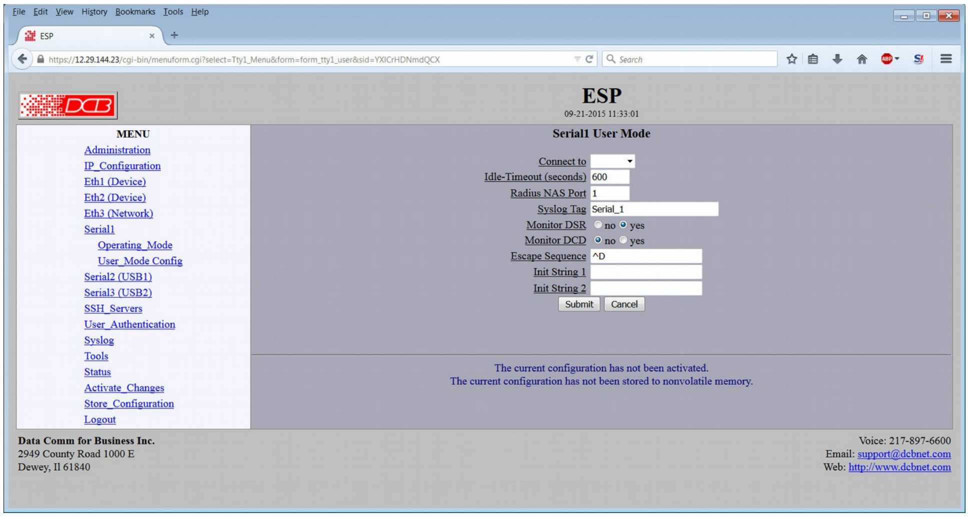
  This field selects the operating mode for the serial port. The supported modes are device, user, and setup. The port should be disabled if it is not being used
- Baud Rate
  Serial port Baud rate. Values range from 300 bps to 115,200 bps.
- Word Size
  Number of data bits in each character, either seven or eight data bits.
- Parity
  Enable parity generation and testing. Parity may be none, even, or odd.
- Stop Bits
  Select between 1 or 2 stop bits.
- Flow Control
  Flow control enable. Options are None, rts/cts, and xon/xoff. This must match the serial connected device.

Notes:

When any field is changed, the Submit button must be clicked or the changes will be lost when changing pages. If the port mode is changed, clicking the Submit button will change the left side screen menu options for that port appropriately.

***Setup Mode* is a special configuration mode which allows the the ESP to be reset to defaults or to allow the IP configuration to be changed. Setup Mode is the default mode for all serial ports and is enabled when the configuration reset sequence is performed on the device. Please refer to the ESP User Manual for more information. During initial configuration, it is best to have at least one serial port configured for Setup Mode. However, for best security, Setup Mode should be disabled once a working configuration has been established.**

Serial 1 User Mode Configuration



ESP

09-21-2015 11:33:01

Serial1 User Mode

Connect to	
Idle-Timeout (seconds)	600
Radius NAS Port	1
Syslog Tag	Serial_1
Monitor DSR	○ no ● yes
Monitor DCD	● no ○ yes
Escape Sequence	^D
Init String 1	
Init String 2	

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Serial 1 User Mode Configuration Screen

The ESB contains three serial ports. This screen is used to configure an individual serial port operating in user mode. User Mode is intended for use when a serial port is connected to a terminal, terminal emulator, or modem. The ESP will then act as an authentication proxy, verifying a user's credentials before granting access to a device's management interface. The port should be disabled if not in use.

Fields

- Connect to
  This field selects the target of the connection. Once a user is authenticated, a connection will be established with this target. Options are Serial 2 or Serial 3.

- Idle Timeout
  The amount of time, in seconds, before an idle connection is disconnected. A value of 0 disables the timer.

- Radius NAS Port
  The NAS port identifier for this resource. This identifier is arbitrary, and may be set to any value between 0 - 32767. However, this identifier is reported to both the Radius server and local authentication server when requesting access for a user.

- Syslog Tag
  The Syslog Tag is a text identifier included in messages sent to a syslog server related to this serial port. The identifier may be up to 28 characters in length and consist of letters, digits, and the underscore character. It would be typically be used to identify the device.

- Monitor DSR
  If set to *yes*, the ESP will monitor the DSR input signal. DSR must be active before a connection can be established. If DSR drops during a connection, the connection will be closed. In addition, if the port is configured for User Mode, the ESP will wait for DSR to go active before sending the Init Strings. This is for proper operation with a modem. If set to *no* the DSR input is ignored.

- Monitor DCD
  If set to *yes*, the ESP will monitor the DCD input signal. DCD must be active before a connecton can be established. If DCD drops during a connection, the conection will be closed. In addition, if the port is

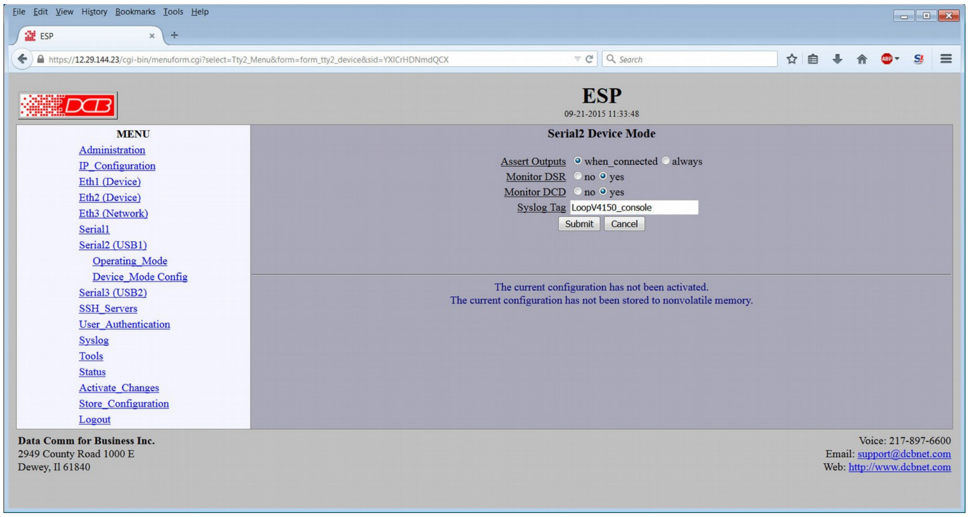
configured for User Mode, the ESP will wait for DCD to go active before displaying the banner and login prompt. If set to *no* the DCD input is ignored.

- Escape Sequence
  The escape sequence is an optional character sequence that can be issued to close a connection. This will force the connection between the User Port and the Device Port to close.
- Init String 1
  The ESP will send this string to the serial port after detecting DSR. This string can be used to initialize a modem. For example, to configure DCB's D-Series modem, you would use the string: "AT&FE0V1&C1&D2&K3N1X4"
- Init String 2
  The ESP will send this command after sending the first init string and delaying 1.5 seconds. This is to allow for additional configuration or to allow for modems that can not be reset and configured with a single command string.

Notes:

When any field is changed, the Submit button must be clicked.

Serial 1 Device Mode Configuration



https://12.29.144.23/cgi-bin/menuform.cgi?select=Tty2_Menu&form=form_tty2_device&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:33:48

Serial2 Device Mode

Assert Outputs ● when_connected ○ always
Monitor DSR ○ no ● yes
Monitor DCD ○ no ● yes
Syslog Tag LoopV4150_console

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Serial 1 Device Mode Configuration Screen

The ESB contains three serial ports.   This screen is used to configure an individual serial port operating in device mode. Device Mode is intended for use when a serial port is connected to the management interface of a device. The ESP will then act as a “lump in the cord” or an ethernet serial server, allowing connection to the device's management interface from either SSH or via a serial port configured for User Mode.   The port should be disabled if not in use.

Fields

- Assert Outputs
  If configured for *when_connected* the ESP will assert the DTR and RTS output signals when a connection is established with the port throught the ESP. When the connection is closed, the ESP will de-assert these signals. If configured for *always*, the ESP will assert RTS and DTR regardless of the state of the connection.

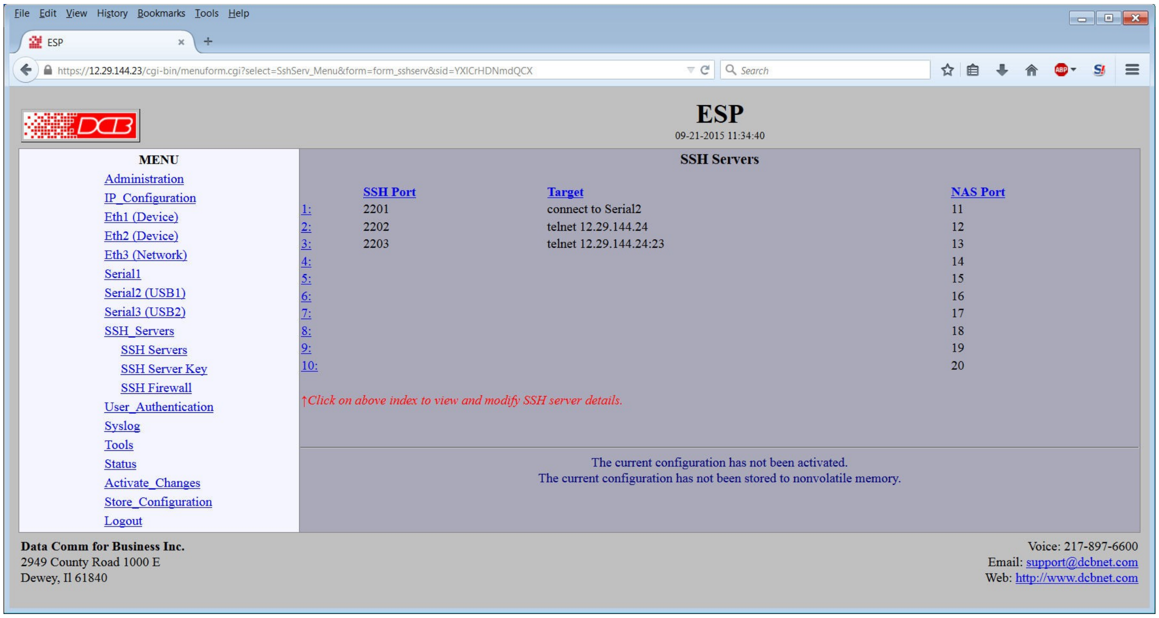
- Monitor DSR
  If set to *yes*, the ESP will monitor the DSR input signal. DSR must be active before a connection can be established. If DSR drops during a connection, the connection will be closed. In addition, if the connected port is configured for User Mode, the ESP will wait for DSR to go active before sending the Init Strings. This is for proper operation with a modem. If set to *no* the DSR input is ignored.

- Syslog Tag
  The Syslog Tag is a text identifier included in messages sent to a syslog server related to this serial port. The identifier may be up to 28 characters in length and consist of letters, digits, and the underscore character. It would be typically be used to identify the device.

Notes:

When any field is changed, the Submit button must be clicked.

SSH Servers



ESP

09-21-2015 11:34:40

SSH Servers

	SSH Port	Target	NAS Port
1:	2201	connect to Serial2	11
2:	2202	telnet 12.29.144.24	12
3:	2203	telnet 12.29.144.24:23	13
4:			14
5:			15
6:			16
7:			17
8:			18
9:			19
10:			20

↑*Click on above index to view and modify SSH server details.*

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

SSH Servers Summary Screen

The ESP can act as a Serial Server or Proxy Server for a protected device. Users wishing to communicate with the protected device must first connect to and authenticate with one of the ESP's SSH servers. Once authenticated, the ESP will establish a connection with the end-device and bridge the two connections together, allowing the user to interact with the device's management interface.

Fields

- SSH Server Number (1-10)

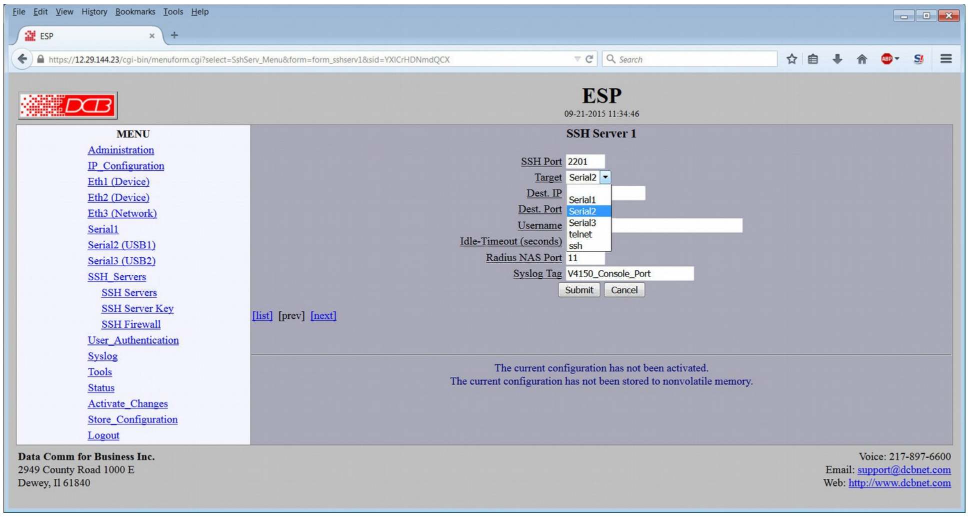
  There are 10 SSH Servers. The rule number displayed on this screen is a link to the detailed SSH Server configuration screens.

- Display Fields

This summary screen displays overview information for the configured SSH servers. SSH server number, SSH incoming Port, Target and NAS Port are displayed for each server.

Notes:

SSH Server 1-10 Configuration



ESP

09-21-2015 11:34:46

SSH Server 1

SSH Port: 2201
Target: Serial2
Dest. IP:
Dest. Port:
Username:
Idle-Timeout (seconds):
Radius NAS Port: 11
Syslog Tag: V4150_Console_Port

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

SSH Server 1-10 Configuration Screen

The ESP can act as a ethernet serial server or poxy server for a protected device. To communicate with the protected device one must first connect to and authenticate with one of the ESP's SSH servers. Once authenticated, the ESP will establish a connection with the end-device and bridge the two connections together, allowing the user to interact with the device's management interface.

Fields

- SSH Port
  This option specifies the listening port for the ESP's SSH Server. Each SSH Server must have a unique port number. It is OK to use the starndard SSH port of 22 for one of the servers.

  When connecting to one of the ESP's servers, you will need to specify the port on the SSH command line. This will be different for each implementation, but most will support either a -p option or allow the port to be included with the IP. For example:

  ```
  ssh -p 2200 someuser@192.168.5.10 or ssh someuser@192.168.5.10:2200
  ```
- Target
  This options specifies the Target of the SSH Server. Once a user has been authenticated, the user will be connected to the target. The target may be an ESP serial port configured for device mode, an end-device telnet server, or an end-device SSH server.

- Destination IP
  This option specifies the TCP/IP Destination IP for SSH and Telnet targets.

- Destination Port
  This option specifies the TCP/IP Destination Port for SSH and Telnet targets. If the option is blank, the default port for SSH, port 22, or the default port for Telnet, port 23, will be used. This field is ignored if the target is not SSH or Telnet.

- Username
  The *Username* is only used if the Target is SSH or Telnet. If a username is provided, it will be sent to the end-device during SSH or Telnet negotiation. Supplying a valid username during SSH negotiation may be required by the end-device. However, Telnet implementations do not support this option.

- Idle Timeout
  This field selects the amount of time, in seconds, before an idle SSH connection is disconnected. A value of 0 disables the timer.

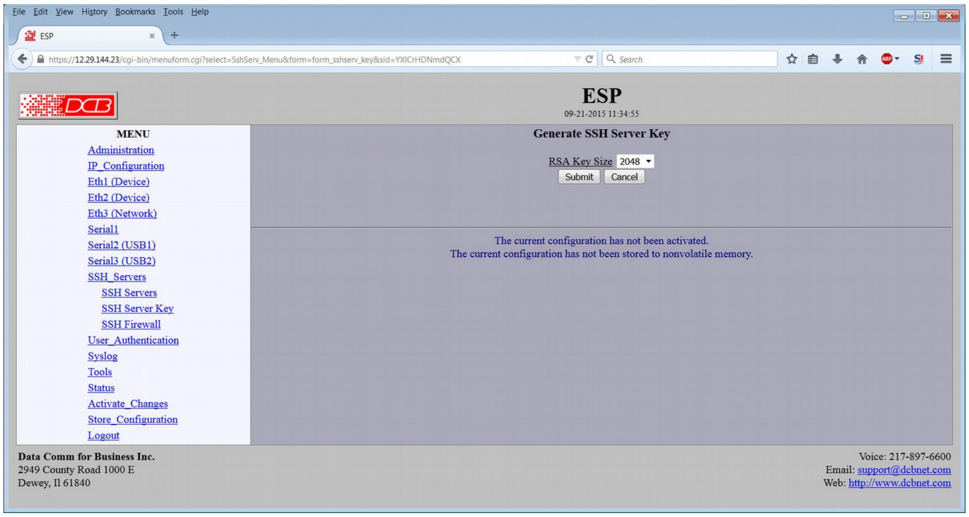
- RadiusNAS Port
  This field specifies the NAS port identifier for this resource. This identifier is arbitrary, and may be set to any value between 0 - 32767. However, this identifier is reported to both the Radius server and local authentication server when requesting access for a user.

- Syslog Tag
  The Syslog Tag is a text identifier included in messages sent to a syslog server related to this serial port. The identifier may be up to 28 characters in length and consist of letters, digits, and the underscore character. It would be typically be used to identify the target device.

Notes:

When any field is changed, the Submit button must be clicked.

Generate SSH Server Key



https://12.29.144.23/cgi-bin/menuform.cgi?select=SshServ_Menu&form=form_sshserv_key&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:34:55

Generate SSH Server Key

RSA Key Size: 2048

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Generate SSH Server Key Screen

The ESP's SSH server requires an RSA key that will be used to identify the ESP to an SSH client. The key must be generated before any of the RSA server's will start.

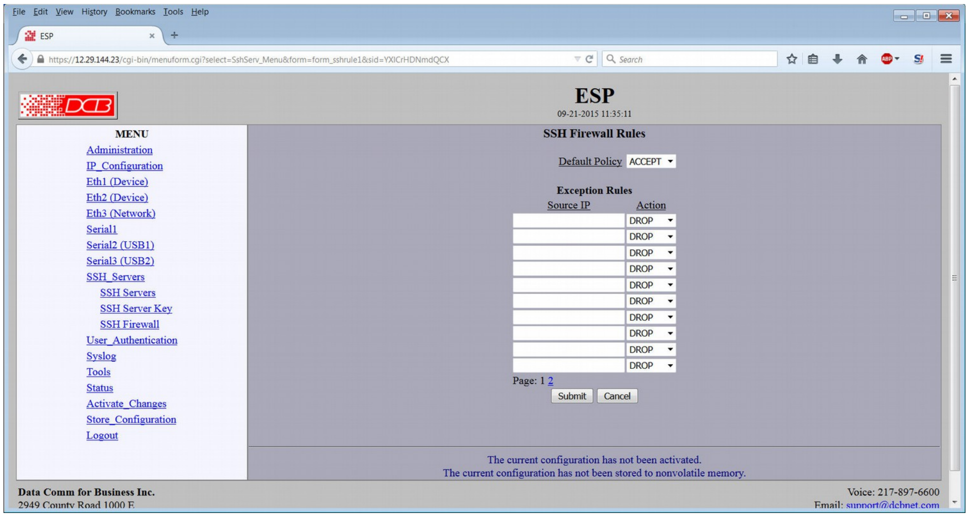
Fields

- RSA Key Size
  This option selects the size of the SSH Server's RSA key. *2048* is the current recommended size. Please keep in mind that not all SSH clients support larger keys. However, if your client only supports *1024* bit keys, it is recommended that you upgrade the client instead of using a 1024 bit RSA key.

Notes:

When any field is changed, the Submit button must be clicked.

SSH Firewall Rules



https://12.29.144.23/cgi-bin/menuform.cgi?select=SshServ_Menu&form=form_sshrule1&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:35:11

SSH Firewall Rules

Default Policy ACCEPT

Exception Rules

Source IP	Action
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP
	DROP

Page: 1 2

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E

Voice: 217-897-6600
Email: support@dcbnet.com

SSH Firewall Rules Screen

The SSH Firewall allows you to control which hosts or networks have access to the ESP's SSH servers. As SSH request packets are received, each packet is compared against the SSH Firewall rules, and the specified action taken if the rule matches.

Entries are made by specifying a Source IP and optional mask. For example, if you want to allow the host 192.168.10.16 access, you would enter:

```
Source IP: 192.168.10.16     Action: ALLOW
```

If you wanted to allow access to all hosts in the subnet 192.168.10.0 to 192.168.10.255, you would enter:

```
Source IP: 192.168.10.0/24   Action: ALLOW
```

The firewall rules are applied in the order displayed. This feature can be used to build more complex rules. For example, if you wanted to allow access to all hosts in a subnet, except for host .13, you could order two rules as follows:

```
Source IP: 192.168.10.13     Action: DROP
Source IP: 192.168.10.0/24   Action: ALLOW
```

Fields

- Default Policy
  The *Default Policy* configures the action to take if the incoming packets doesn't match any of the exception rules. The two actions are to *ACCEPT* the packet, or *DROP* the packet.
- Source IP
  This field specifies the Source IP address and optional subnet mask. It is specified as an *address/mask* where the */mask* part is optional and may be in the dotted format or bit count format. For example:

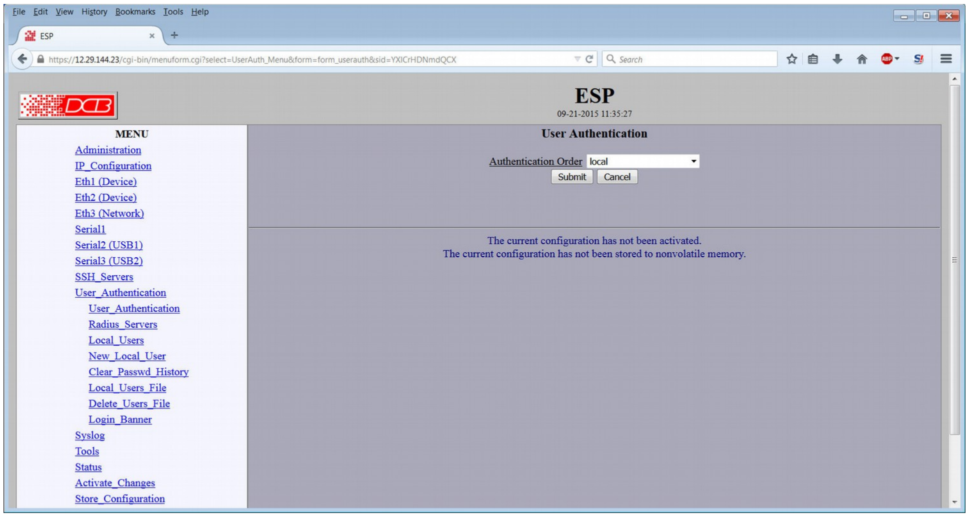
```
192.168.0.1
192.168.0.0/255.255.255.0
192.168.0.0/24
If the Source IP field is blank, the action is ignored.
```

- Action
  Drop or Accept the frames.

Notes:

When any field is changed, the Submit button must be clicked.

User Authentication



https://12.29.144.23/cgi-bin/menuform.cgi?select=UserAuth_Menu&form=form_userauth&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:35:27

User Authentication

Authentication Order: local

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

User Authentication Screen

Users are authenticated using either a Radius server or a local user's database. The ESP can authenticate users via a Radius server or by referencing a local Users database, or combination of both based upon the rules configured on this screen.

Fields

- Authentication Order
  This option sets the order in which the ESP will attempt to authenticate a user. When set to *local* the ESP will only reference the local Users database.

  When set to *radius* the ESP will only reference the Radius server.

  When set to *local, radius*, the ESP will first attempt to authenticate the user from the local Users database. If that fails, it will attempt to authenticate the user using the Radius server.

  When set to *radius, local,*, the ESP will first attempt to authenticate the user using the Radius server. If that fails, it will then attempt to authenticate the user using the local Users database.

  Finally, if set to *radius, local-on-timeout*, the ESP will first attempt to authenticate the user using the

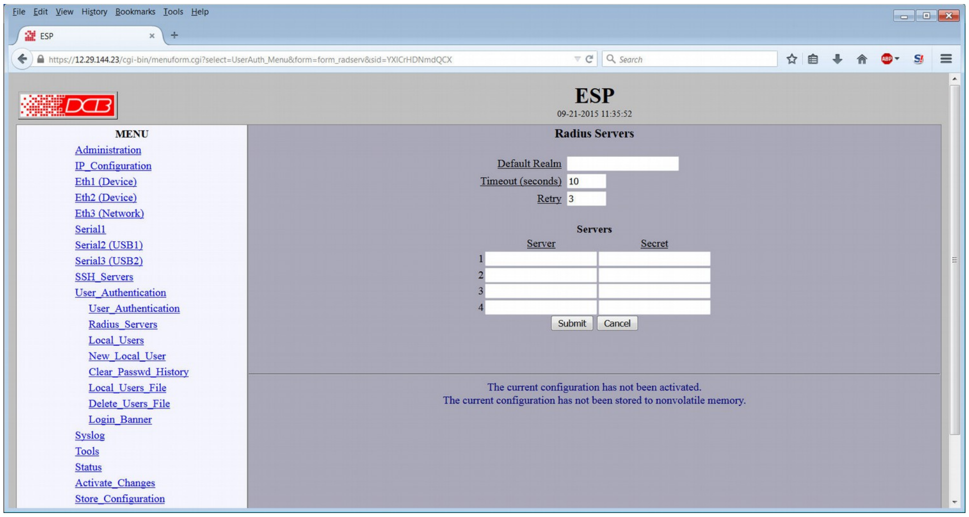
Radius server. If the Radius server rejects the user, then the user will not be granted access. However, if the Radius server does not respond, the ESP will then attempt to authenticate the user using the local Users database.

Notes:

Consider these options carefully as there are security as well as access availability ramifications for each option.

When any field is changed, the Submit button must be clicked.

Radius Servers



ESP

09-21-2015 11:35:52

Radius Servers

Default Realm:

Timeout (seconds): 10

Retry: 3

Servers

	Server	Secret
1		
2		
3		
4		

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Radius Servers Screen

Users are authenticated using either a Radius server or a local user's database. These configuration values are required when using a Radius server as an authentication method.

Fields

- Default Relm
  A *Default Realm* is a string that will be appended to a users name when sending it to a radius server, if the user's name doesn't already contain a realm. For example if a user entered the name "Bob" and the default realm was set to "esp1", the name "Bob@esp1" would be sent to the Radius server. However, if the user entered the name "Bob@home", then the default realm would not be added to the name and would be unchanged when sent to the radius server.

  Note: Not all radius servers support realms, thus it may not be necessary to set this field.

- Timeout
  This field sets how long to wait for a response from the Radius server before retrying the request.

- Retry
  This field set the number of time to retry a request before giving up on a Radius server.

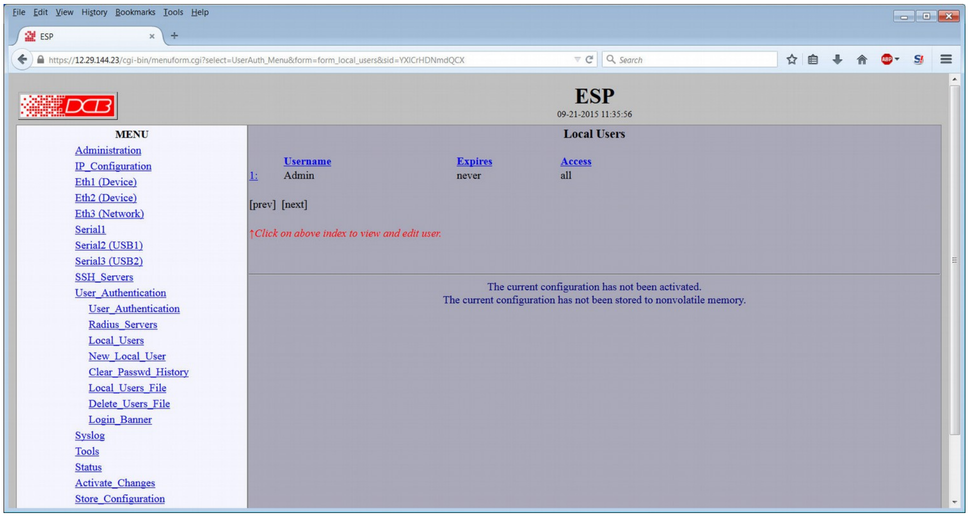
- Server
  This field sets the IP address or the hostname of the radius server. Up to 4 radius servers may be specified. If a hostname is used, DNS must be configured under the IP Configuration.

- Secret
  This field sets the shared secret for the ESP device and the radius server. The radius server must be configured with the same shared secret.

Notes:

When any field is changed, the Submit button must be clicked. I

Local Users List



ESP

09-21-2015 11:35:56

Local Users

	Username	Expires	Access
1:	Admin	never	all

[prev] [next]

↑Click on above index to view and edit user.

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Local Users List Screen

Users are authenticated using either a Radius server or a local user's database. This screen lists all local users, their expiration limit and access capabilities. The numbers link to individual user configuration edit screens.

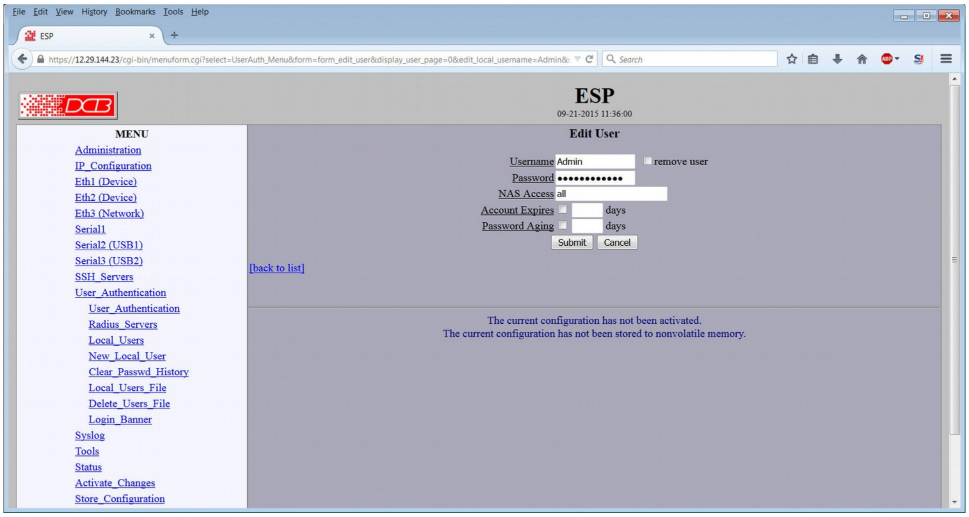
Fields

- User edit screen link
  Clicking on the numbers in the first column links to a user configuration screen.
- Prev, Next
  Displays additional user screens.
- Display fields
  User name, Expires, and Access fields display current values for existing users.

Notes:

When any field is changed, the Submit button must be clicked.

Edit User



https://12.29.144.23/cgi-bin/menuform.cgi?select=UserAuth_Menu&form=form_edit_user&display_user_page=0&edit_local_username=Admin&

ESP

09-21-2015 11:36:00

Edit User

Username Admin □ remove user
Password ••••••••••••
NAS Access all
Account Expires □ days
Password Aging □ days

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Edit User Screen

Users are authenticated using either a Radius server or a local user's database. This screen allows editing of information in the local users file.

Fields

- Username
  The username must be 1 to 15 characters in length. It may only contain letters and digits. The username is case sensitive.

- Remove User (check box)
  Check this box to remove the specified user. Remember to “submit” the screen.

- Password
  The password must be 8 to 15 characters in length and contain 3 of the 4 following types of character: upper-case, lower-case, digit, or special character. The password may contain any printable ASCII character, with the exception of the double-quote, space, and the backslash characters. The password is case sensitive. Strong passwords are required for proper security.

- NAS Access
  The ESP uses NAS port numbers for allowing or denying access to a resource. This field is a list of NAS ports that the user is allowed to access. For example, if NAS Access is set to "1 2 3", The user would be allowed access to the resources that have a NAS port ID of 1, 2, or 3. Optionally, the field may be set to the word *all* to allow access to all resources.

- Account Expires (check box and value)
  A user account can be configured to expire after some time period. The valid range is 1 - 365 days. The ESP will convert the setting to a calendar date, so be sure the date and time are correctly configured on the ESP prior to entering this information. Uncheck the box to disable account expiration.

- Password Aging (Check box and value)
  A user account can be configured to require the user to periodically change their password. The valid range is 1 - 356 days. Once a password has expired, the user will be required to change the password when they attempt to access a resource. A password history is maintained to prevent reuse of old passwords. Passwords are time-stamped with the current calendar date, so be sure the ESP is

configured with the correct date and time before entering this information. Uncheck the box to disable password expiration.

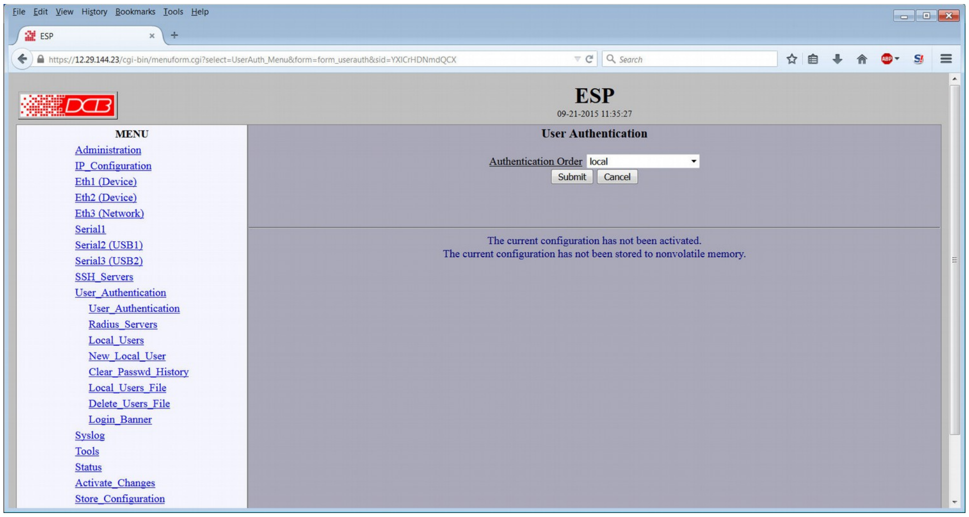
- Back to List
  Returns to the user list screen.

Notes:

Consider these options carefully as there are security as well as access availability ramifications for each option.

When any field is changed, the Submit button must be clicked.

Add New User



ESP

09-21-2015 11:35:27

User Authentication

Authentication Order: local

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Add New User Screen

Users are authenticated using either a Radius server or a local user's database. This screen allows adding a new user to the local users file.

Fields

- Username
  The username must be 1 to 15 characters in length. It may only contain letters and digits. The username is case sensitive.

- Password
  The password must be 8 to 15 characters in length and contain 3 of the 4 following types of character: upper-case, lower-case, digit, or special character. The password may contain any printable ASCII character, with the exception of the double-quote, space, and the backslash characters. The password is case sensitive. Strong passwords are required for proper security.

- NAS Access
  The ESP uses NAS port numbers for allowing or denying access to a resource. This field is a list of NAS ports that the user is allowed to access. For example, if NAS Access is set to "1 2 3", The user would be allowed access to the resources that have a NAS port ID of 1, 2, or 3. Optionally, the field may be set to the word *all* to allow access to all resources.

- Account Expires (check box and value)
  A user account can be configured to expire after some time period. The valid range is 1 - 365 days. The

ESP will convert the setting to a calendar date, so be sure the date and time are correctly configured on the ESP prior to entering this information. Uncheck the box to disable account expiration.

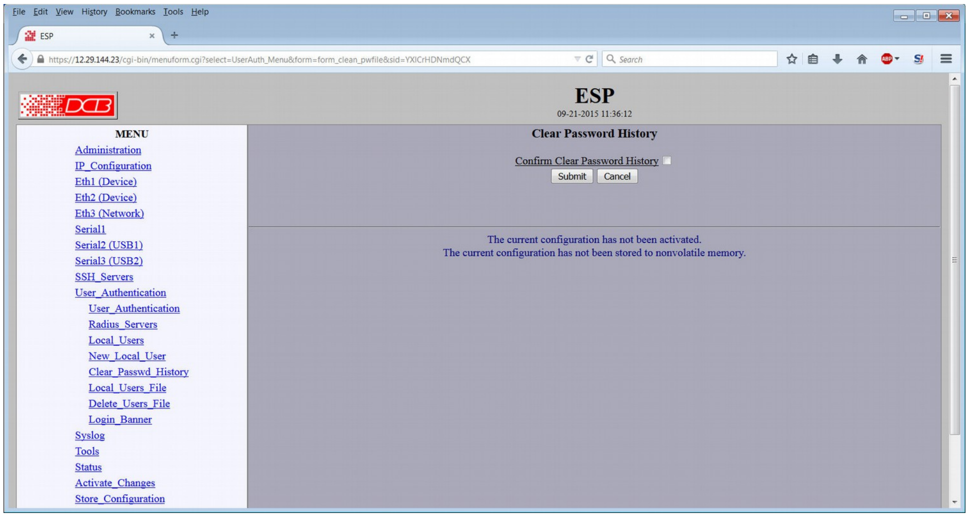
- Password Aging (Check box and value)
  A user account can be configured to require the user to periodically change their password. The valid range is 1 - 356 days. Once a password has expired, the user will be required to change the password when they attempt to access a resource. A password history is maintained to prevent reuse of old passwords. Passwords are time-stamped with the current calendar date, so be sure the ESP is configured with the correct date and time before entering this information. Uncheck the box to disable password expiration.

Notes:

Consider these options carefully as there are security as well as access availability ramifications for each option.

When any field is changed, the Submit button must be clicked.

Clear Password History



ESP

09-21-2015 11:36:12

Clear Password History

Confirm Clear Password History □

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Clear Password History Screen

The local users database contains a password history for each user. This screen action allows that history to be cleared.

Fields

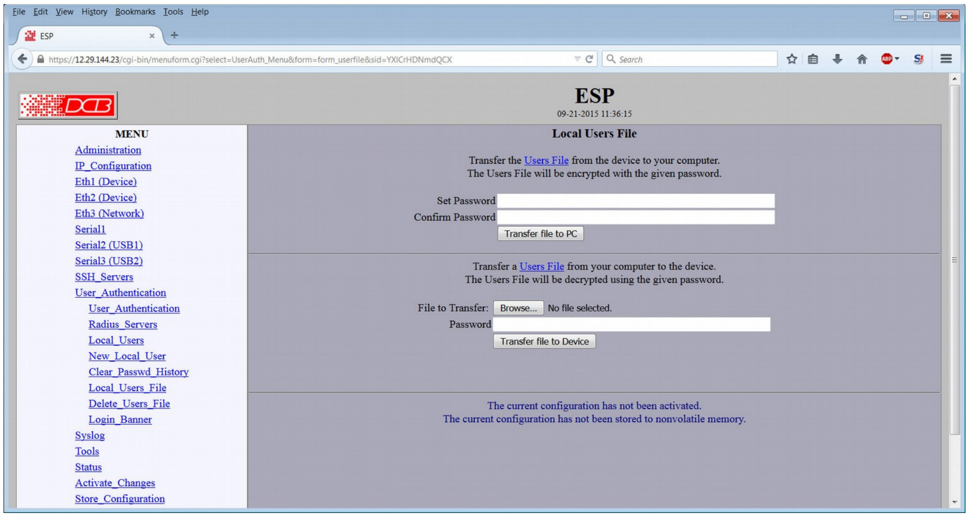
- Confirm Clear Password History (check box)
  To clear the password history from the users data base, click this field.

Notes:

You must Activate Changes for this operation to be completed.

When any field is changed, the Submit button must be clicked.

Local users File



ESP

09-21-2015 11:36:15

Local Users File

Transfer the Users File from the device to your computer.
The Users File will be encrypted with the given password.

Set Password

Confirm Password

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

File to Transfer: No file selected.

Password

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Local Users File Screen

A copy of the local users database can be pulled from or pushed to the ESP. This is for the purpose of backing up the database or for copying it to another ESP device. It is not a human readable file and the contents may not be viewed or modified outside of the ESP device. The local users file is password protected with an encryption password supplied by the user.

Fields

Transfer the local users file to the PC

- Set Password. The file you save will be encrypted on the PC. **This password will be required to retrieve the file later.**
- Confirm Password Verify the password entered above.
- Transfer File to PC (action) Click this button to copy the local users file to an encrypted file on the PC.

Retrieve a local users file from the PC

Transfers a previously stored local users file from the PC to the ESP.

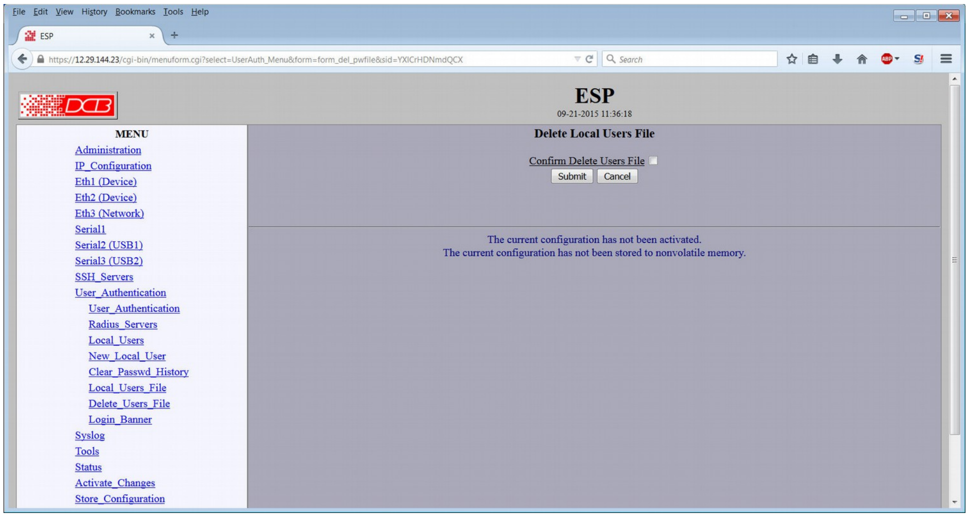
- File to Transfer The Click the Browse button to select a file to be transferred.
- Password the password used to encrypt the file when it was saved.
- Transfer File to Device (action) Click this button to copy the file into the ESP.

Notes:

Consider these options carefully as there are security as well as access availability ramifications for each option.

When any field is changed, the Submit button must be clicked.

Delete Users File



ESP

09-21-2015 11:36:18

Delete Local Users File

Confirm Delete Users File □

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Delete Local Users File Screen

This operation will delete the local users database from the ESP, effectively removing all users and their password history.

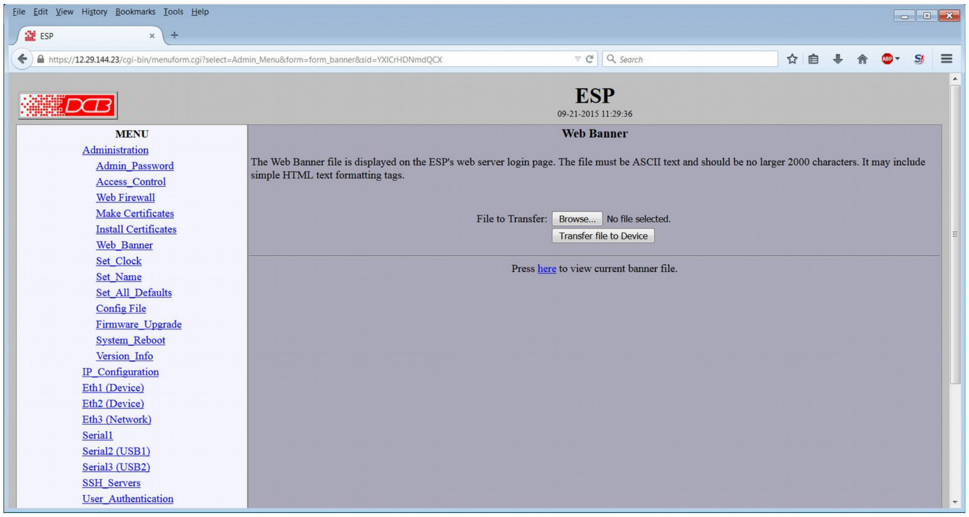
Fields

- Confirm Delete Users File (click box)
  Clicking this box will delete the local users database file from the ESP, effectively removing all users and their password history.

Notes:

Consider these options carefully as there are security as well as access availability ramifications for each option. When any field is changed, the Submit button must be clicked.

Login Banner



ESP

09-21-2015 11:29:36

Web Banner

The Web Banner file is displayed on the ESP's web server login page. The file must be ASCII text and should be no larger 2000 characters. It may include simple HTML text formatting tags.

File to Transfer: Browse... No file selected.

Press here to view current banner file.

Log In Banner Screen

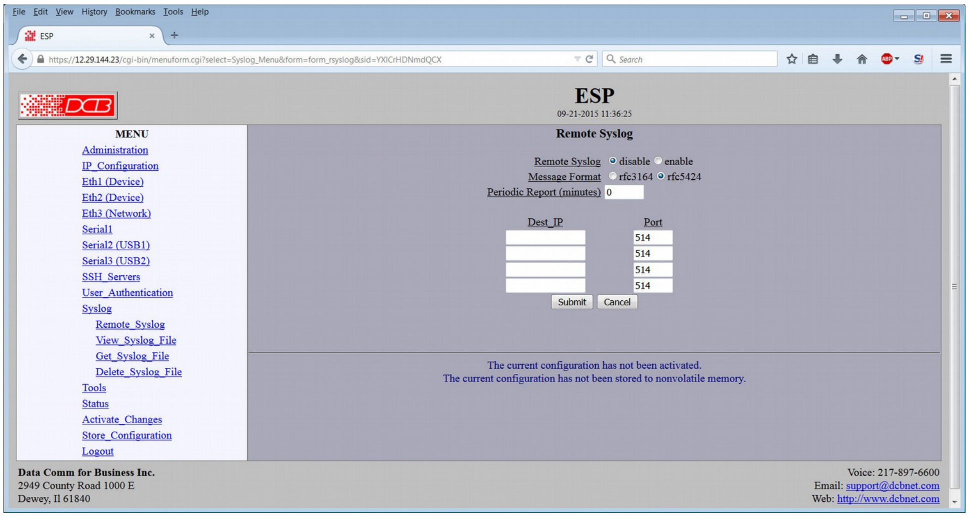
The Login Banner file is displayed when an SSH or serial terminal session is started with the ESP device. The file must be ASCII text and should be no larger than 2000 characters nor consist of more than 20 lines. Use this screen to transfer a file from a PC to the ESP.

Fields

- Browse (action)
  Click this button to browse to a file on the PC to be transferred to the ESP.
- Transfer File to Device
  Click this button to transfer the file to the ESP.
- Press here to view current banner file
  Click here to display the current ESP banner file.

Notes:

Remote Syslog



ESP

09-21-2015 11:36:25

Remote Syslog

Remote Syslog ● disable ○ enable

Message Format ○ rfc3164 ● rfc5424

Periodic Report (minutes) 0

Dest_IP	Port
	514
	514
	514
	514

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Remote Syslog Screen

Activity on the ESP may be logged locally or remotely.   This screen configures the operation of remote syslog (Rsyslog).

Fields

- Remote Syslog
  Disable or enable sending log messages to a remote syslog server.

- Message Format
  This option selects the format of the messages sent to the remote syslog server. 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"*.

  Note: This setting will also apply to the format of the local syslog file.

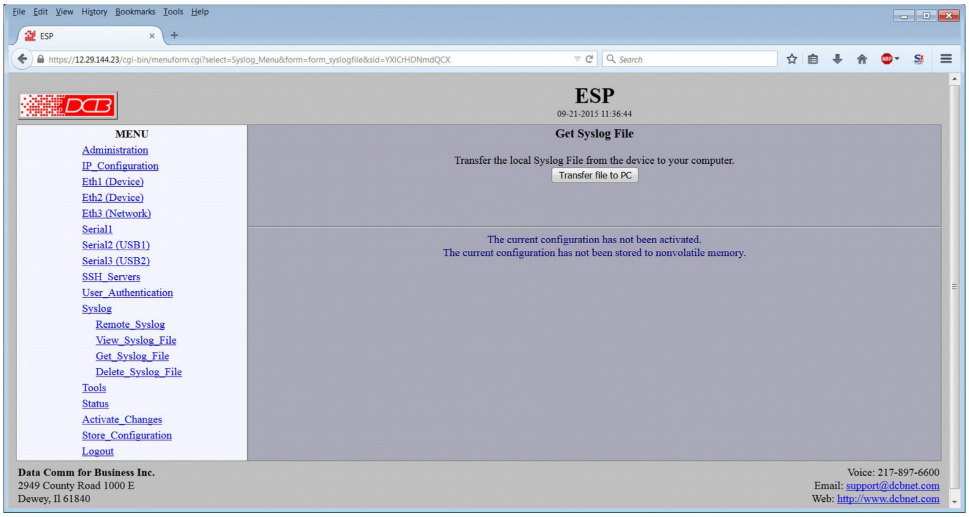
- Destination IP
  The IPv4 address of a remote syslog server. Hostnames are not allowed.

- Protocol
  The field selects the transport protocol. Most syslog servers use the UDP protocol.

- Destination Port
  The UDP or TCP port number of the remote syslog server. Port 514 is the port typically reserved for rsyslog.

Notes:

Get Syslog File



ESP

09-21-2015 11:36:44

Get Syslog File

Transfer the local Syslog File from the device to your computer.

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Get Syslog File Screen

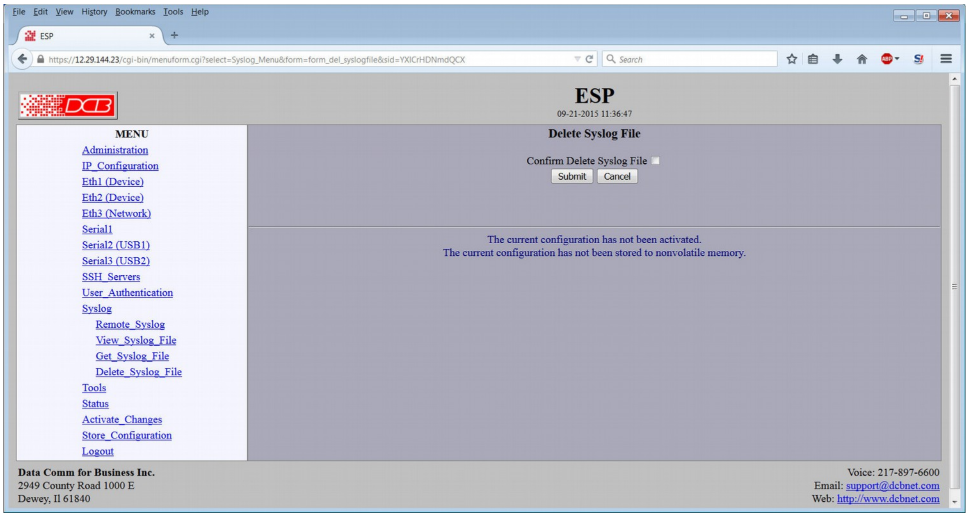
This screen is used to view or transfer the local syslog file from the ESP to your computer. This is a text file and is not encrypted.

Fields

- Transfer file to PC
  Click this button to copy the syslog file to your PC.
- View file
  Click this button to view the syslog file.

Notes:

Delete Syslog File



ESP

09-21-2015 11:36:47

Delete Syslog File

Confirm Delete Syslog File □

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Delete Syslog File Screen

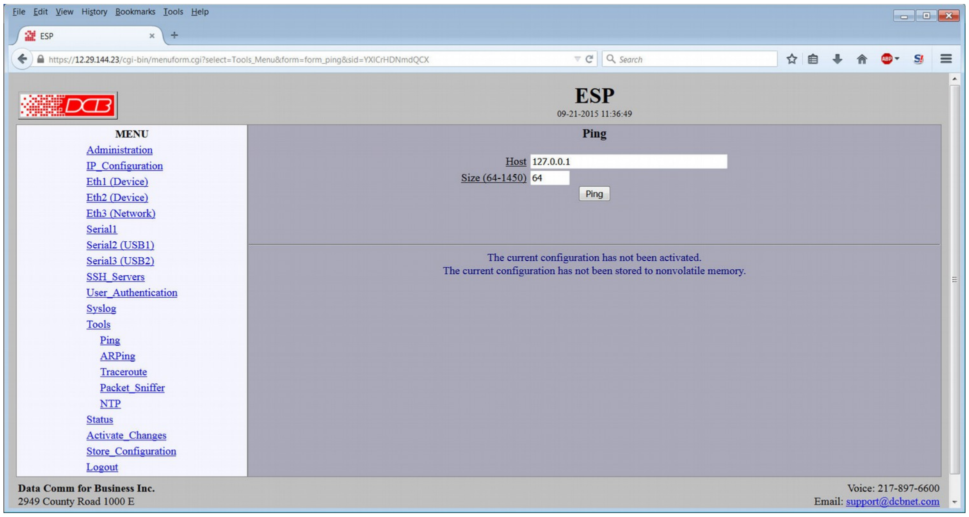
This screen deletes the local syslog file. If needed for future reference, be sure to transfer the file to your workstation prior to deletion.

Fields

- Confirm Delete Syslog File (checkbox)
  Click this button to delete the syslog file. Then press the Submit button.

Notes:

Ping Screen



ESP

09-21-2015 11:36:49

Ping

Host 127.0.0.1

Size (64-1450) 64

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E

Voice: 217-897-6600
Email: support@dcbnet.com

Ping Screen

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

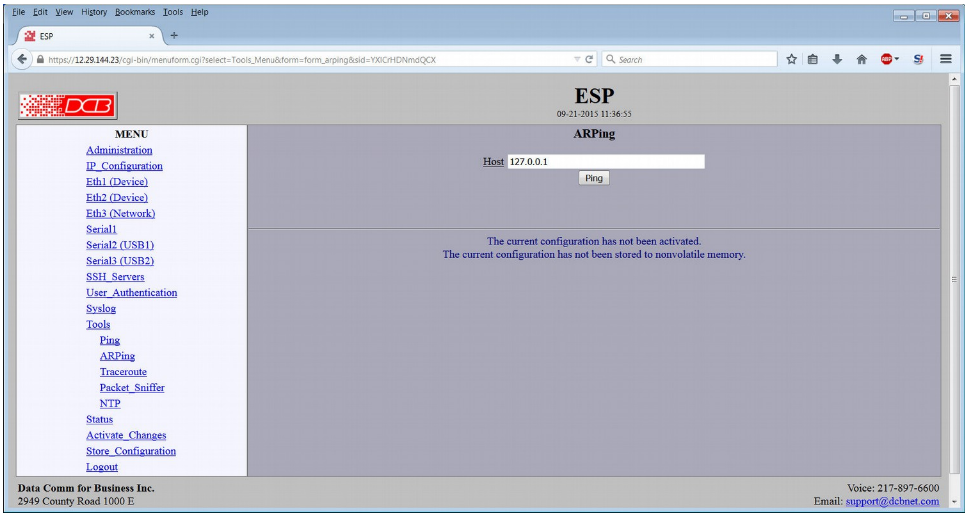
Fields

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

Notes

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

ARPing Screen



https://12.29.144.23/cgi-bin/menuform.cgi?select=Tools_Menu&form=form_arping&sid=YXICrHDNmdQCX

ESP

09-21-2015 11:36:55

ARPing

Host 127.0.0.1

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E

Voice: 217-897-6600
Email: support@dcbnet.com

ARPing Screen

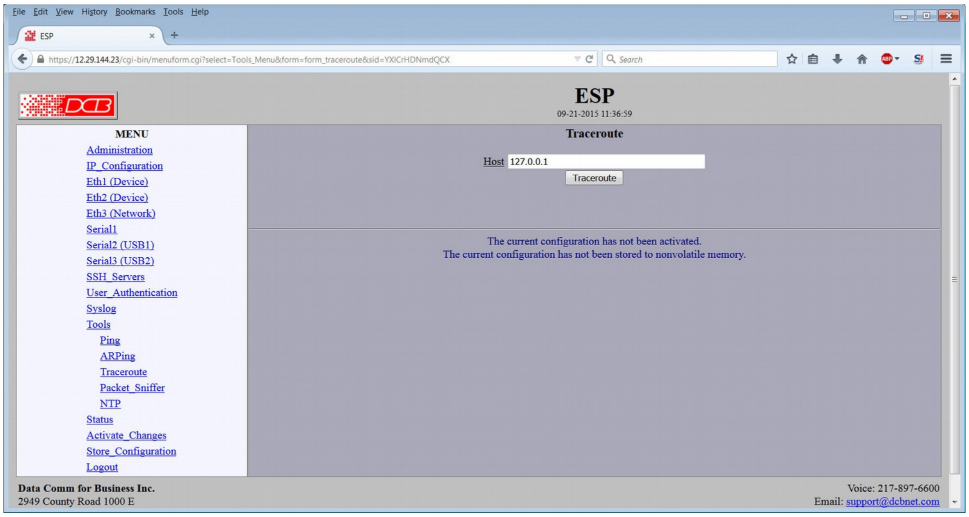
Ping will send four ARPing echo requests to the specified host. This command is useful for determining the MAC adddress of a device.

Fields

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

Notes

Traceroute Screen



ESP

09-21-2015 11:36:59

Traceroute

Host 127.0.0.1

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E

Voice: 217-897-6600
Email: support@dcbnet.com

Traceroute Screen

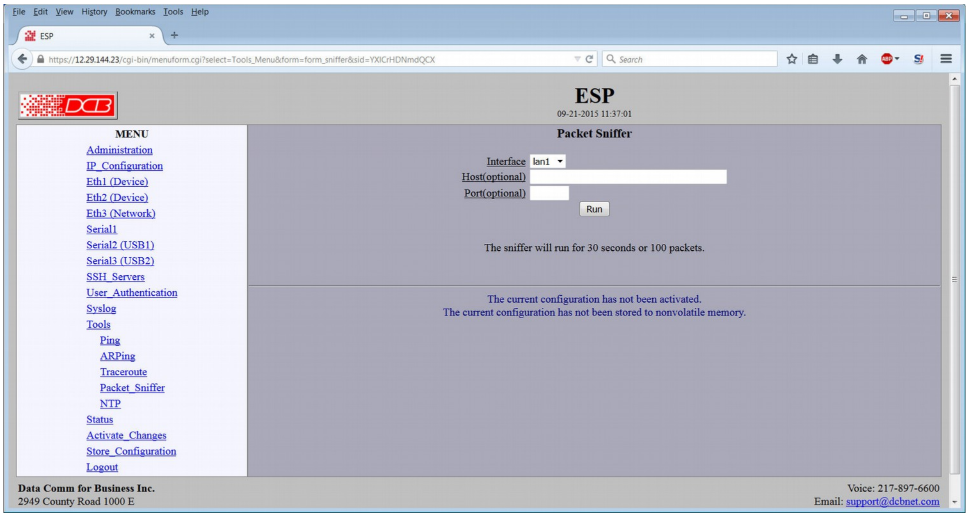
Traceroute displays the route that a packet will take to reach another host. This is performed by sending UDP packets to port 33434 with progressively larger Time-to-Live values and listening for ICMP TIME-EXCEEDED responses from the devices along the way.

Fields

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

Notes

Packet Sniffer



ESP

09-21-2015 11:37:01

Packet Sniffer

Interface: lan1

Host(optional):

Port(optional):

The sniffer will run for 30 seconds or 100 packets.

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E

Voice: 217-897-6600
Email: support@dcbnet.com

Packet Sniffer Screen

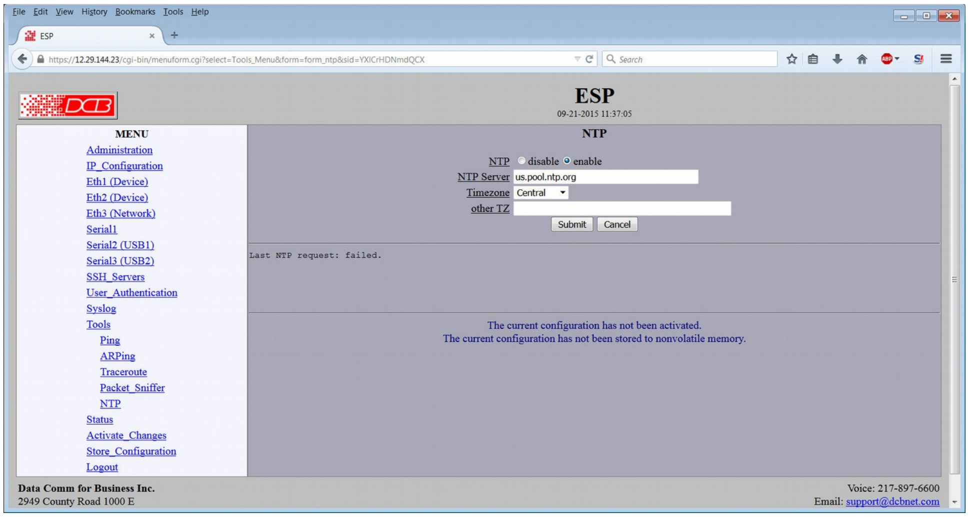
The Packet Sniffer allows you to take a snapshot of the network traffic passing through an interface.

Fields

- Interface
  This field selects which interface to monitor. Selecting Lan1 will monitor all three Ethernet interfaces. Otherwise, selecting Eth1, Eth2, or Eth3 will monitor traffic sent and received on that specific interface.
- 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

NTP Configuration



ESP

09-21-2015 11:37:05

NTP

NTP ○ disable ● enable

NTP Server us.pool.ntp.org

Timezone Central

other TZ

```
Last NTP request: failed.
```

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E

Voice: 217-897-6600
Email: support@dcbnet.com

NTP Configuration Screen

The use of an NTP server and the protocol to keep a current clock is recommended. The clock is used to timestamp log entries.

Fields

NTP Enable/Disable

Enable/Disable the NTP client. When enabled the NTP client will request the current time from a time server and set the internal clock. It will repeat this process each 24 hours.

NTP Server

The name or IP address of the NTP server to be used. If a host name is used, a DNS server address must be configured. There is a free, open NTP server available at the address us.pool.ntp.org .

Time zone

NTP servers report the time in Coordinated Universal Time (UTC). If you wish to convert UTC time to your local time, you must specify the timezone. If your timezone is not in the preconfigured list you may select *other TZ* then encode your timezone in the following field.

Other Time Zone

The timezone is encoded as follows:

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

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

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

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

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

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

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

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

```
Mm.n.d
```

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

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

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

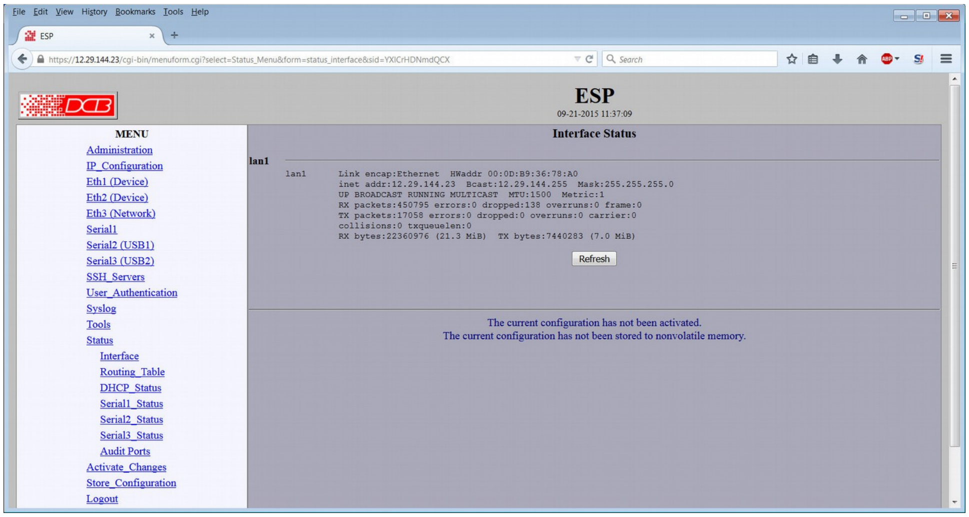
As an example, US Central time is 6 hours behind UTC during standard time and 5 hours behind UTC during daylight savings time. Daylight savings time takes effect the 2nd Sunday in March at 2am. Standard time resumes the 1st Sunday in November at 2am. It would be encoded as follows:

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

Notes

If possible, use of NTP is strongly recommended to insure an accurate clock.

Interface Status



ESP

09-21-2015 11:37:09

Interface Status

lan1

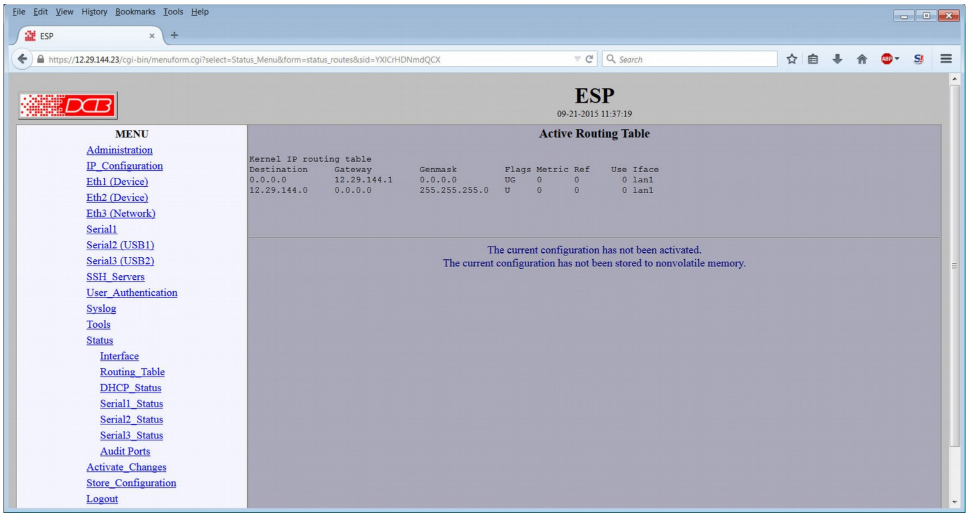
```
lan1      Link encap:Ethernet  HWaddr 00:0D:B9:36:78:A0
          inet addr:12.29.144.23  Bcast:12.29.144.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:450795 errors:0 dropped:138 overruns:0 frame:0
          TX packets:17058 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22360976 (21.3 MiB)  TX bytes:7440283 (7.0 MiB)
```

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Interface Status Screen

The Interface Status screen shows port status and packet counters for each ethernet interface.

Routing Table



ESP

09-21-2015 11:37:19

Active Routing Table

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         12.29.144.1     0.0.0.0         UG    0      0        0 lan1
12.29.144.0     0.0.0.0         255.255.255.0   U     0      0        0 lan1
```

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Routing Table Screen

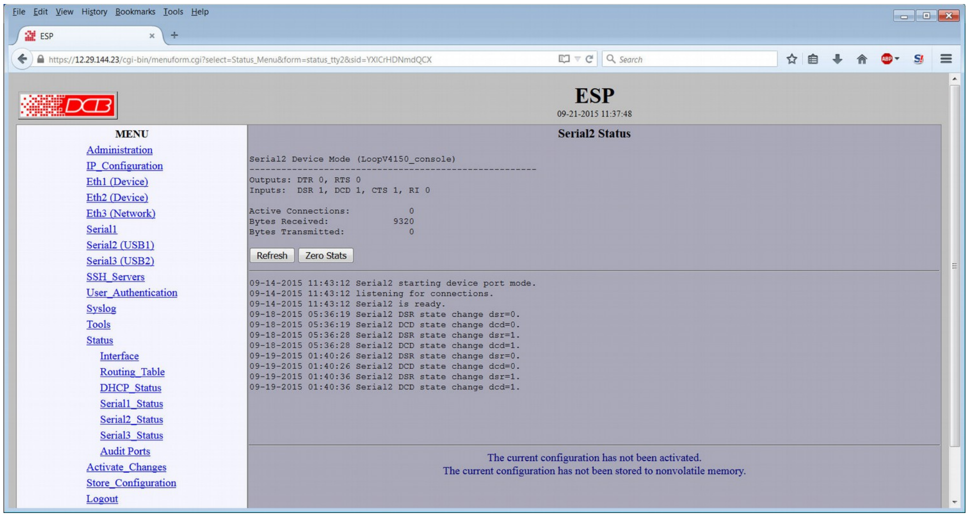
The Routing Table screen shows all routes configured in the ESP.

DHCP Status

DHCP Status Screen

The DHCP Status Screen displays DHCP status if DHCP is enabled on the ESP.

Serial Status



ESP

09-21-2015 11:37:48

Serial2 Status

```
Serial2 Device Mode (LoopV4150_console)
-------------------------------------------------------
Outputs: DTR 0, RTS 0
Inputs:  DSR 1, DCD 1, CTS 1, RI 0

Active Connections:           0
Bytes Received:            9320
Bytes Transmitted:            0
```

```
09-14-2015 11:43:12 Serial2 starting device port mode.
09-14-2015 11:43:12 listening for connections.
09-14-2015 11:43:12 Serial2 is ready.
09-18-2015 05:36:19 Serial2 DSR state change dsr=0.
09-18-2015 05:36:19 Serial2 DCD state change dcd=0.
09-18-2015 05:36:28 Serial2 DSR state change dsr=1.
09-18-2015 05:36:28 Serial2 DCD state change dcd=1.
09-19-2015 01:40:26 Serial2 DSR state change dsr=0.
09-19-2015 01:40:26 Serial2 DCD state change dcd=0.
09-19-2015 01:40:36 Serial2 DSR state change dsr=1.
09-19-2015 01:40:36 Serial2 DCD state change dcd=1.
```

The current configuration has not been activated.
The current configuration has not been stored to nonvolatile memory.

Serial Status Screen

This screen displays statistics and a log file for the serial ports.

Fields

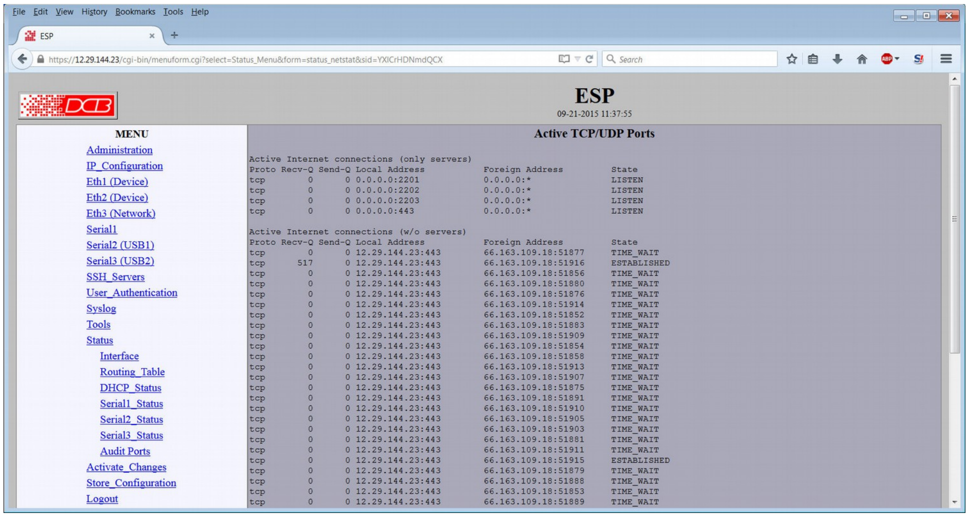
- **Display Fields**
  Serial port RS-232 interface status and counters are displayed.

- **Refresh (Click Button)**
  Refresh the screen display

- **Zero Stats (Click Button)**
  Zero the displayed statistics.

- **Serial Log display Fields**
  A log showing serial port connection activity

Audit Ports



ESP

09-21-2015 11:37:55

Active TCP/UDP Ports

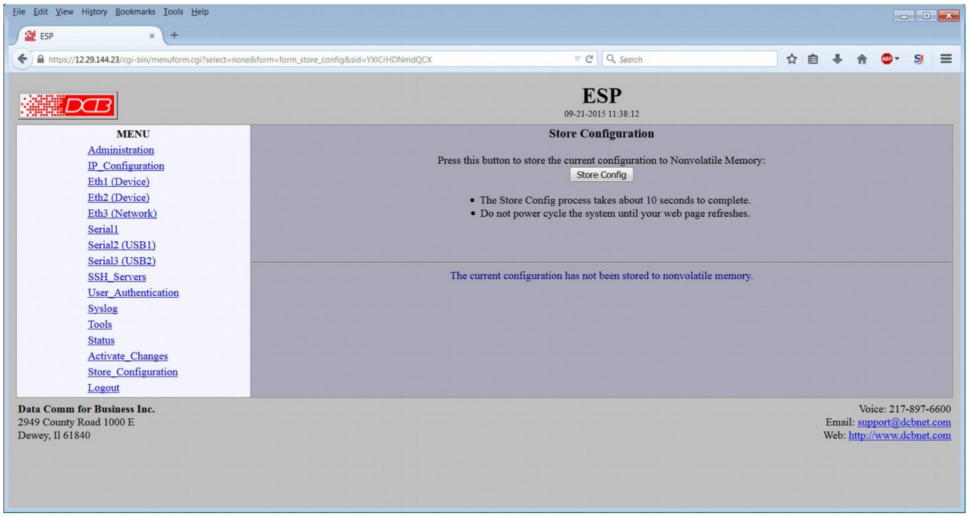
```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:2201            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2202            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2203            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN

Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 12.29.144.23:443        66.163.109.18:51877     TIME_WAIT
tcp      517      0 12.29.144.23:443        66.163.109.18:51916     ESTABLISHED
tcp        0      0 12.29.144.23:443        66.163.109.18:51856     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51880     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51876     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51914     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51852     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51883     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51909     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51854     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51858     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51913     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51907     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51875     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51891     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51910     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51905     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51903     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51881     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51911     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51915     ESTABLISHED
tcp        0      0 12.29.144.23:443        66.163.109.18:51879     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51888     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51853     TIME_WAIT
tcp        0      0 12.29.144.23:443        66.163.109.18:51889     TIME_WAIT
```

Audit Ports Screen

This screen shows active Active Internet connections (with and without servers).

Store Configuration



ESP

09-21-2015 11:38:12

Store Configuration

Press this button to store the current configuration to Nonvolatile Memory:

- The Store Config process takes about 10 seconds to complete.
- Do not power cycle the system until your web page refreshes.

The current configuration has not been stored to nonvolatile memory.

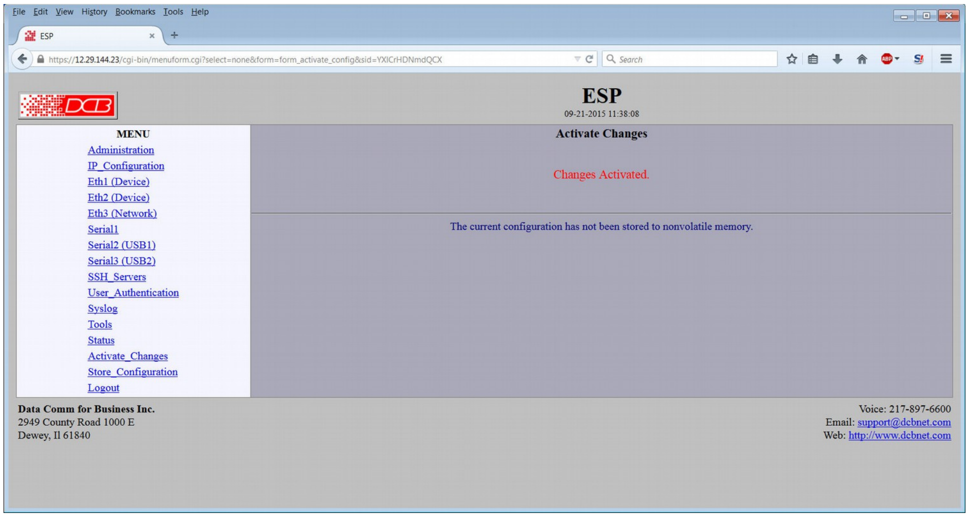
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

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



ESP

09-21-2015 11:38:08

Activate Changes

Changes Activated.

The current configuration has not been stored to nonvolatile memory.

Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

Voice: 217-897-6600
Email: support@dcbnet.com
Web: http://www.dcbnet.com

Activate Configuration Screen

The Activate configuration screen is used to activate the current changes. Configuration changes are made to a temporary area as the **Submit Screen** buttons are clicked, but are not actively running the ESP. Upon Activation, these changes will become immediately active, overwriting the pre-existing configuration for the duration of this session. Changes may be “stored” using the store configuration screen, in which case they will be written to non-volatile memory and used at the next reset or power-up.

Chapter 5

Operation

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

Common Uses – Overview

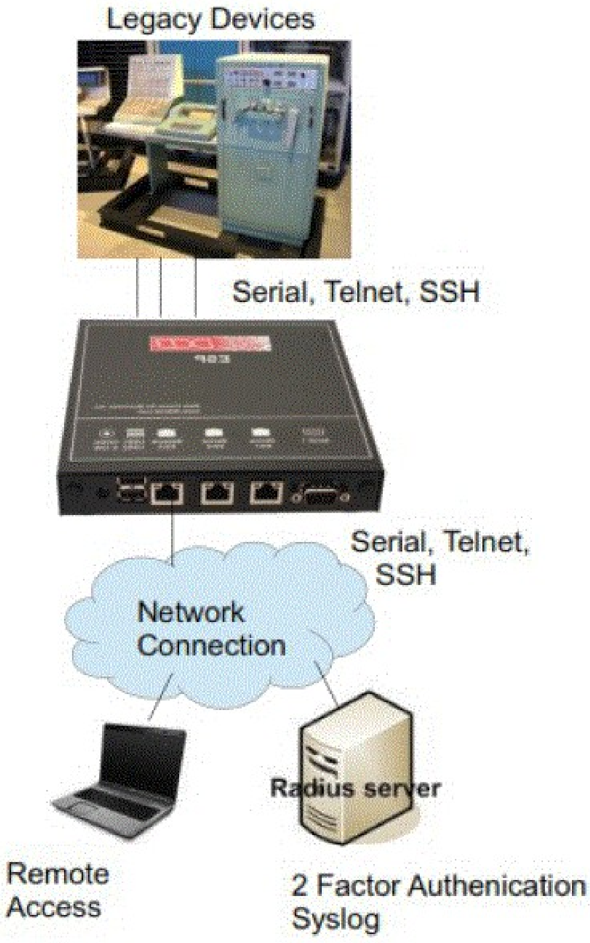
In an **ethernet protection application,** the ESP is installed between the local ethernet network (typically connected to Eth3) and the equipment to be protected (typically connected to Eth1). It's then configured as a transparent firewall containing black-hole features, as a RADIUS enabled front-end authentication box, or as a SSH front end to the protected equipment's telnet port. Authentication and logging may be local or remote.

For a **serial protection application**, the ESP is installed between the equipment to be protected and the incoming serial line. It provides logging, authentication, and serial "firewalling" to protect the RS-232 serial interface.

In both of those typical installations, the ESP uses a remote RADIUS server for centralized authentication or an optional local authentication database. In all installations, the ESP can be configured for remote syslog logging of an audit trail or maintenance of a temporary local log.

The ESP can also be configured to allow **SSH access to the legacy equipment's serial interface via ethernet**. In many cases, this option will allow the removal of vulnerable telephone modem lines since more secure ethernet is often being installed in CIPS locations.

An illustration of a typical installation is shown on the next page:



Typical Installation

Untrusted LAN to Device LAN Protection

In an **ethernet protection application,** the ESP is installed between the local ethernet network (typically connected to Eth3) and the equipment to be protected (typically connected to Eth1). It's then configured as a transparent firewall containing black-hole features, as a RADIUS enabled front-end authentication box, or as a SSH front end to the protected equipment's telnet port. Authentication and logging may be local or remote.

Protecting a Serial Port on Legacy Equipment

For a **serial protection application**, the ESP is installed between the equipment to be protected and the incoming serial line. It provides logging, authentication, and serial "firewalling" to protect the RS-232 serial interface. In many cases, this option will allow the removal of vulnerable telephone modem lines since a more secure ethernet is often being installed in CIPS locations. The ethernet connection allows Radius authentication and remote syslog features. When using two serial ports, one USB to serial cable is required.

User SSH with Legacy Telnet Server Devises

The ESP can also be configured to allow **SSH access to the legacy equipment's ethernet telnet interface**.. One ethernet port is used for incoming connections, a second ethernet port is connected to the equipmnent under protection, and one ethernet connection (which may be shared with the incoming network) allows Radius authentication and remote syslog features.

Typical Application Diagrams

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 ESP still does not function properly, please contact your vendor or DCB technical support for assistance. **DCB technical support contact information is displayed near the bottom on every configuration screen.**

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 ESP connected. If it is off, make sure the network cable between the ESP 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 ESP correctly ie. https:// instead of http:// .
- Start troubleshooting from a known state. Power the ESP OFF and ON to reboot.
- Is a proper IP address configured in the ESP and PC? Same subnet?
- "Ping" the ESP 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 ESP (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 ESP have compatible IP addresses.**
- It may be that your workstation "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.**
- 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 (9600 8N1).
- Hold the configuration button depressed for at least 3 or 4 seconds.
- Power is available... an LED is on.
- The PC terminal program is operating properly. Try a loopback connector at the ESP 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, wrong COM: port, or the Windows Hyperterm program not operating correctly.

P: "Error 22" in the log file.
S: This indicates that an ethernet interface is down.

P: "Error 28" in the log file.
S: Usually displayed when there is no gateway configured and it's attempting to communicate with an off-subnet address.

P: "Error 101" in the log file.
S: There is a routing error. Most likely is an incorrect gateway and subnet mask.

How To Reset To Factory Defaults

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 address is 192.168.0.1 .

If you do not know the IP address, there are two methods, First, you may use the serial setup method described in chapter two of this manual.

Or a more convenient method is to boot the unit with a temporary factory configuration. This method uses the mode switch on the front of the unit. The mode switch is behind a hole in the front panel Use a small wire (paperclips work well) to press the button.

The process is to apply power to the unit.

The BIOS will illuminate all 3 LEDs, then turn off LEDs 2 and 3.

At this point, press and hold the mode switch until LED 2 is flashed (about 8 seconds later). You may then release the switch. The unit will be running on default values and the serial setup re-enabled.

Note: The default settings are not written to non-volatile memory. The user must store the settings from either the serial port or the web interface.

Appendix A

Specifications

ESP Security Appliance Specifications

- Security Modes: Password policy enforcement, Syslog support, Radius support, transparent firewal, SSH to telnet conversion, transparent firewall
- Authentication modes: Local users file, Radius
- Logging: Local log file, syslog (Rsyslog)
- Ethernet Interfaces: Three ports configured as 10/100/1000BaseTx, Autosense
- Serial Port one RS-232 port, two USB ports (suitable for USB-to-RS-232 conversion cables) Speeds 300bps to 115.2 Kbps
- OS: Embedded Linux
- CPU: Dual core gigabit X86 processor
- Standalone or DIN mounting
- Dimensions :6.61” x 6.18” x 1.18”
- One Pound
- Power: 12 VDC 12 watts supplied with 100-240 VAC external supply (optional power supplies available)
- LED: Power, Status, LAN Activity(per port), LAN speed(per port)
- Default LAN IP address: 192.168.0.1
- Browser Management port: 443 (HTTPS)
- Operational Temperature -20C to +70C

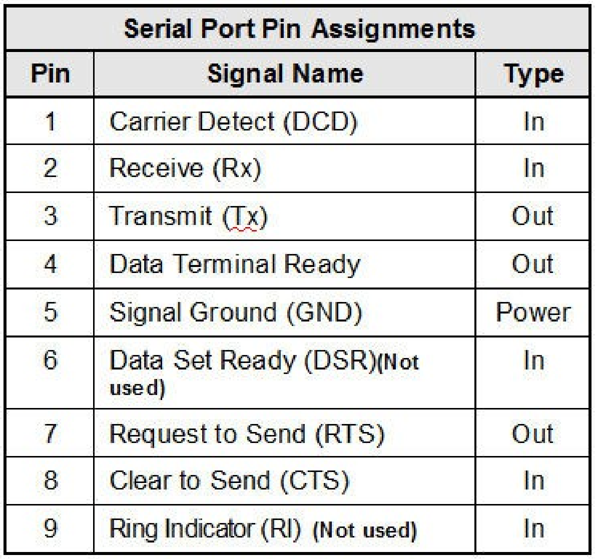
Cables

ESP to hub or ethernet switch

Use any commercially available 10/100BaseT cable. If using 100BaseT or 1000BaseT, an appropriately rated cable is required. Ports are MDI/MDI-X so crossover cables are not required.

RS-232 Interface

Cabling required depends upon the device being connected.   The DE-9 (PC 9-pin) RS-232 serial port configuration is configured for DTE.



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

RS-232 Port Pin Assignments

Control Signal Operation

DCD

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

Receive Data

Input, data into the bridge

Transmit Data

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

DTR

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

Signal Ground

Common ground

DSR

Input. Ignored

RTS

Output. Input flow control. When the internal buffer reaches the “Flow Off” buffer level, this signal is lowered. When the buffer level decreases to the “Flow ON” buffer level, this signal is raised. When pin 8 input is LOW, the serial interface turns OFF the pin 4 (DTR) and 7 (RTS) output signals.

CTS

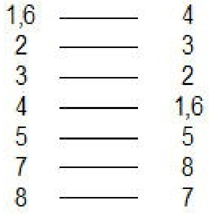
Input. When Flow Control is set for CTS/RTS, lowering this signal will halt data flow from the bridge's RS-232 port.

Ring Indicator

Not used

PC 9-pin COM: port

Since the 9-pin DE-9 connector is identical to a PC COM: port connector pinout, either a straight-through or null-modem cross-over cable is normally used.



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

Null-Modem Cable Pinout

USB serial cable

USB serial cable pin out depends upon the USB serial cable adapter used.

Appendix B

Open Source Software Information

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

Introduction

Some models of the ESP were designed and programmed with Open Source Linux software in mind. The core Linux operating system is available from http://www.linux.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. There is an "about" screen on each product that details which open source projects are in use.

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

Application Examples

The ESP appliance can be used in numerous ways to increase the security of legacy products.   These are some of the most commonly used topologies.

Introduction