PMT-Series

Encrypted Ethernet Tunnel

Product Family

User's Guide

Revised September 20, 2007

Firmware Version 1.x

FCC Statement

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

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

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

Version 1.x

RoHS 6/6 COMPLIANT

RoHS - the entire PMT-6601 hardware is RoHS compliant except the CF card. However a RoHS CF card is used when 6/6 compliance is required.

TABLE OF CONTENTS

Chapter 1

Introduction

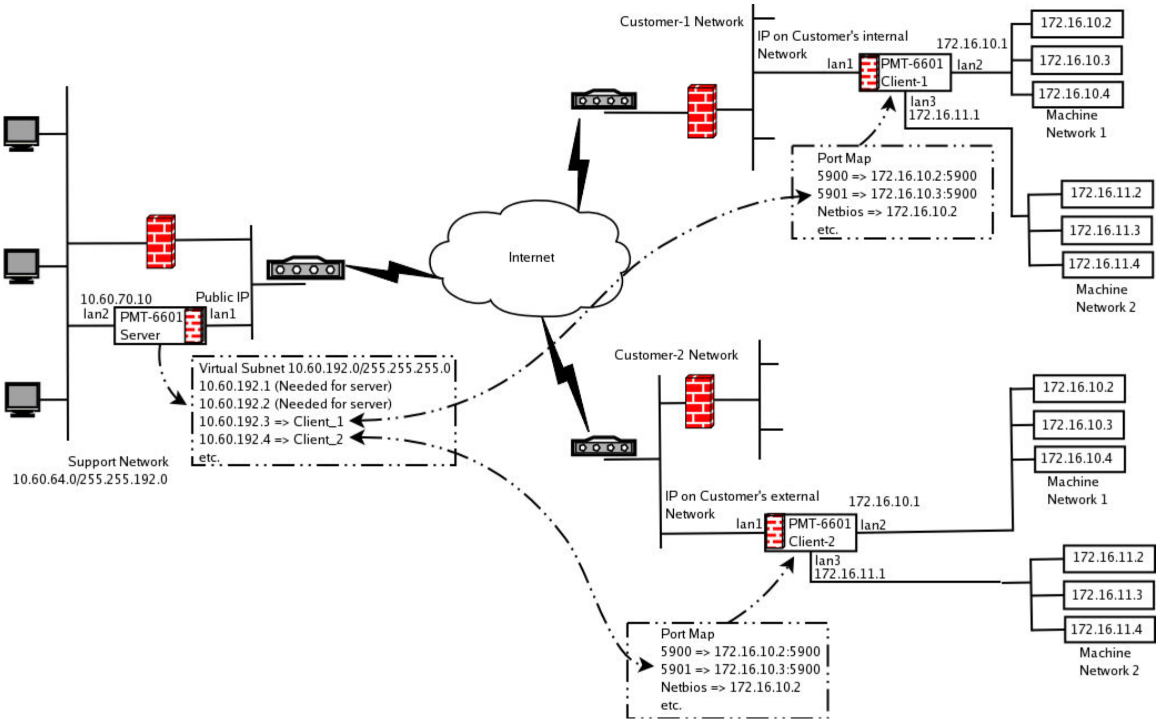
This chapter provides an overview of the PMT Port Mapping Tunnel's features and capabilities.

Congratulations on the purchase of your new PMT Encrypted Ethernet Tunnel. This is a simple, easily configured multi-point tunneling device with three 10/100BaseT Ethernet interfaces. It's primary use is in large dispersed networks, where access to individual remote IP devices is required from a host site, yet strict security needs to be enforced at that host site.

PMTs connect using standard UDP/IP over any insecure IP connection path,. They tunnel IP packets from the secure interface of each device to the other devices. The PMTs unique NAT mapping and filtering features allow easy setup for large, multi-site private networks connected via the public Internet.

Unlike other tunneling bridges (such as DCB's ET family), the PMT restricts data flow severely. It allows only packets destined for a specific port on a specific machine node located behind the remote PMT devices. Packets originated at the remote sites, even if from an allowed node, are not allowed back into the host site.

The connection between remote sites is a VPN-like tunnel, encrypted using the AES algorithm.



Typical PMT Application

The PMT is commonly used for remote support of equipment using IP protocols. Example applications include machine tools using CNC controllers, large printing presses, MRI machines, PCs used in point of sale applications, security controllers and other PC based applications.

The PMT operates by creating a hardware based VPN tunnel between the host site PMT unit and one or more remote site PMT devices. This connection is encrypted using the AES algorithm, and provides privacy between the PMT units. Maps which are configured into the PMT devices redirect IP connections from the host site to individual machines on the back side of remote PMT devices. Although communications are two-way, all communications between user devices must originate at the host location. This prevents any nodes on the remote LAN from accessing the host LAN segment.

A typical use would be to enable technicians at the host site to maintain remote equipment using SMB file transfers, remote terminal operations, VNC, or windows remote support applications. The system also allows automated file "pulls" from remote devices such as point of sale PCs and registers and the ability to push update files and firmware out to remote devices.

The PMT port mapping feature allows multiple sites to use standard hardware configurations with identical IP addresses at the end nodes. For example, every remote site might have the first controller addressed as 10.1.1.1 , and the second one at 10.1.1.2. The PMT configuration map will translate packets destined to each device to a virtual subnet address on the host LAN. Each remote site will have different mapping, which allows the use of standard end node hardware configurations.

Other Features

Remote (client) units configurable with DHCP

The client units may be configured manually, or obtain the public IP addressing information via DHCP servers.

Protocols

All IP protocols are supported. It does not pass IPX, AppleTalk, and other non-routable protocols.

Upgradeable Firmware

Firmware upgrades may be installed using any web browser.

Security and Firewall Features

The PMT supports a number of security features. On the "insecure" side, communications between clients and servers is through the SSL/TLS protocol. The encryption methodology is industry-standard 128 bit AES. Only workstations on the "secure" side of a unit may be used to configure or control it.

On-board Tools

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

Package Contents

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

- The PMT hardware
- Power Adapter or AC cord
- This User's Guide CDROM

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

Software Requirements

The bridge supports IP and associated protocols such as UDP, ICMP, DHCP, and any protocol built upon IP or TCP/IP**.** The initial IP address may be entered using any terminal or terminal emulation software on a PC, or by using a properly configured web browser.

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

PMT-6601 Specific – Three High Performance Ports

The PMT-6600 family consists of various models with different internal hardware or firmware options. The ET-6601 includes three 10/100BaseT High Performance Ethernet ports.

Introduction

The PMT-6601 contains three 10/100BaseT Ethernet ports.

Basic Configuration

This model contains a single serial interface to be used in initial setup (if needed). This serial port is available for setup by pressing the escape key once upon bootup after hearing two beeps from the unit. . Once a compatible IP address is available, the browser setup screens are much easier to use.

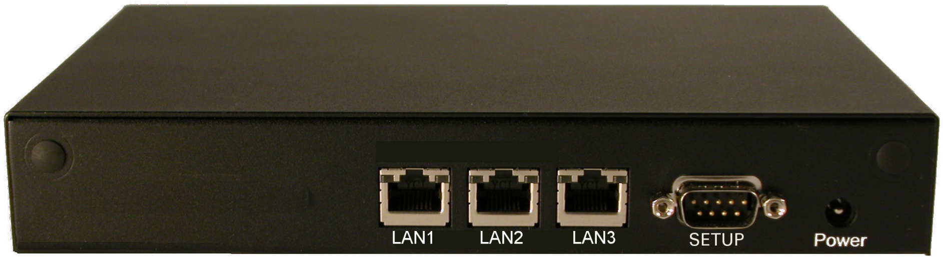
PMT-6601 Front Panel

PMT-6601 Front Panel

The front panel contains LED indicators for ethernet port activity, port link, power, and virtual disk activity.

PMT-6601 Rear Panel

The rear panel contains three 10/100BaseT ethernet ports (two trusted, one untrusted), console DE-9P (PC 9-pin) console port, and power input.



PMT-6601 – Rear Panel

Chapter 2

Installation

This Chapter details the installation process for the PMT6601.

Overview

The PMT is normally configured using a web browser directed to its address. If the LAN 2 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 PMT (without using a proxy) and continue with configuration. The unit may be configured using LAN 2 or LAN 3. The LAN 3 default IP address is 192.168.3.1 . If these addresses are not appropriate for your network, the IP address must be configured using the initial terminal method below.

The remote PMT units may be pre-configured and centrally managed for remote plug and play operation.

The CDROM contains more detailed step-by-step instructions for a commonly used configuration. Printing that document and using it is highly recommended, and will save time when first configuring the units. This configuration is also contained in an appendix to this document.

Quick Start

Quick start instructions are in the following section. Installation is an easy process, but you are must have a thorough understanding of IP networking, subnetting, and routing. You should have a network diagram illustrating IP addresses, subnetting, and all IP routing that you intend to use prior to configuration and installation.

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.

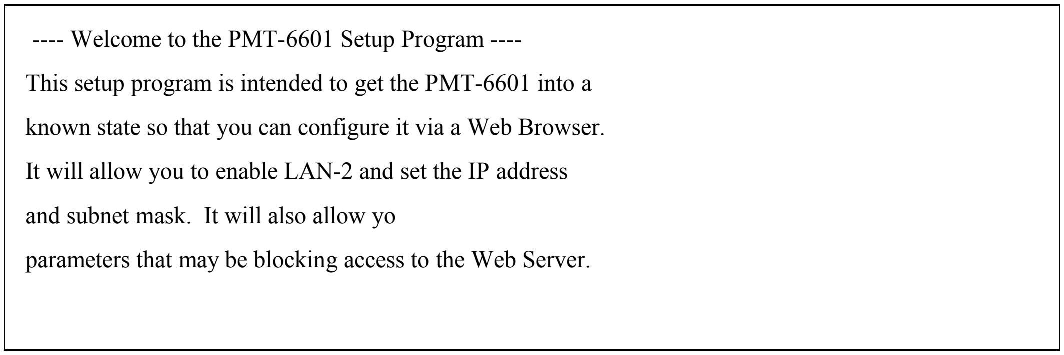
Entries are always tested for valid values. However, there are many "valid" values that are not appropriate for any given configuration. So, "appropriateness" isn't tested. For example, an IP address of 300.400.500.256 will not be accepted, but the field will accept an IP address that is not appropriate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

Installation and Configuration

1. Configure the server's IP address

If the PMT's default address (192.168.0.1) is appropriate for your network, skip to step 2, "Connect the Ethernet Cable".

1. Connect a terminal or PC running terminal emulation program (Hyperterm, Procomm, etc) to the serial port of the PMT.
2. Start the terminal emulation program using 9600 bps, 8-bits, No parity, No flow control.
3. Power up the PMT. Wait for the PMT to sound two beeps. Then press the escape key on your keyboard one time. The prompts will then display on the screen. I

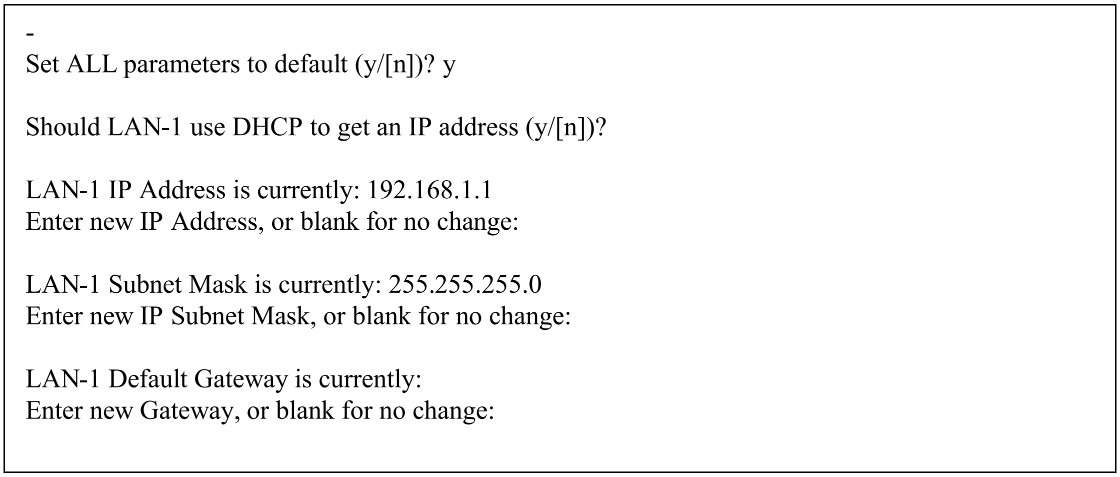


```
 ---- Welcome to the PMT-6601 Setup Program ----
This setup program is intended to get the PMT-6601 into a
known state so that you can configure it via a Web Browser.
It will allow you to enable LAN-2 and set the IP address
and subnet mask.  It will also allow yo
parameters that may be blocking access to the Web Server.
```

Login Screen

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

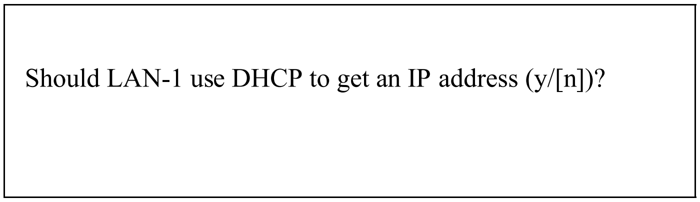
5. You will then be asked if you wish to set ALL parameters to factory defaults. If you have previously changed any values and want to return to the factory defaults, answer “Y”, otherwise answer “N”.



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

Should LAN-1 use DHCP to get an IP address (y/[n])?

LAN-1 IP Address is currently: 192.168.1.1
Enter new IP Address, or blank for no change:

LAN-1 Subnet Mask is currently: 255.255.255.0
Enter new IP Subnet Mask, or blank for no change:

LAN-1 Default Gateway is currently:
Enter new Gateway, or blank for no change:
```

Default Screen

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



```
Should LAN-1 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 an IP address, gateway, and subnet mask for each ethernet interface. Enter the values as required.

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

```
Saving Configuration. Do not cycle power...

Setup complete.

After rebooting the system, you will be able to configure
the unit from a Web Browser via LAN-2.  Use the URL http://192.168.0.1
press <enter> to reboot system...
```

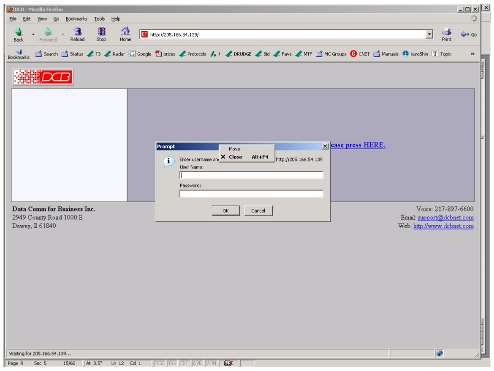
9. The PMT will now reboot.

2. Connect the Ethernet Cable

Connect a LAN cable from your hub or switch to LAN 2. Reboot with a power cycle. The PMT will now be available to any web browser on the same LAN segment. If your web browser does not see it, verify that you do not have a proxy server configured in the browser. If so, properly configure the browser to bypass the proxy server for this URL. The PMT's LAN 2 default address is 192.168.0.1. This address must be appropriate for your local LAN and workstation, or step 1 above must be followed.

3. Verify the IP Address Configuration

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



http://205.166.54.139/

Enter username an[d] ... http://205.166.54.139

User Name:

Password:

ease press HERE.

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

Waiting for 205.166.54.139...

Login Screen

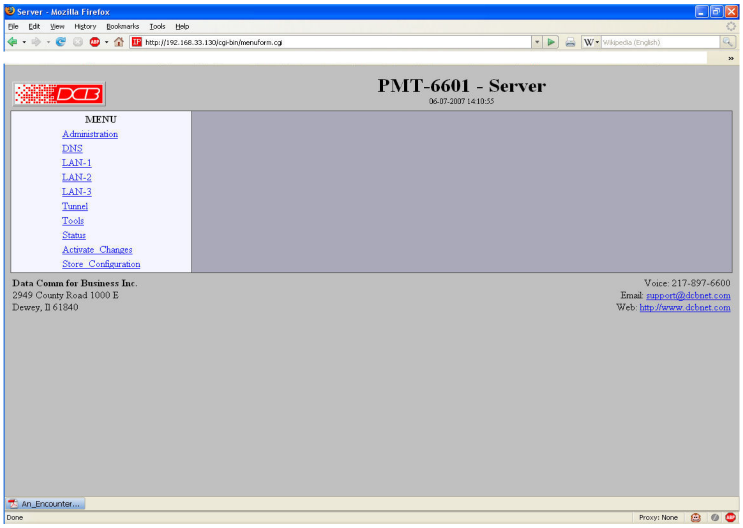
Log in using the user name "admin" and no password (blank field). If this screen doesn't display, check the Troubleshooting Section in Chapter 6.

4. Enter Your Configuration

Initial Main Menu

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

5. Minimum Configuration



http://192.168.33.130/cgi-bin/menuform.cgi

PMT-6601 - Server
06-07-2007 14:10:55

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

The minimum configuration items required for basic operation are:

For the Server Unit:

1. Secure side ethernet configuration. Configure ethernet port LAN 2 (IP address, etc.).

2. Insecure (public) side ethernet port (LAN 1) configuration. This must be a publicly accessible IP address that the remote units can connect to.

3. Tunnel mode, server configuration, and remote users map.

Configure these items and the PMT server is ready for use.

For the Client Units:

4. Secure side ethernet configuration. Configure ethernet port LAN 2 (IP address, etc.).

5. Insecure (public) side ethernet port (LAN 1) configuration. This may be supplied by DHCP, but it must have a route back to the server unit's public IP address.

6. Tunnel mode, client configuration, and port forwarding map. Virtual servers (if used).

Configure these items and the PMT client is ready for use.

Chapter 3

The Configuration Process

This Chapter describes the configuration management process on the PMT-Family products using a Web Browser.

Overview

This product contains a quite 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 and configuration changes to it.

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

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

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

Using the Configuration Flexibility

When starting from a power-off condition, it loads an active configuration from its non-volatile memory. This active configuration is also copied to the working memory and is the "active" configuration.

Whenever the configuration screens are used to change values, **only** the *pending* configuration is changed… not the *active* configuration.

Using the configuration screens will change the pending configuration. You may change the active configuration by copying the pending configuration over it. This change is performed using the "Activate Configuration" screen. Going to this screen activates the pending configuration by copying the pending configuration over the top of the active configuration.   This does not store the configuration in non-volatile memory. When the unit is next reset or powered up, it will begin using the old stored configuration from before the changes were made and activate command clicked.

Using the "store configuration" screen will copy the pending configuration into Non-volatile memory. It will not cause this configuration to begin running. However, upon the next reset or power cycle, the unit will begin using the stored configuration.

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

Configuration Process Examples

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

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

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

This method allows one to configure without actually using the new configuration. Make the changes to the pending configuration and save them. Your current session will not be affected, but when reset, the new configuration will be used. This method is useful when you are configuring to use a new LAN address range while still on the old LAN.

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

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

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

Note regarding saved configurations

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

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

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

Note that site names and passwords are stored in the clear in this configuration files. These files should be protected from unauthorized access.

Chapter 4

Configuration

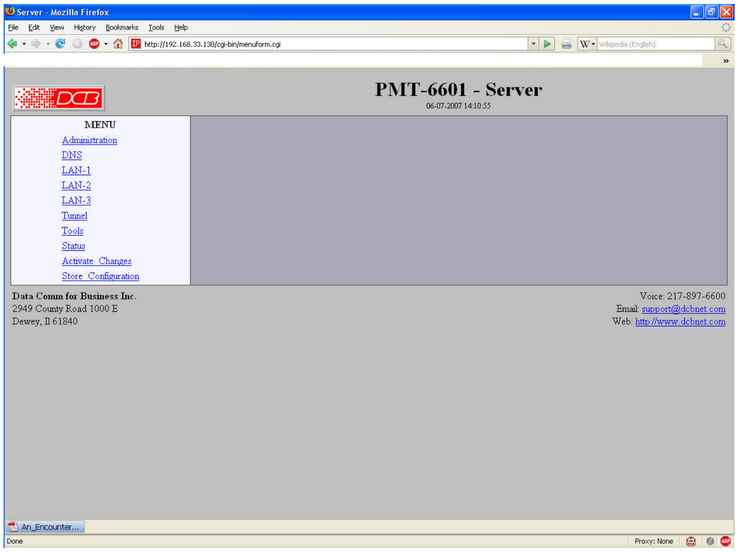
This Chapter describes configuration screens and some configuration hints for the PMT_6601.

Overview

The PMT-6601 is configured using forms displayed on a web browser. In this chapter, we illustrate all entry forms, and describe their use. This is not a tutorial on IP, bridging, or routing. Familiarity with IP and related information is required before you can configure any ethernet product.

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

Configuration screens should only be made available via the secure interface. This default operation may be changed during configuration or testing, but it is highly recommended that configuration be locked to the secure interface.



PMT-6601 - Server

06-07-2007 14:10:55

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

PMT-6601 Main Screen

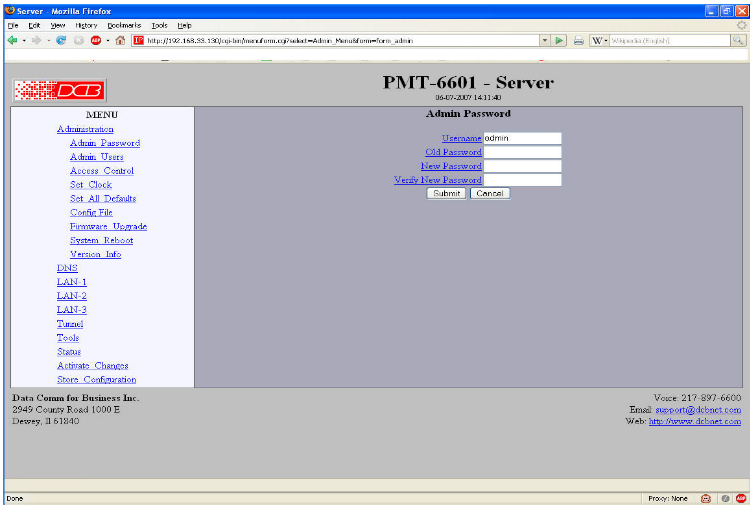
From this index, click on a menu keyword to open the appropriate screen. In this manual, screens are discussed in the order shown on the index screen.

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



PMT-6601 - Server

06-07-2007 14:11:40

Admin Password

Username admin

Old Password

New Password

Verify New Password

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

Admin Password Screen

The web server screens should be available ONLY via the secure side of the PMT. This is configurable using the Admin Access Control Screen.

Access to the Web Server Configuration screens is protected by HTTP Basic Authentication. This is a simple methodology where the Web Server will require a Web Browser to provide a user name and password for each page requested. The Web Browser will typically ask the user to enter the user name and password once, then will remember it for the duration that the Web Browser is running.

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

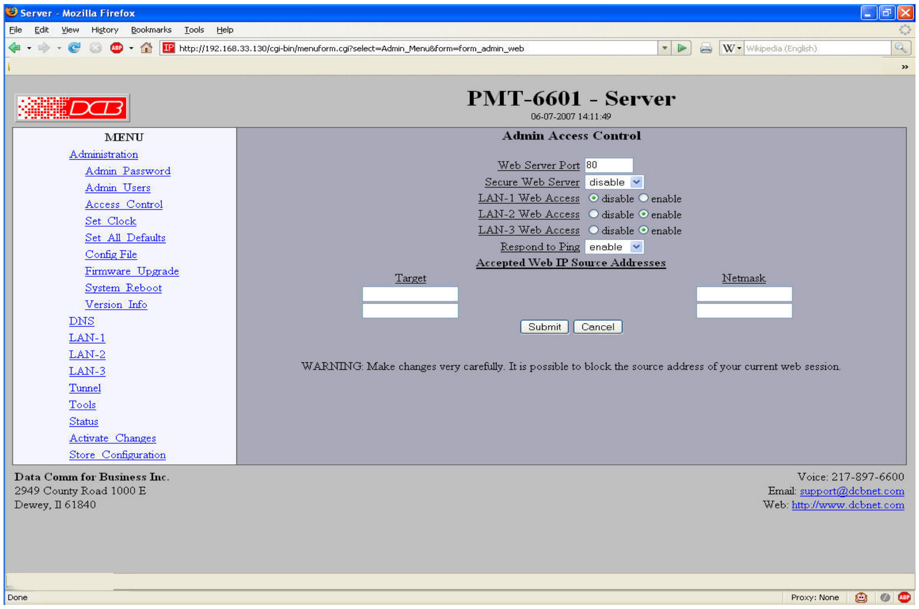
Fields

- User Name
  This field may be a string of 0 to 15 printable characters. Do not use space or control characters. If you leave this field blank, you will need to enter a blank username during authentication.
- Old Password
  In order to change the username and password, you must know the old password. When making a change, enter the current password in this field.
- New Password
  When changing the username and password, this field provides the new password. It may be a string of 0 to 15 characters. If you leave this field blank, you will need to enter a blank password during authentication.
- Verify New Password
  Retype the password to verify that it was correctly entered.

Notes

- If you forget your username or password, you can use the Serial Port Setup to erase the current settings and return the unit to factory defaults.
- Security Note: HTTP Basic Authentication may be easily hacked if the attacker has the ability to sniff network packets. The username is transmitted in the clear and the password is transmitted in an obfuscated but possibly recoverable format. For this reason, configuration should only be available via the secure ethernet interface on the bridge. This operation is configurable via the Admin Access Control screen.

Admin Access Control



PMT-6601 - Server

06-07-2007 14:11:49

Admin Access Control

Web Server Port: 80

Secure Web Server: disable

LAN-1 Web Access: ● disable ○ enable

LAN-2 Web Access: ○ disable ● enable

LAN-3 Web Access: ○ disable ● enable

Respond to Ping: enable

Accepted Web IP Source Addresses

Target	Netmask

WARNING: Make changes very carefully. It is possible to block the source address of your current web session.

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

Administrative Access Control Screen

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

Fields

- Web Server Port
  This is the TCP Port to use for the PMT's internal Web Server. Typically it is set to port 80. However you may set it to any value between 1 and 65535.

  There are several reasons that you may want to change the web server port. By changing it to a non-standard value, you reduce the chance that a random attacker will find the web interface and attempt to break in. A different port may be needed to accommodate local firewalling.

  If you change the web server port number to any value other that 80, remember that you will have to include the port number in your URL. For example, https://192.168.0.1:7995 OR http://192.168.0.1:7995 .
- Secure Web Server
  The use of secure sockets web configuration is allowed and encouraged. If this is enabled, instead of

http://address, you must use https://address to access the configuration screens. It is much more secure than using the regular web server for configuration.

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

- Web Access
  These options allow you to block web access through the specified interface. If you are using the PMT across a public network, you are strongly advised to disable web access from the interface attached to the public network.

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

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

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

  Target: 192.168.10.0 Netmask: 255.255.255.0

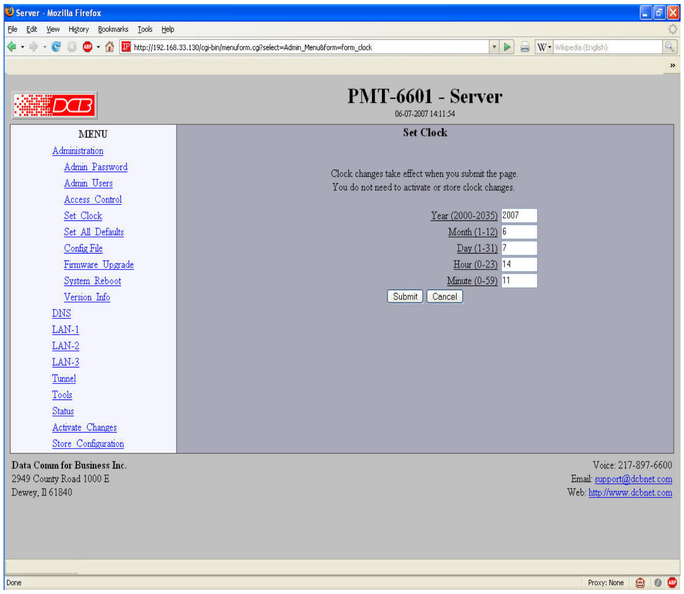
- Target
  Host or Network address.

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

Notes

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

Set Clock



http://192.168.33.130/cgi-bin/menuform.cgi?select=Admin_Menu&form=form_clock

PMT-6601 - Server

06-07-2007 14:11:54

Set Clock

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

Year (2000-2035) 2007
Month (1-12) 6
Day (1-31) 7
Hour (0-23) 14
Minute (0-59) 11

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

Set Clock Screen

This form allows you to set the software clock. The setting will take effect when you "Activate Changes".

Fields

Year Year in the range 2000 to 2035.

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

Day Day of month in the range 1 to 31.

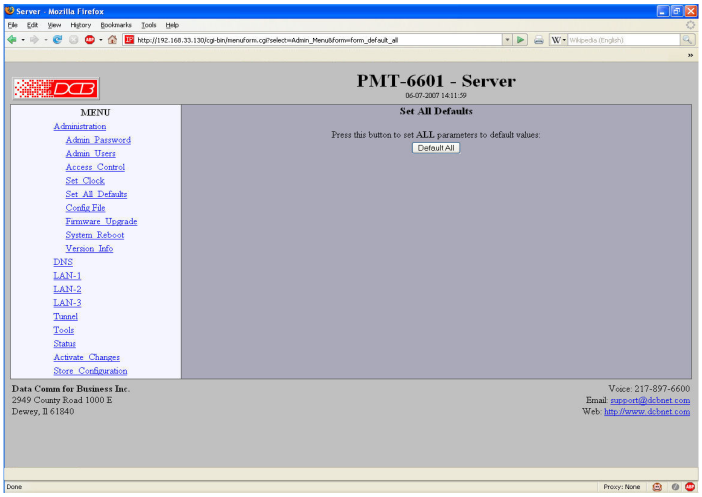
Hour Hour of the day in the range 0 to 23.

Minute Minutes in the range 0 to 59.

Notes

- If you save the time to non-volatile memory, the clock will be set to the specified time at each reboot.
- The unit does not contain a real-time clock, nor has the ability to remember the current time across reboots. The software clock is used for time stamping log entries.
- The default values shown on this screen are the “boot” values… not the current time.

Set All Defaults



PMT-6601 - Server

06-07-2007 14:11:59

Set All Defaults

Press this button to set ALL parameters to default values:

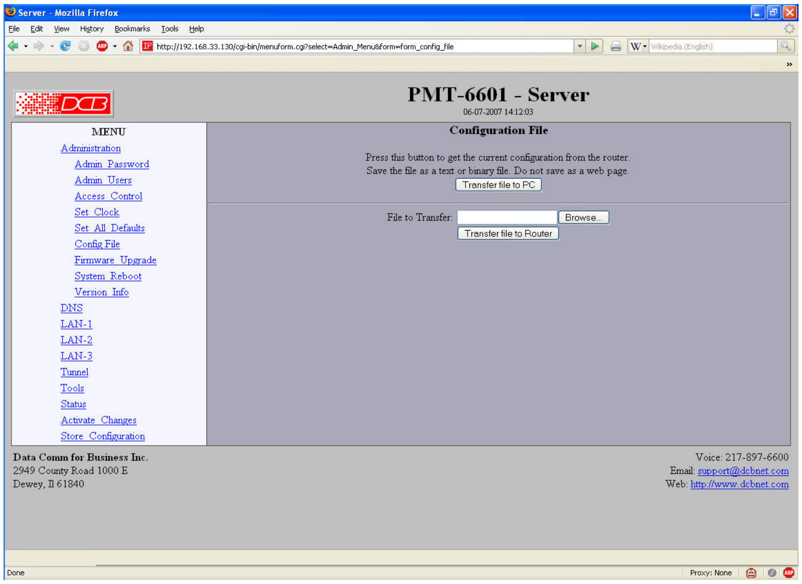
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

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

Set All Defaults Screen

This form will allow you to set all parameters to their default value. Before you "Activate Changes", you should configure the interface that you are using to access the tunnel. Otherwise, there may not be a valid TCP/IP route back into the unit.

Configuration File



PMT-6601 - Server

06-07-2007 14:12:03

Configuration File

Press this button to get the current configuration from the router.
Save the file as a text or binary file. Do not save as a web page.

File to Transfer:

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

Configuration File Screen

This form will allow you to copy the bridge's configuration to a file on your PC. You can also use the form to transfer a configuration file from your PC to the bridge.

Fields

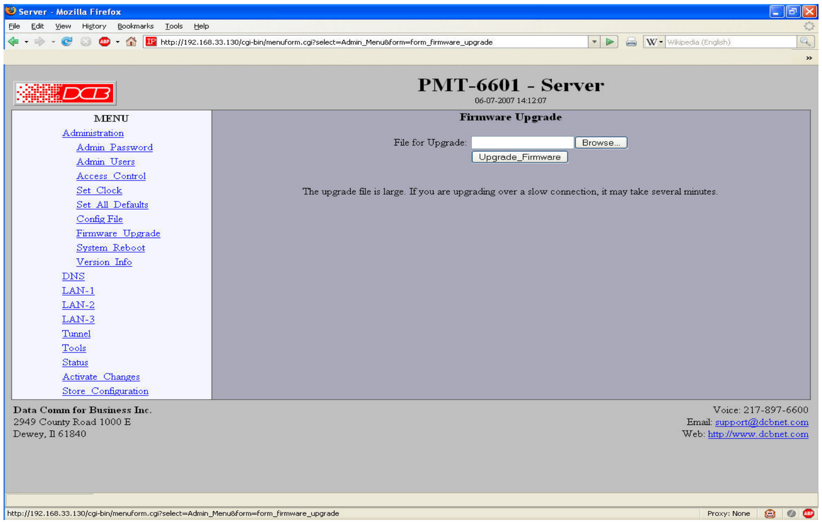
- File to Transfer
  This is the name of the configuration file on your PC to be transferred to the unit.

- Transfer file to PC (action)
  Transfers the current bridge configuration file to this PC.
- Transfer file to Bridge (action)
  Transfers the named file to the bridge.

Notes

- The configuration file is a specially formatted text file. It may be edited with any text editor.
- You may save multiple configuration files on the PC by using different names for them.
- After transferring a configuration file to the PMT, you may either activate the changes (with the activate screen), or store the changes (with the store configuration screen). If you activate the changes, it will immediately begin using the new configuration. If the changes are stored, it will use the new configuration only after a reboot or reset.
- If you activate the new configuration, first be sure that you can access the unit using its new configuration before storing it. Otherwise, it may be necessary to return to the old stored configuration with a reset.
- You must SECURE this text file on your PC with encryption, or move it to a secure place. Access to the saved configuration file may compromise the security of your system. Usernames and passphrases are stored in the clear in this file.

Firmware Upgrade



http://192.168.33.130/cgi-bin/menuform.cgi?select=Admin_Menu&form=form_firmware_upgrade

PMT-6601 - Server
06-07-2007 14:12:07

Firmware Upgrade

File for Upgrade:

The upgrade file is large. If you are upgrading over a slow connection, it may take several minutes.

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

Firmware Upgrade Screen

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

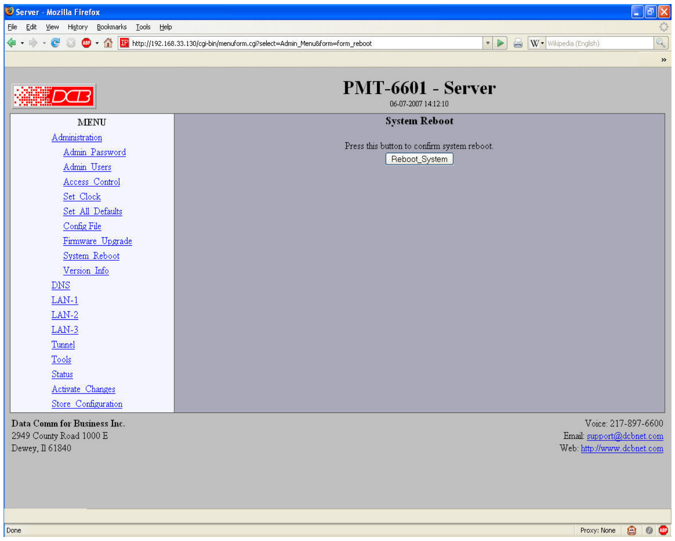
Fields

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

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



PMT-6601 - Server

06-07-2007 14:12:10

System Reboot

Press this button to confirm system reboot.

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

System Reboot Screen

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

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

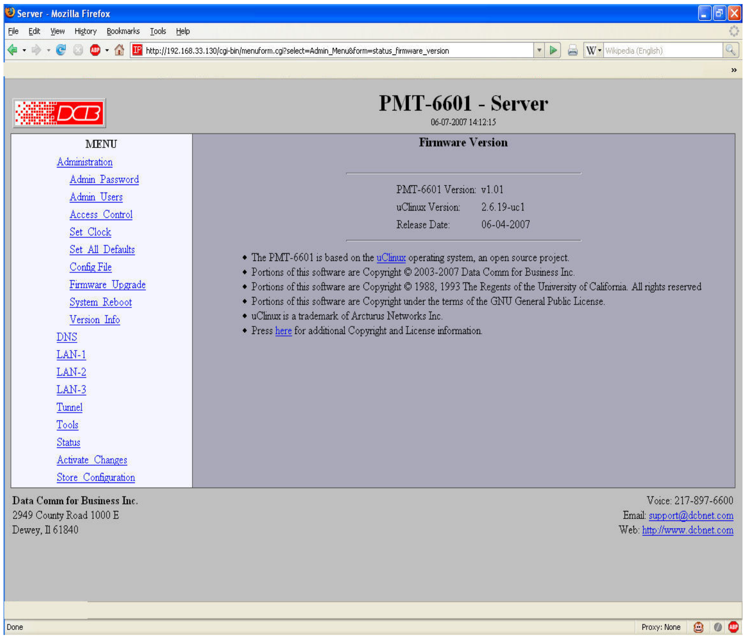
Fields

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

Notes

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

Version Information Screen



PMT-6601 - Server

06-07-2007 14:12:15

Firmware Version

PMT-6601 Version:	v1.01
uClinux Version:	2.6.19-uc1
Release Date:	06-04-2007

- The PMT-6601 is based on the uClinux operating system, an open source project.
- Portions of this software are Copyright © 2003-2007 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.
- uClinux is a trademark of Arcturus Networks Inc.
- Press here for additional Copyright and License information.

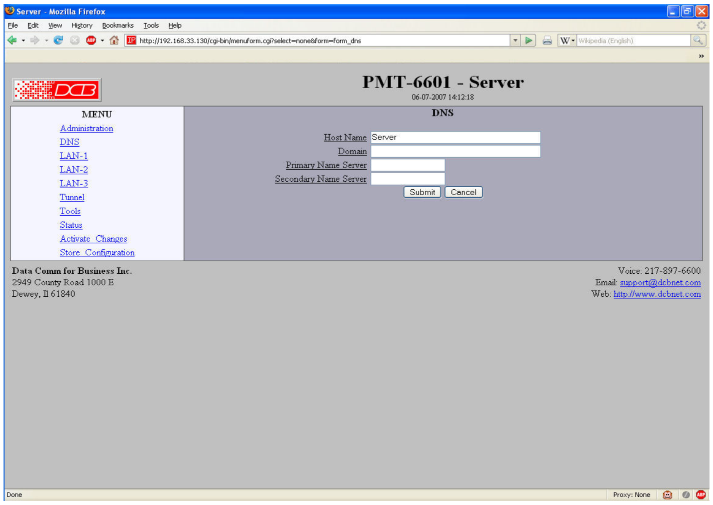
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

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

Version Information Screen

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

DNS



http://192.168.33.130/cgi-bin/menuform.cgi?select=none&form=form_dns

PMT-6601 - Server

06-07-2007 14:12:18

DNS

Host Name: Server

Domain:

Primary Name Server:

Secondary Name 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

DNS Screen

The Domain Name System, DNS, is a distributed database used by applications to map between IP addresses and hostnames. The PMT has support for the client side of DNS. It does not act as a DNS server. The DNS settings are passed to DHCP clients. Use of DNS is optional.

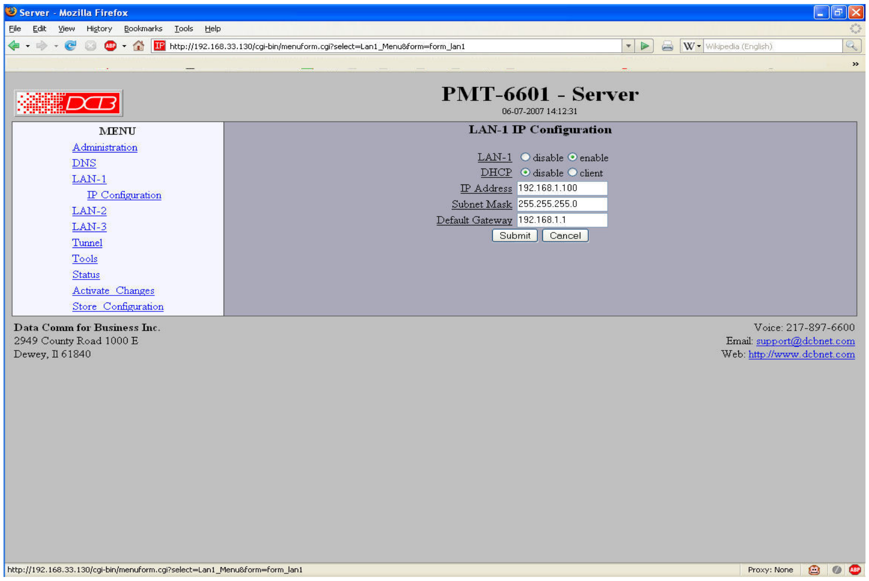
Fields

- HostName
  The name given to this hardware. If you enter a name, it will also be displayed on the title of the web pages.
- Domain
  The name of the local domain. For example: widgets.com
- Primary DNS Server
  The IP address of the primary DNS server. This value will be provided to DHCP clients users during option negotiation.
- Secondary DNS Server
  The IP address of the secondary DNS server. This value will be provided to DHCP clients during negotiation.

Notes

- The unit does not act as a DNS server.
- The DNS settings are passed to DHCP clients.
- Use of DNS is optional.

LAN -1/2/3 Configuration



PMT-6601 - Server

06-07-2007 14:12:31

LAN-1 IP Configuration

LAN-1 ○ disable ● enable

DHCP ● disable ○ client

IP Address 192.168.1.100

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

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 Configuration Screen

The PMT contains three Ethernet LAN interfaces. Depending upon the actual model, Ethernet-A is typically a higher speed 10/100 (or 10/100/1000) controller configured for auto-sense. Ethernet-B often is 10BaseT only. Ethernet port A is always the local, secure side of the tunnel. The public network interface may be either Ethernet port B, or a serial port. If used, Ethernet B is always the insecure side, and is usually used with a broadband WAN or public Internet connection. This screen is used to configure both IP parameters and DHCP server parameters (if the DHCP server function is used)

Fields

- Enable/Disable
  Each interface may be individually enabled or disabled. If you do not plan to use an interface, it is a good idea to disable it. Doing so will free up system resources.

- DHCP Fields
  Dynamic Host Configuration Protocol, DHCP, is a client/server protocol automating the configuration of systems using TCP/IP. Client systems will broadcast a request asking for configuration. Server systems will respond, assigning the client system an IP address and providing other related configuration information such as subnet mask, DNS, and gateway addresses.

  If you enable DHCP Client, the unit will request and IP configuration from a DHCP server. It is common to enable DHCP client on a broadband interface to an Internet Service Provider.

  When DHCP Client is enabled, the IP Address and Netmask fields are ignored. Only LAN-1 may be configured with DHCP.

- IP Address
  an IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. If you are directly connected to the Internet, it must globally unique.
  This field is not used if DHCP Client has been enabled for this port. The DHCP server will assign the IP address.

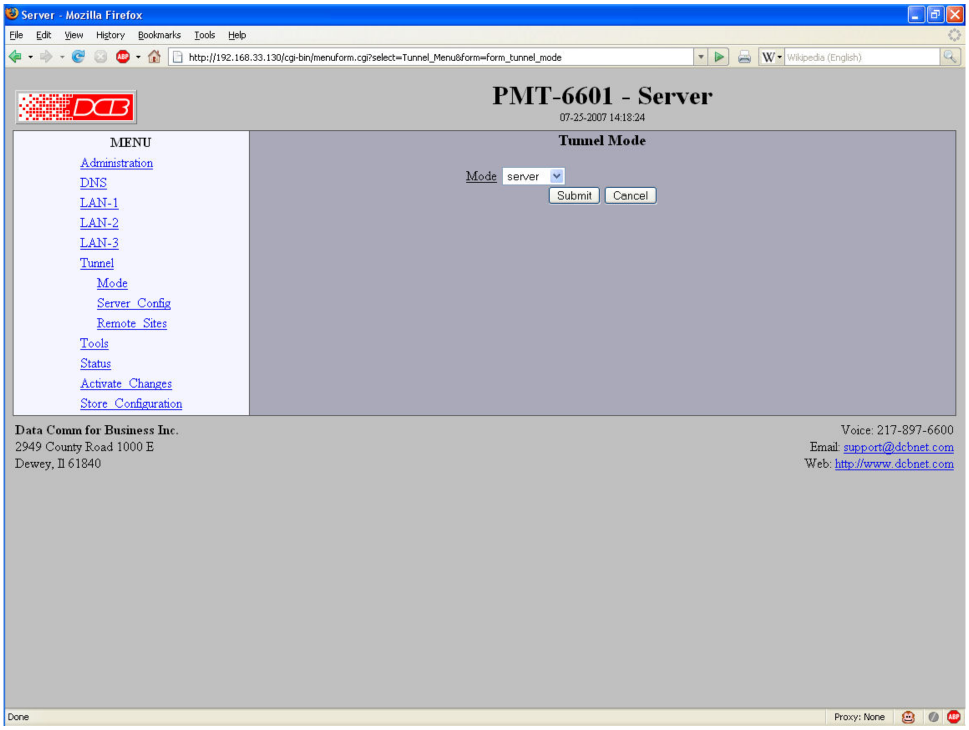
- Subnet Mask
  A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, many subnets have a mask of 255.255.255.0. This means the first 24 bits of the address is the subnet identifier and the last 8 bits is the host identifier.

  This field is not used if DHCP Client has been enabled for this port. The subnet mask will be assigned by the DHCP server.
- Default Gateway
  This is the default gateway. LAN-1 and LAN-2 have this configuration option. LAN-3 always uses the default gateway setting from LAN-2.

Notes:

- For maximum throughput, always disable unused interfaces.

Tunnel Mode



PMT-6601 - Server

07-25-2007 14:18:24

Tunnel Mode

Mode: 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

Tunnel Mode Screen

Fields

Tunnel Mode

The PMT may be configured odes: Disabled, Server, or Client.

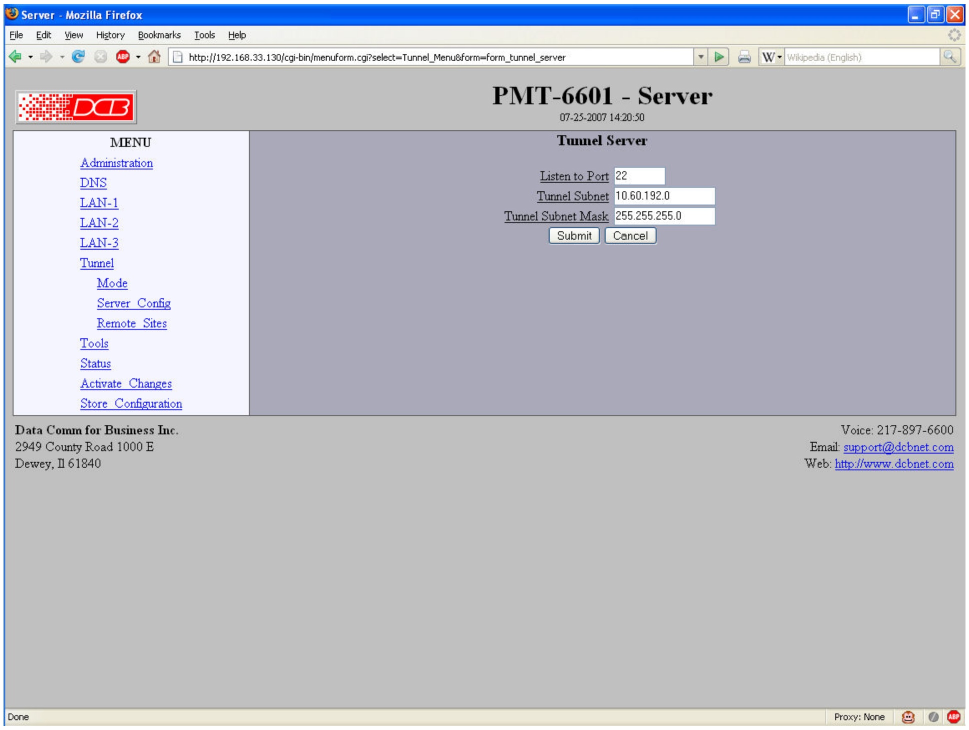
Disabled
Disable the PMT to stop all tunneling operations.

Server
One PMT in each system must be a server. This is typically the unit at the central location. Other units in client mode connect to this unit, so it must have a fixed, visible IP address (or be accessible via port mapping on a firewall) on LAN-1.

Client
One or more units will be configured in client mode. These units will connect to the server PMT. They may have temporary IP addresses on LAN-1

Notes

Tunnel Server Configuration



http://192.168.33.130/cgi-bin/menuform.cgi?select=Tunnel_Menu&form=form_tunnel_server

PMT-6601 - Server

07-25-2007 14:20:50

Tunnel Server

Listen to Port: 22

Tunnel Subnet: 10.60.192.0

Tunnel 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

Tunnel Server Configuration Screen

Fields

Listen-to Port

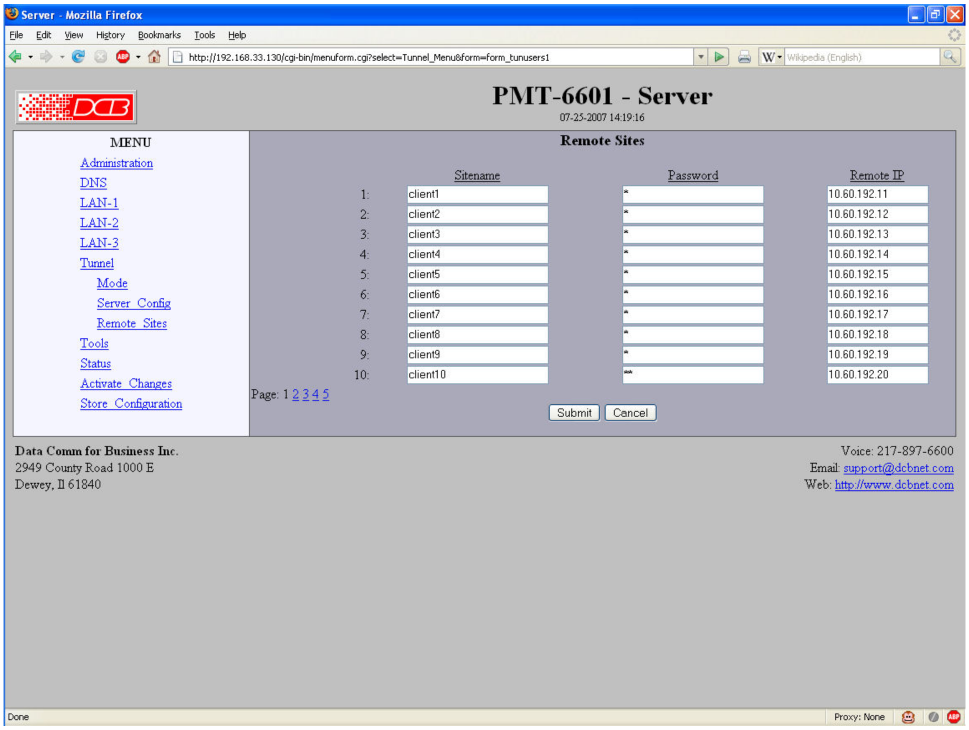
The UDP/IP port to listen to when server mode is enabled.   This must match the client Connect-To Port or be NATted through a firewall.

Tunnel Subnet

The Tunnel Subnet and Tunnel Subnet Mask specify the range of addresses used within the tunnel subnet. In other words, this is the inclusive range of addresses used by the server and all clients The server will allocate the first two addresses for its own use. The remaining addresses are assigned to clients. Based on the *Tunnel* Users configuration.

Notes

Tunnel – Remote Sites



http://192.168.33.130/cgi-bin/menuform.cgi?select=Tunnel_Menu&form=form_tunusers1

PMT-6601 - Server

07-25-2007 14:19:16

Remote Sites

	Sitename	Password	Remote IP
1:	client1	*	10.60.192.11
2:	client2	*	10.60.192.12
3:	client3	*	10.60.192.13
4:	client4	*	10.60.192.14
5:	client5	*	10.60.192.15
6:	client6	*	10.60.192.16
7:	client7	*	10.60.192.17
8:	client8	*	10.60.192.18
9:	client9	*	10.60.192.19
10:	client10	**	10.60.192.20

Page: 1 2 3 4 5

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

Tunnel Remote Sites

Fields

Site Name

This is the name that the client tunnel will use for authentication and configuration with the server. The server tunnel must have a matching entry in its table of tunnel users. Each sitename must be unique. The sitename may be up to 24 characters long and include any characters in the set '0' through '9', 'a' through 'z', 'A' through 'Z', '-', '_', '@', '.'. The sitename is case sensitive.

Password

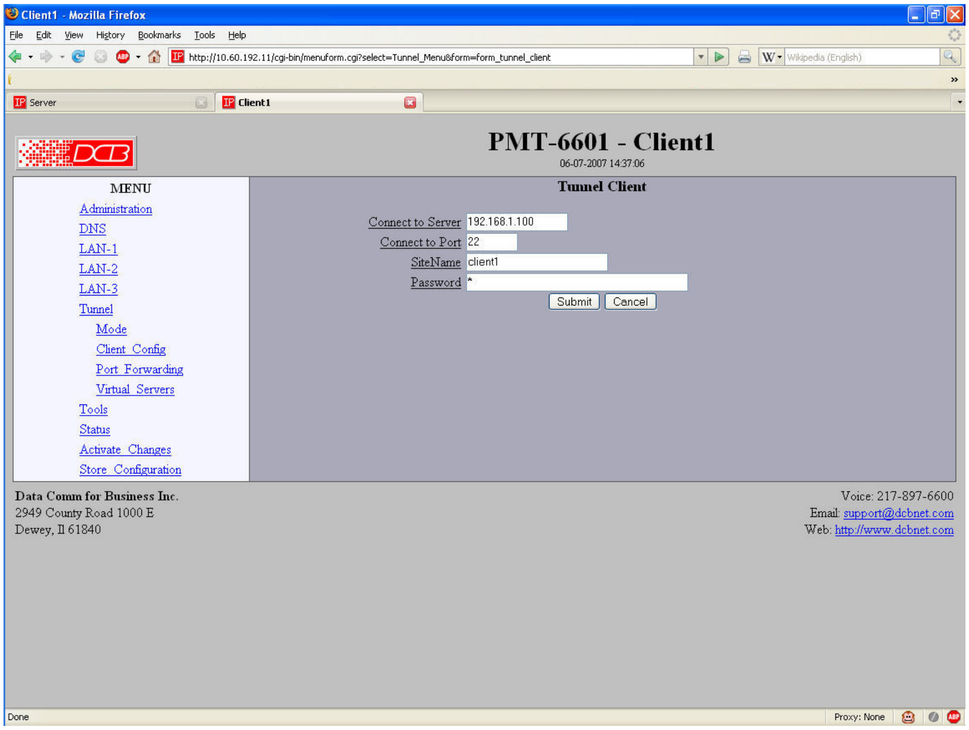
This is the password that the client tunnel will use for authentication with the server. The password may be up to 38 characters long and include any characters in the set '0' through '9', 'a' through 'z', 'A' through 'Z', '-', '_', '@', '.'. The password is case sensitive.

IP Address

This field sets the IP address to be assigned to the remote client. Each client must have a unique IP address.

Notes

Tunnel Client Configuration



http://10.60.192.11/cgi-bin/menuform.cgi?select=Tunnel_Menu&form=form_tunnel_client

PMT-6601 - Client1

06-07-2007 14:37:06

Tunnel Client

Connect to Server	192.168.1.100
Connect to Port	22
SiteName	client1
Password	*

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

Tunnel Client Configuration Screen

Fields

Connect To Server
Public IP address of the server that this client will attach to. This may be a NATted address.

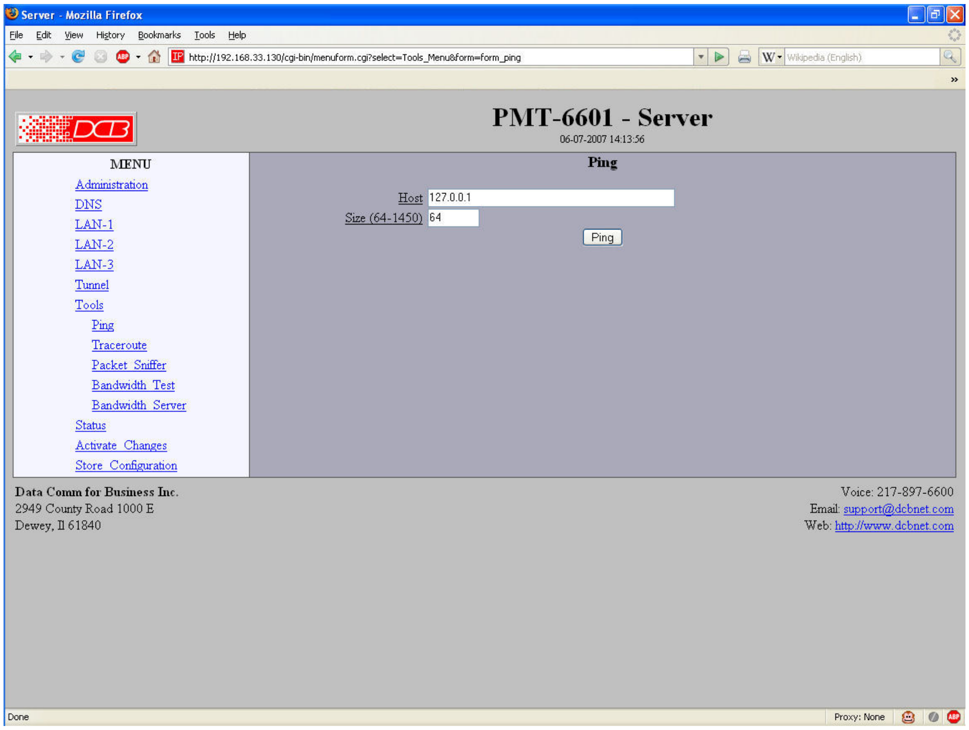
Connect To Port
The UDP port that the server tunnel is listening to for client connections.

Site Name
This is the name that the client tunnel will use for authentication and configuration with the server. The client tunnel must be configured with a matching sitename. Each sitename must be unique. The sitename may be up to 24 characters long and include any characters in the set '0' through '9', 'a' through 'z', 'A' through 'Z', '-', '_', '@', '.'. The sitename is case sensitive.

Password
This is the password that the client tunnel will use for authentication with the server. The password may be up to 38 characters long and include any characters in the set '0' through '9', 'a' through 'z', 'A' through 'Z', '-', '_', '@', '.'. The password is case sensitive.

Notes

Ping Screen



PMT-6601 - Server

06-07-2007 14:13:56

Ping

Host 127.0.0.1

Size (64-1450) 64

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

Tools - Ping Screen

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

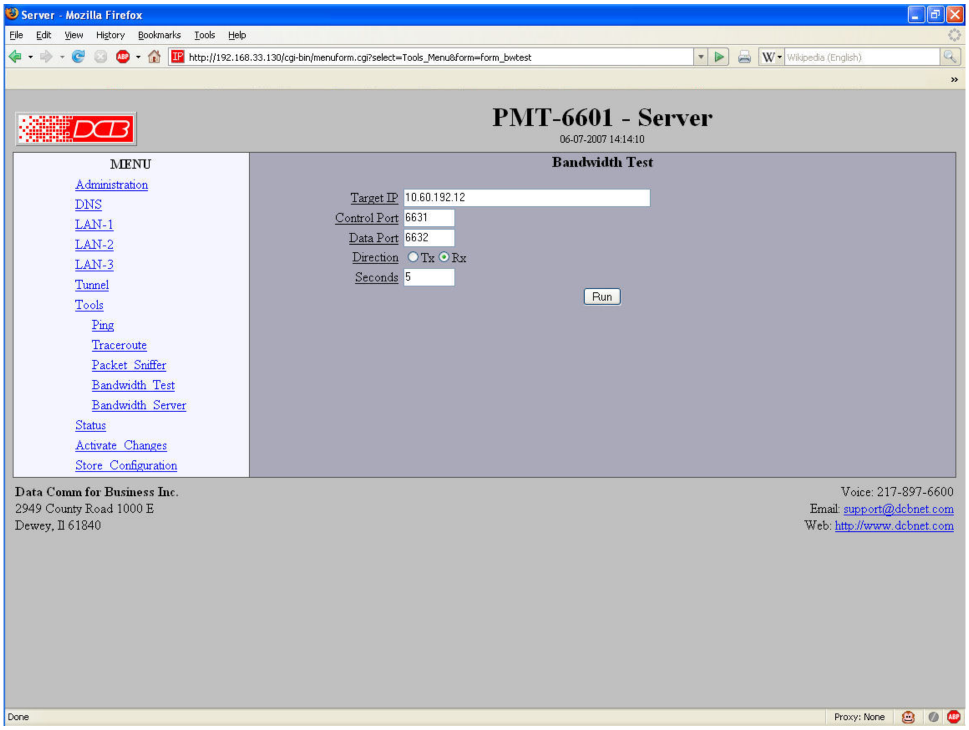
Fields

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

Notes

- Ping and traceroute are useful tools to determine if routing is correct.
- Ping may also be used to ”force” a dial-up connection to dial.

Bandwidth Test



PMT-6601 - Server

06-07-2007 14:14:10

Bandwidth Test

Target IP: 10.60.192.12
Control Port: 6631
Data Port: 6632
Direction: ○ Tx ● Rx
Seconds: 5

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

Bandwidth Test Screen

This screen is used to test the link between two units and measure the actual bandwidth available. This tool runs the client side of the NutTCP network test utility. It is run in TCP mode to measure the bandwidth between the client and the server devices.

Fields

- **Target IP**

  IP address or host name of the target device to run the bandwidth test against. The target device must have the NutTCP server running.

- **Control Port**

  The control port number to use for connecting to the NutTCP server. The target device NutTCP server must be configured with the same control port number.

- **Data Port**

  The data port number to use for connecting to the NutTCP server.

- **Direction**

  This field selects the direction of the data transfer test with respect to the NutTCP client.

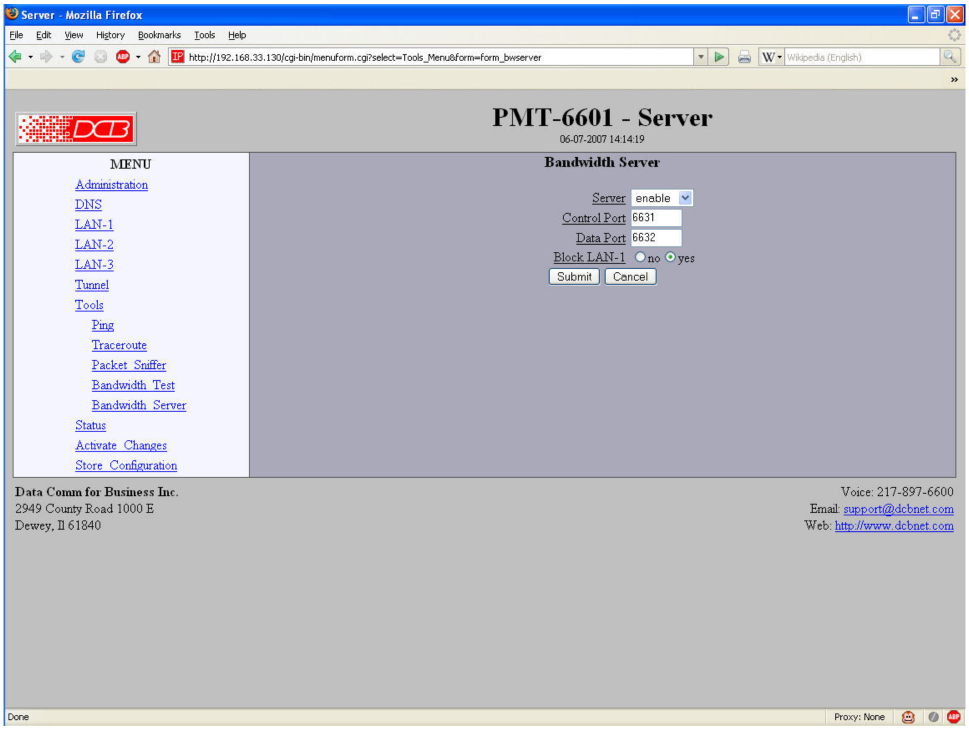
- **Seconds**

  This field sets the duration of the data transfer in seconds. Duration may be set from 1 to 20 seconds.

Notes

- The NuTCP network test utility is a commonly used bandwidth test. It requires that the NuTCP server running. See the Bandwidth Test Server Screen for server configuration.

Bandwidth Test Server Configuration



PMT-6601 - Server

06-07-2007 14:14:19

Bandwidth Server

Server: enable

Control Port: 6631

Data Port: 6632

Block LAN-1: ○ no ● yes

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

Bandwidth Test Server Configuration

This tool enables the server side of the NutTCP network test utility. .

Fields

- Server
  Enable/disable the NutTCP server. The NutTCP server uses little system resources when inactive, so it is OK to always have it enabled. However, if you do, it is recommended to firewall it from LAN-1 access by enabling the Block LAN-1 option. .

- Control Port
  The control port number to listen to for client connections. The NutTCP client must use this same port number.

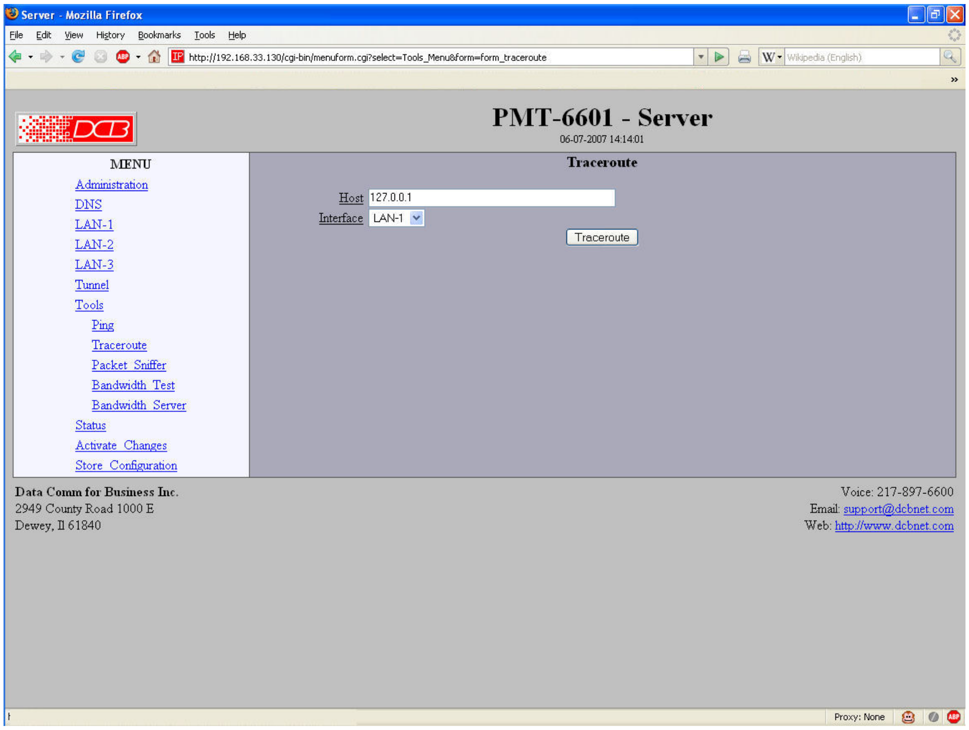
- Data Port
  The data port number to expect the NutTCP client to use. This port number does not directly apply to the NutTCP server. However, to properly firewall LAN-1, this should be set to the same port number used by the NutTCP client.

- Block LAN-1
  When set to *yes*, firewall rules will be applied blocking access to the NutTCP server via LAN-1.

Notes

The NutTCP bandwidth measurement tool is a popular software package used to measure the actual bandwidth between two nodes.

Traceroute Screen



PMT-6601 - Server
06-07-2007 14:14:01

Traceroute

Host 127.0.0.1
Interface LAN-1

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

Traceroute Screen

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

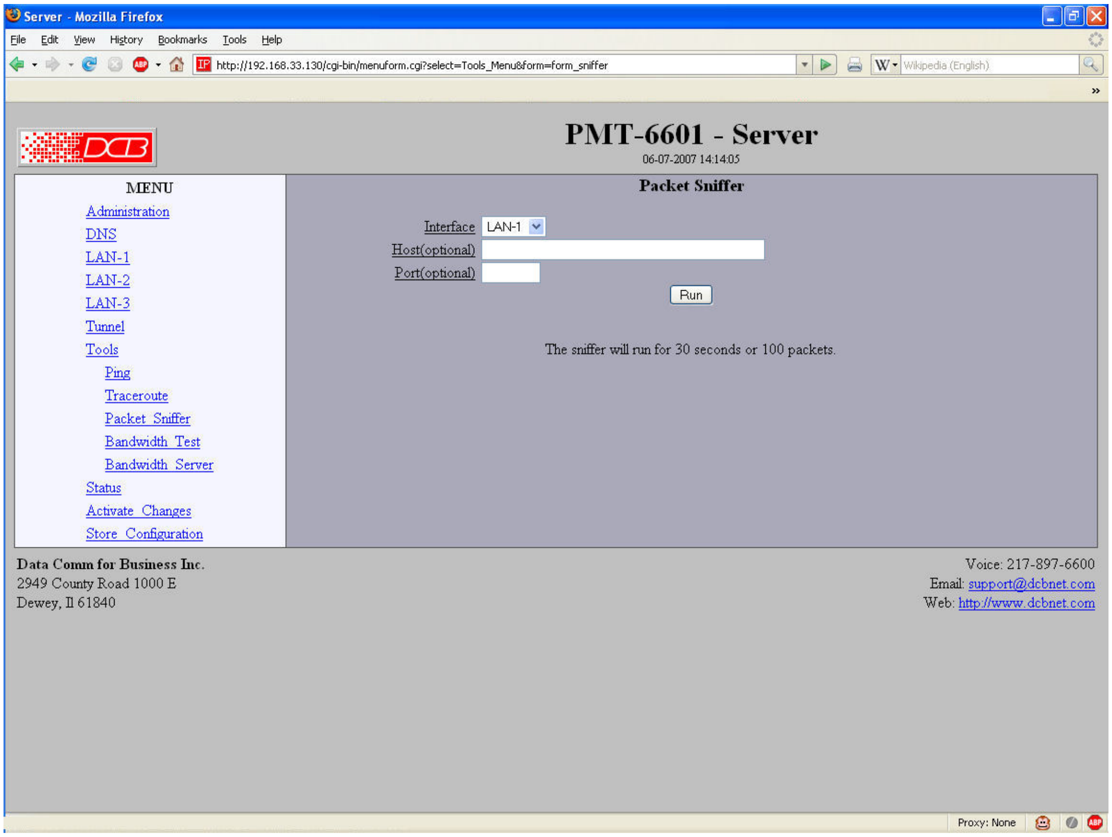
Fields

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

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

Notes

Packet Sniffer Screen



PMT-6601 - Server

06-07-2007 14:14:05

Packet Sniffer

Interface: LAN-1

Host(optional):

Port(optional):

The sniffer will run for 30 seconds or 100 packets.

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

Packet Sniffer Screen

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

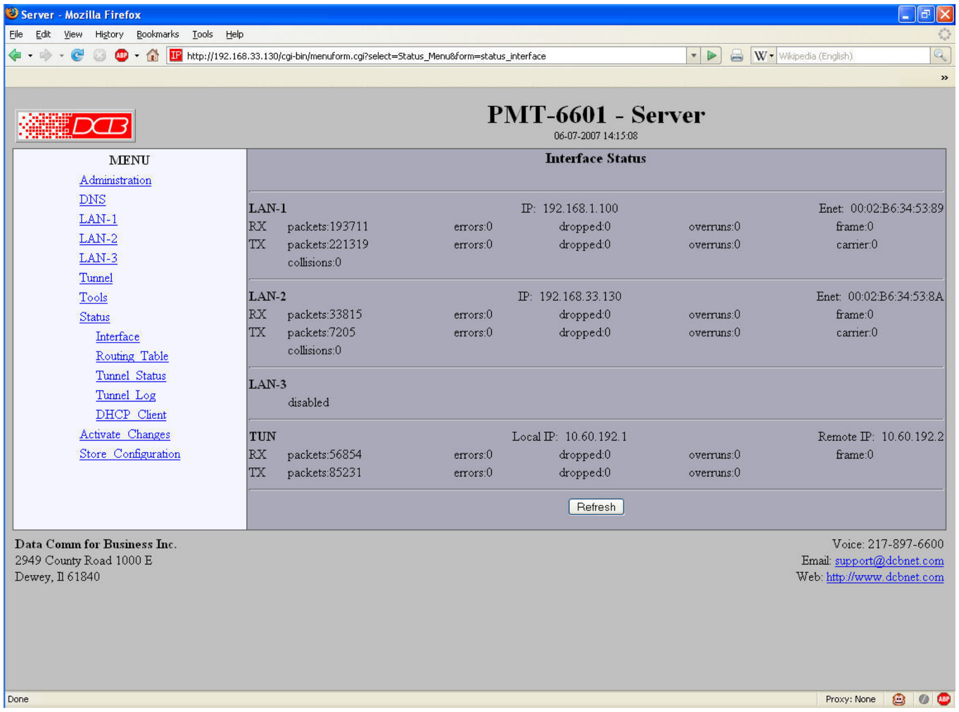
Fields

- Interface
  Which interface to use.
- Host
  This applies a host filter. Only packets with a matching source or destination IP address will be included in the trace.
- Port
  This applies a port number filter. Only TCP or UDP packets with a matching source or destination port number will be included in the trace..

Notes

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

Interface Status Screen



PMT-6601 - Server

06-07-2007 14:15:08

Interface Status

```
LAN-1                                 IP: 192.168.1.100                       Enet: 00:02:B6:34:53:89
RX   packets:193711     errors:0      dropped:0        overruns:0      frame:0
TX   packets:221319     errors:0      dropped:0        overruns:0      carrier:0
     collisions:0

LAN-2                                 IP: 192.168.33.130                      Enet: 00:02:B6:34:53:8A
RX   packets:33815      errors:0      dropped:0        overruns:0      frame:0
TX   packets:7205       errors:0      dropped:0        overruns:0      carrier:0
     collisions:0

LAN-3
     disabled

TUN                                   Local IP: 10.60.192.1                   Remote IP: 10.60.192.2
RX   packets:56854      errors:0      dropped:0        overruns:0      frame:0
TX   packets:85231      errors:0      dropped:0        overruns:0
```

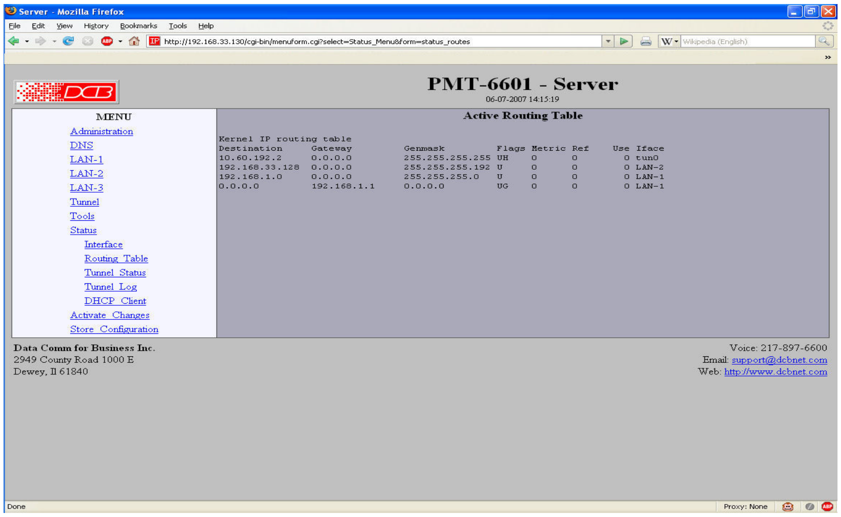
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

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

Interface Status Screen

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

Routing Table Screen



PMT-6601 - Server

06-07-2007 14:15:19

Active Routing Table

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.60.192.2     0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.33.128  0.0.0.0         255.255.255.192 U     0      0        0 LAN-2
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 LAN-1
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 LAN-1
```

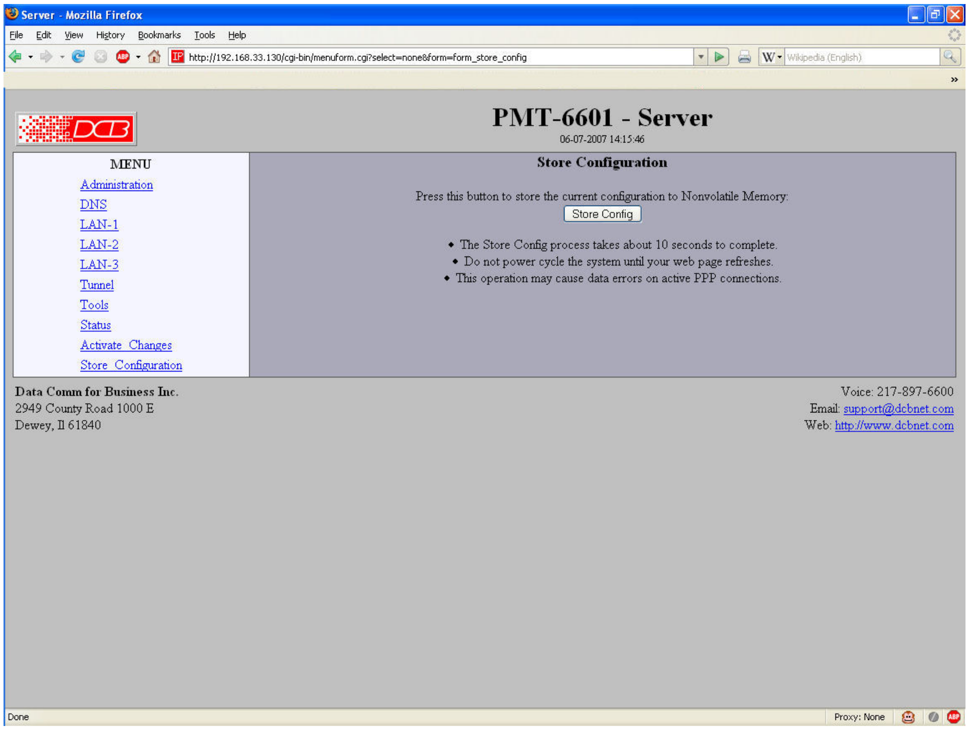
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

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

Routing Table Screen

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

Store Configuration Screen



PMT-6601 - Server

06-07-2007 14:15:46

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.
- This operation may cause data errors on active PPP connections.

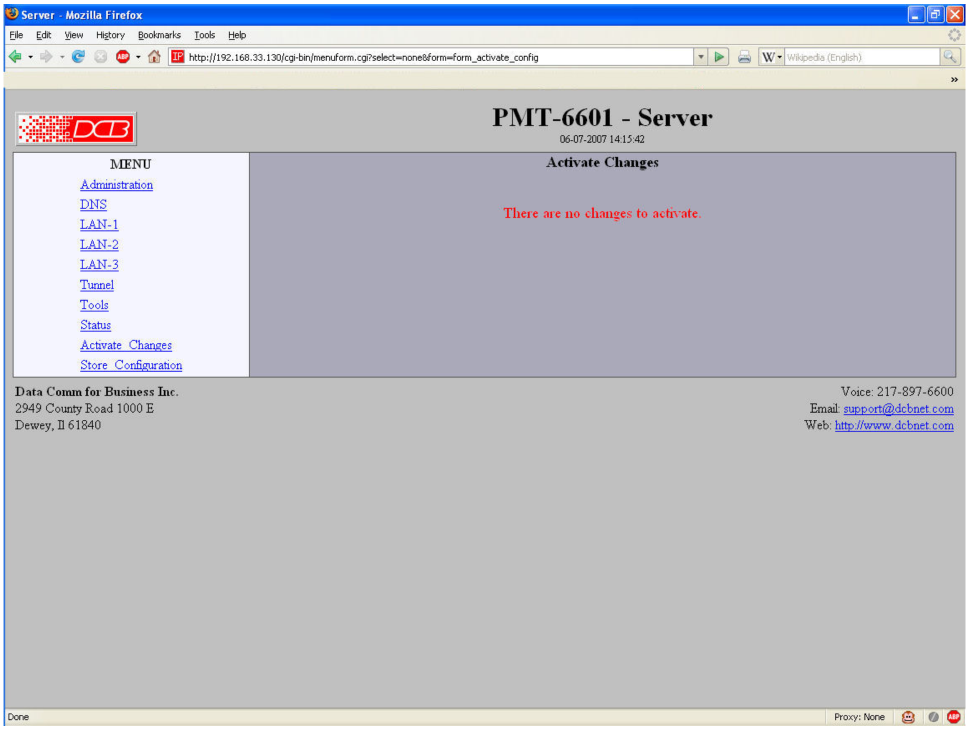
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

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.

Activate Configuration Screen



http://192.168.33.130/cgi-bin/menuform.cgi?select=none&form=form_activate_config

PMT-6601 - Server

06-07-2007 14:15:42

Activate Changes

There are no changes to activate.

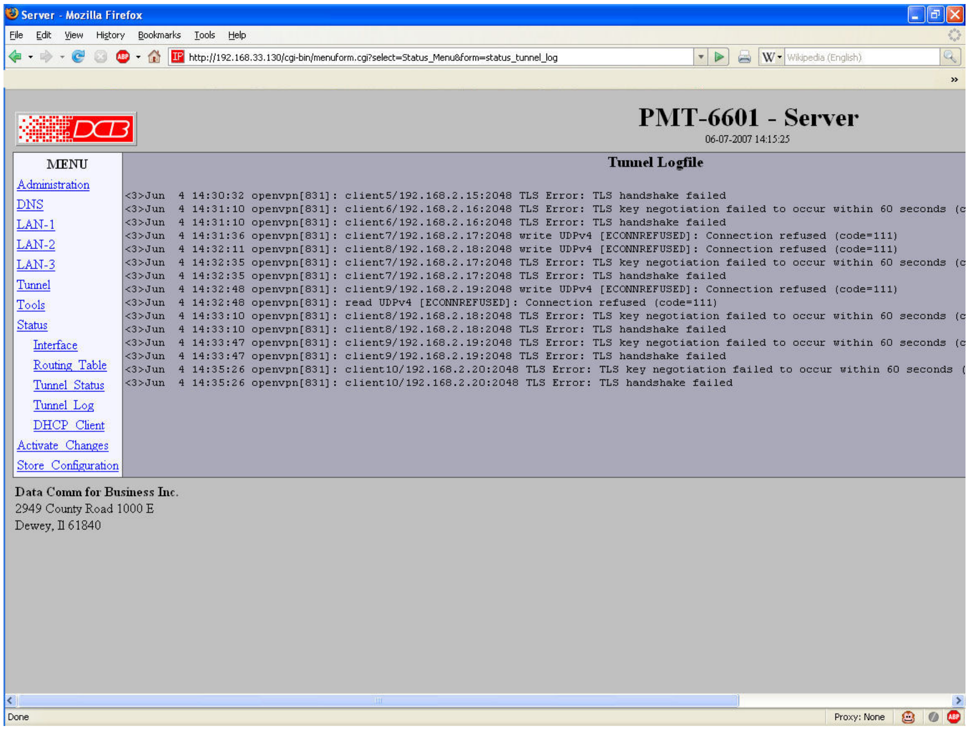
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

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. These changes will become immediately active, overwriting the pre-existing configuration for the duration of this session. Changes may be “stored” using the store configuration screen, in which case they will be written to non-volatile memory and used at the next reset or power-up.

Tunnel Log Screen



PMT-6601 - Server

06-07-2007 14:15:25

Tunnel Logfile

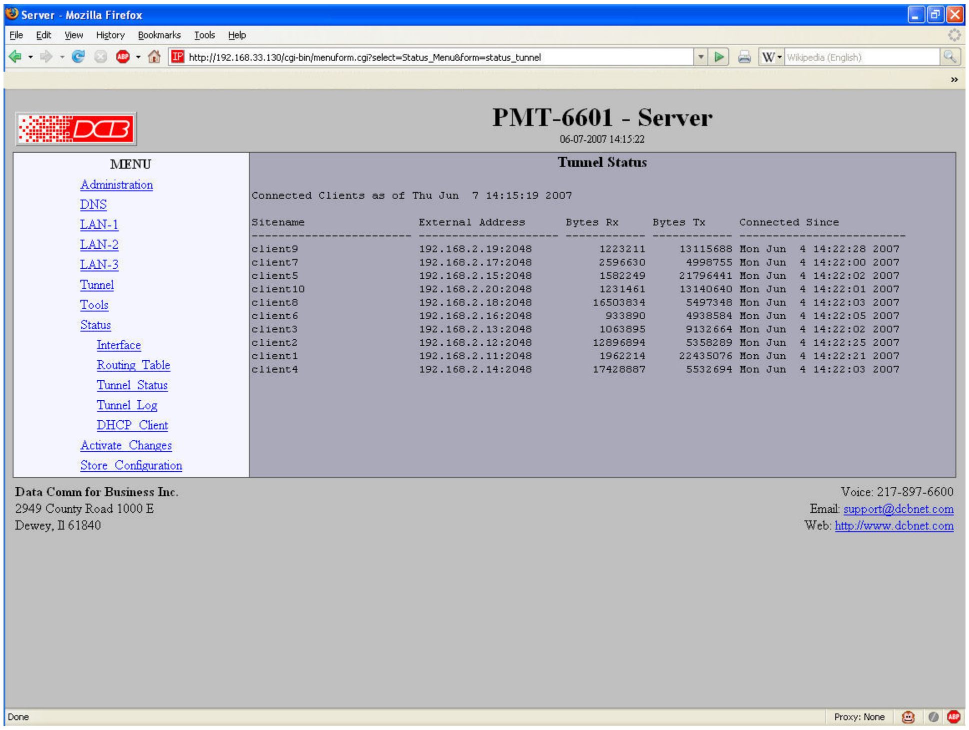
```
<3>Jun  4 14:30:32 openvpn[831]: client5/192.168.2.15:2048 TLS Error: TLS handshake failed
<3>Jun  4 14:31:10 openvpn[831]: client6/192.168.2.16:2048 TLS Error: TLS key negotiation failed to occur within 60 seconds (c
<3>Jun  4 14:31:10 openvpn[831]: client6/192.168.2.16:2048 TLS Error: TLS handshake failed
<3>Jun  4 14:31:36 openvpn[831]: client7/192.168.2.17:2048 write UDPv4 [ECONNREFUSED]: Connection refused (code=111)
<3>Jun  4 14:32:11 openvpn[831]: client8/192.168.2.18:2048 write UDPv4 [ECONNREFUSED]: Connection refused (code=111)
<3>Jun  4 14:32:35 openvpn[831]: client7/192.168.2.17:2048 TLS Error: TLS key negotiation failed to occur within 60 seconds (c
<3>Jun  4 14:32:35 openvpn[831]: client7/192.168.2.17:2048 TLS Error: TLS handshake failed
<3>Jun  4 14:32:48 openvpn[831]: client9/192.168.2.19:2048 write UDPv4 [ECONNREFUSED]: Connection refused (code=111)
<3>Jun  4 14:32:48 openvpn[831]: read UDPv4 [ECONNREFUSED]: Connection refused (code=111)
<3>Jun  4 14:33:10 openvpn[831]: client8/192.168.2.18:2048 TLS Error: TLS key negotiation failed to occur within 60 seconds (c
<3>Jun  4 14:33:10 openvpn[831]: client8/192.168.2.18:2048 TLS Error: TLS handshake failed
<3>Jun  4 14:33:47 openvpn[831]: client9/192.168.2.19:2048 TLS Error: TLS key negotiation failed to occur within 60 seconds (c
<3>Jun  4 14:33:47 openvpn[831]: client9/192.168.2.19:2048 TLS Error: TLS handshake failed
<3>Jun  4 14:35:26 openvpn[831]: client10/192.168.2.20:2048 TLS Error: TLS key negotiation failed to occur within 60 seconds (
<3>Jun  4 14:35:26 openvpn[831]: client10/192.168.2.20:2048 TLS Error: TLS handshake failed
```

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

Tunnel Log Screen

The Tunnel Log File Screen displays a record of all key changes, connections, authentications, and disconnects.

Tunnel Status Screen



PMT-6601 - Server

06-07-2007 14:15:22

Tunnel Status

```
Connected Clients as of Thu Jun  7 14:15:19 2007

Sitename                 External Address     Bytes Rx     Bytes Tx     Connected Since
------------------------ -------------------- ------------ ------------ ------------------------
client9                  192.168.2.19:2048         1223211     13115688 Mon Jun  4 14:22:28 2007
client7                  192.168.2.17:2048         2596630      4998755 Mon Jun  4 14:22:00 2007
client5                  192.168.2.15:2048         1582249     21796441 Mon Jun  4 14:22:02 2007
client10                 192.168.2.20:2048         1231461     13140640 Mon Jun  4 14:22:01 2007
client8                  192.168.2.18:2048        16503834      5497348 Mon Jun  4 14:22:03 2007
client6                  192.168.2.16:2048          933890      4938584 Mon Jun  4 14:22:05 2007
client3                  192.168.2.13:2048         1063895      9132664 Mon Jun  4 14:22:02 2007
client2                  192.168.2.12:2048        12896894      5358289 Mon Jun  4 14:22:25 2007
client1                  192.168.2.11:2048         1962214     22435076 Mon Jun  4 14:22:21 2007
client4                  192.168.2.14:2048        17428887      5532694 Mon Jun  4 14:22:03 2007
```

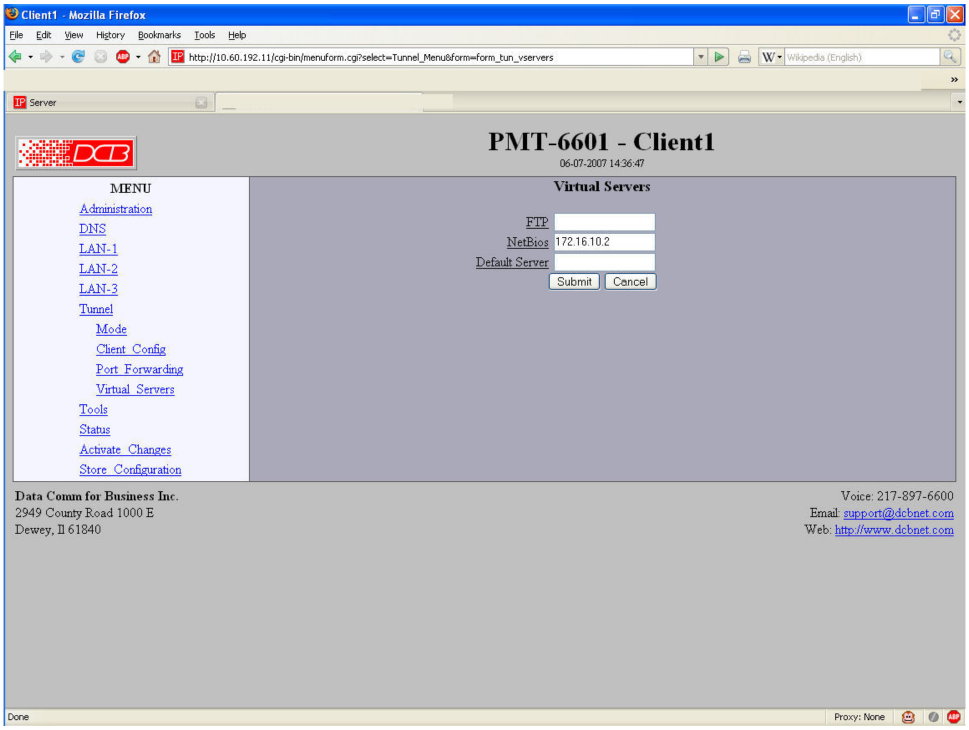
Data Comm for Business Inc.
2949 County Road 1000 E
Dewey, Il 61840

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

Tunnel Status Screen

The Tunnel Status Screen displays status for currently connected remote nodes.

Virtual Servers Screen



PMT-6601 - Client1

06-07-2007 14:36:47

Virtual Servers

FTP

NetBios 172.16.10.2

Default 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

Virtual Servers Screen

Virtual Servers is a simplified version of Port Forwarding. Both are also referred to as Destination Network Address Translation (Destination NAT). It is a process where incoming server requests are redirected to the specified IP address regardless of the destination IP address. It is commonly used when you have IP sharing enabled to allow servers on your internal network to appear on the external network.   While most applications require port forwarding to various client nodes, this screen provides a convenient method to enable commonly used servers.

Fields

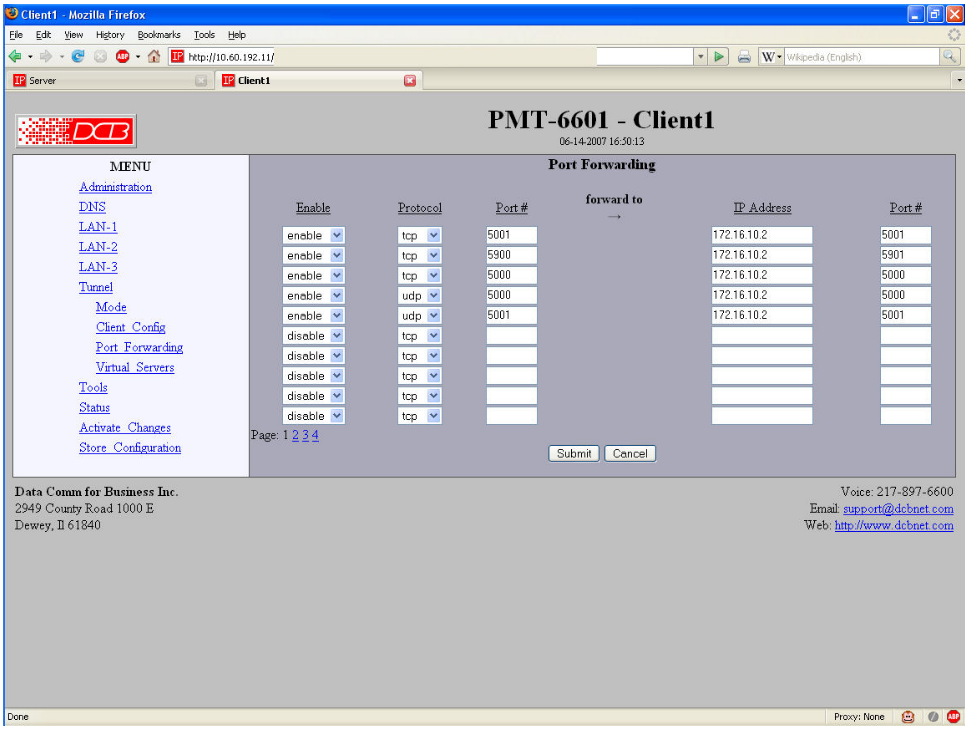
- FTP
  The IP address of where to direct FTP (TCP port 20 and 21) requests.
- Netbios
  The IP address of where to direct NetBios (TCP and UDP ports 137, 138, and 139) requests.
- Default Server
  The IP address of where to direct any IP packets not redirected by other Virtual Server or Port forwarding entries.

Notes

This screen is only seen when the device is configured as in client mode.

Maximum number of individual port forwarding entries is 40.

Port Forwarding Screen



PMT-6601 - Client1

06-14-2007 16:50:13

Port Forwarding

Enable	Protocol	Port #	forward to →	IP Address	Port #
enable	tcp	5001		172.16.10.2	5001
enable	tcp	5900		172.16.10.2	5901
enable	tcp	5000		172.16.10.2	5000
enable	udp	5000		172.16.10.2	5000
enable	udp	5001		172.16.10.2	5001
disable	tcp				
disable	tcp				
disable	tcp				
disable	tcp				
disable	tcp				

Page: 1 2 3 4

Submit Cancel

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

Port Forwarding Screen

Port Forwarding, also known as Destination Network Address Translation (Destination NAT), is a process where incoming server requests are redirected to an alternate server address regardless of the original destination IP address. It is commonly used when IP sharing is enabled to allow servers on your internal network to appear on the external network.   This table forms the core of the forwarding system performed by the PMT.

Fields

- Enable
  Enable/Disable this entry in the Port Forwarding Table.

- Disable
  The IP address of where to direct NetBios (TCP and UDP ports 137, 138, and 139) requests.

- Protocol
  The Protocol type, TCP or UDP, of the service you wish to forward. For example, Telnet is a TCP protocol. TFTP is a UDP protocol.

- Port No.
  The Port Number, 1 - 65535, of the service you wish to forward. For example, Telnet is port number 23. TFTP is port number 69.

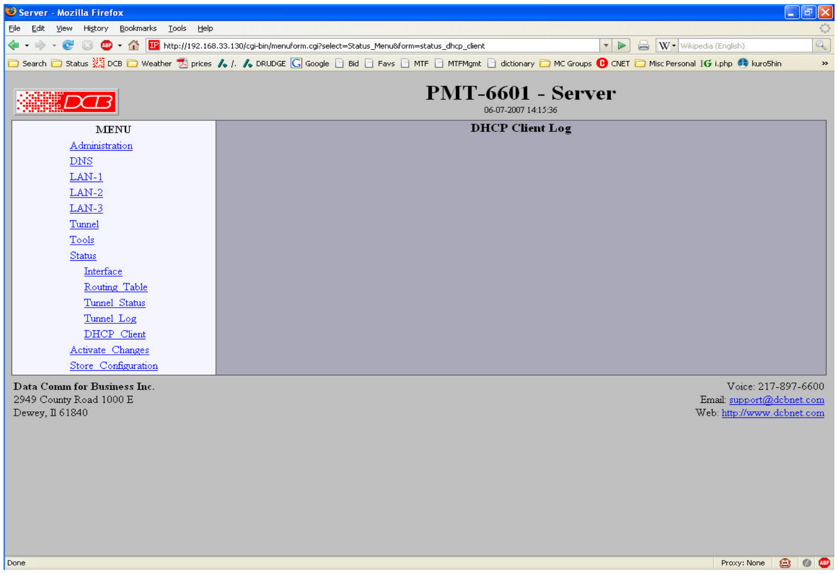
- Forward to IP Address
  The IP address of where to forward the request.

- Forward to Port Number
  The Port number to use when forwarding these requests. If this field is left blank, the original port number is used.

Notes

This screen is only seen when the device is configured as in client mode.

DHCP Client Log Screen



http://192.168.33.130/cgi-bin/menuform.cgi?select=Status_Menu&form=status_dhcp_client

PMT-6601 - Server
06-07-2007 14:15:36

DHCP Client Log

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

DHCP Client Log Screen

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

Chapter 5

Operation

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

Operation – Overview

The PMT operates by creating a hardware based VPN tunnel between the host site PMT unit and one or more remote site PMT devices. This connection is encrypted using the AES algorithm, and provides privacy between the PMT units. Maps which are configured into the PMT devices redirect IP connections from the host site to individual machines on the back side of remote PMT devices. Although communications are two-way, all communications between user devices must originate at the host location. This prevents any nodes on the remote LAN from accessing the host LAN segment.

A typical use would be to enable technicians at the host site to maintain remote equipment using SMB file transfers, remote terminal operations, VNC, or windows remote support applications. The system also allows automated file “pulls” from remote devices such as point of sale PCs and registers and the ability to push update files and firmware out to remote devices.

The PMT port mapping feature allows multiple sites to use standard hardware configurations with identical IP addresses at the end nodes. For example, every remote site might have the first controller addressed as 10.1.1.1 , and the second one at 10.1.1.2. The PMT configuration map will translate packets destined to each device to a virtual subnet address on the host LAN. Each remote site will have different mapping, which allows the use of standard end node hardware configurations.

Once the units are configured and installed, the “virtual” IP subnet allows the remote nodes to be accessed by any workstation on the host subnet. However, connections may not be initiated from the remote side subnets, and only specifically mapped IP addresses are allowed to communicate through the system.

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 PMT still does not function properly, please contact your dealer for further advice.

Hardware Problems

Before anything else, check that all cables are wired correctly and properly connected.

***P*:** All the LEDs are off.
S: Check the power supply or power connection.

P: When using 10/100/1000Base-T cabling, the unit does not work.
S: Check the switch or hub's link LED for the port to which the bridge is connected. If it is off, make sure the network cable between the bridge and hub is in good condition.

Can't Connect to the units

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

- Insure that you are addressing the PMT correctly ie. https:// vs. http:// for some models .
- Start troubleshooting from a known state. Power OFF and ON to reboot.
- Is a proper IP address configured in the PMT and PC?
- "Ping" the PMT 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 PMT (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 PMT have compatible IP addresses.**
- It may be that your "ARP table" contains invalid entries. You can clear the "ARP table" by rebooting, or, on some Windows versions, by typing the following command at the command prompt or *Run* dialog box.: `ARP * -d`
- Check that you are using the proper Ethernet connection.
- The PMT is meant to be connected to a hub or ethernet switch. If connected directly to a PC, an ethernet crossover cable must be used.
- In some cases, "smart" hubs and switches must be power-cycled to clear their internal ARP cache. This is often a problem on test bench setups where IP addresses are moved between different equipment or a unit is moved between ethernet switch receptacles.

Other Problems

***P*: ** Can’t run the initial configuration program using a serial cable connection.
S: Check that:

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

Checking PMT Operation

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

From a PC at the host location, connect to one of the remote devices. If the connection succeeds, then two-way operation is confirmed.

Verify communications to each device behind the remote PMT units.

It may be helpful to configure a remote PC at each site as a default server for testing. That way, you can test using various ports, as well as use that PC remotely to work on problems from both ends once a valid connection is made to that one.

Appendix A

Specifications

PMT-6601 Specifications

- Flash Memory: 128 Mbytes Minimum
- DRAM: 128 Mbytes
- LAN A Interface: 10/100/BaseT, Autosense
- LAN B Interface: 10/100/BaseT, Autosense
- LAN C Interface: 10/100/BaseT, Autosense
- CPU: AMD GX-2 333 Mhz
- OS: uCLinux
- Power: 120 VAC or 240 VAC,   12 VDC or Optional power supplies
- Stand alone package
- Connection uses 128 bit AES encryption
- Throughput: greater than 10 Mbps
- Supports simultaneous remote PMT units
- LED: (LAN Activity, LAN Status (per interface), Power, Virtual HD Activity)
- Setup via serial connection or Web browser(preferred)
- Default IP address: LAN-1: DHCP Client
- Default IP address: LAN-2: 192.168.0.1/255.255.255.0
- Default IP address: LAN-2: 192.168.3.1/255.255.255.0
- Authentication with built-in database
- Browser Management port: 80
- Operational Temperature 0C to +50C

LAN port to PC crossover ethernet cable

A crossover cable may be constructed to allow the PMT **ethernet port** to directly connect to a PC without using a hub.

Use the following pinout to build an ethernet crossover cable:

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

Appendix B

Open Source Software Information

Some models of this product series were designed in conjunction with Open Source Linux software.

Introduction

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

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

Obtaining the Source Code

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

Open Source Software Administrator

Data Comm for Business, Inc.

2949 CR 1000 E

Dewey, IL. 61840

Appendix C

Sample Configuration

This is a sample "workbook" type configuration example

Address Information Needed Prior to Setup

In this discussion, the "customer's network" is the external side network being utilized at either the host or remote site. The "machine network" is the local network consisting of the end node being supported by the PMT.

Before beginning the setup process, collect IP addresses, netmask, and gateway addresses. These often need to be assigned by a network administrator, or in the case of the public IP address, obtained from your ISP. Please refer to the diagram to see where these addresses fit in the network topology.

For the Server...

- LAN-1 will need a public IP address, netmask, and upstream gateway address.
- LAN-2 will need an internal IP address and netmask,
- A virtual subnet is needed which will be used as a pool of addresses for accessing the remote PMT-6601 clients. For routing reasons, this needs to be a valid subnet with a minimum of 4 addresses.

For the Clients...

- LAN-1 will need an IP address, netmask, and upstream gateway address on either the customer's internal or external network. If the customer is running a DHCP server, LAN-1 may be configured to obtain this information automatically. If the PMT-6601 is placed on the customer's internal network, the firewall must allow outbound UDP connections on port 22 (or the port you choose to use when you set up the server).
- LAN-2 will need an IP address and netmask compatible with the machine network.
- LAN-3 will need an IP address and netmask compatible with the machine network. Use of this interface is optional. However, if you choose to use it, it must not overlap with LAN-2's configuration. LAN-2 and LAN-3 are isolated from each other, thus broadcasts traffic will not traverse between these interfaces.
- Note about LAN-2 and LAN3 – It is important that the subnets on these interfaces not overlap with the customer's subnet on LAN-1.

Initial Setup

From the factory, the LAN interfaces will come configured with the following settings:

LAN-1 – DHCP client mode – will try to obtain IP, netmask, and gateway automatically

LAN-2 – 192.168.0.1/255.255.255.0

LAN-3 – 192.168.3.1/255.255.255.0

Most users prefer to not deal with the serial setup. If you are comfortable with reconfiguring your PC's IP address, you can temporarily change the IP address to 192.168.0.2 and go directly to the web interface to configure the PMT-6601's LAN interfaces. If you choose to use this method, make sure these addresses do not interfere with any other devices on your network. It is often best to directly connect your PC to the PMT-6601 using a network crossover cable.

Serial Setup

The COM port on the PMT-6601 may be used to reset the configuration to default and to set the IP addresses for all three LAN interfaces. To do so, you will need a terminal or a terminal emulation program, such as HyperTerm, running on a PC. Connect the terminal to the PMT-6601's COM port using a null modem cable. A DE-9 to DE-9 null modem cable was provided with the unit. Configure the terminal for 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

To enter serial setup mode, power up the PMT-6601 and listen for the beeps. Approximately 5 seconds after power up, you will hear a single beep. At this point, do nothing. Approximately 15 seconds later, you will hear two beeps. At this point, press the <esc> key. If all goes well, you will immediately hear three beeps and about 1 second later you should see a login prompt on your terminal screen. If instead, you hear a single beep, you have missed the setup window and will have to try again. If you fail to enter setup, verify your serial cable connection and your terminal configuration.

At the login prompt, enter the word "*setup*". Follow the prompts to reset the configuration and to setup the LAN interfaces.

Accessing the Web Interface

The PMT-6601 is configured using a standard web browser. By default, web access through LAN-1 is blocked, so you will need to use either LAN-2 or LAN-3. To access the web interface, use the IP address of the LAN interface as the URL. For example:

http://192.168.0.1

This should bring up a web screen and a HTTP authentication window. Enter the username "admin" and leave the password field blank. If you can not access the web interface, verify that both the PC and the PMT-6601 are showing a valid link LED, that both are on the same subnet, and that you have connected to the correct LAN interface on the PMT-6601.

Along the left side of the the web screen, you should see a menu bar and on the right side a form window. When you select an item on the left side, it will open up a form window on the right. When you make changes to a form, you must submit the changes before you change to another page. If you do not, you will lose the changes you made. Changes do not take effect until you press the *Activate_Changes* item.

Changes are not committed to non-volatile storage until you press the *Store Config* button. This three step process allows you to make multiple form changes before they take effect. It also allows you to test the changes before committing them to storage. If a configuration change is bad, you can power cycle the unit to return back to the previously stored configuration.

Help information is available for every configuration item on the form side of the web screen. Simply click on the item name and a new browser window will open up with the on-line help file.

Web Server Setup

When setting up a unit, the first thing you should set is a username and password for the web interface. This is done from the *Administration – Admin Password* form. After you activate the change, you will have to re-authenticate to the PMT-6601 using the new username and password.

At this point you should decide if you want to use secure HTTPS for administration of the the PMT-6601. Doing so will cause all traffic between the PMT-6601 and your web browser to be encrypted, preventing any passwords or usernames from being sent in the clear. If you want to use HTTPS, go to the *Administration – Access Control* form and change the *Web Server Port* to *443* and *enable Secure Web Server*. When you activate this change, you will need to change your URL to https. So, for example you would use:

https://192.168.0.1

One last point regarding the web interface. If one of the services, or ports, you plan to map on your machine network is HTTP (port 80) or HTTPS (port 443), you will need to use an alternate port number for the web interface. Doing so will allow you to access a client PMT-6601's web interface while still allowing you to map HTTP or HTTPS on your machine network. For example, you could select port 8000. To access the web interface, you would then append the port number to the URL. For example:

http://192.168.0.1:8000

https://192.168.0.1:8000

Host Name Setup

If you notice the web screen title, you will see the name PMT-6601 – PMT. The second PMT is the DNS host name for the unit. Use of DNS is not require, but you can set the host name of the device so that it will show up on the web screen making it easier to remember which unit you are talking to. The host name is set from the *DNS* form.

LAN Setup

If you did not use the serial interface to configure the LAN ports, go to the *LAN-1/2/3 - IP Configuration* forms to do so now. Use the addresses collected previously as explained in the first section. Note that if you change the IP address of the interface you are using for configuration, when you activate the change, you will have to adjust the HTTP URL to the new address.

If you do not plan to use LAN-3, it is best disable the interface to prevent the off-chance that it may interfere with another subnet.

Tunnel Setup – Server

To place the PMT-6601 in server mode, select the *Tunnel – Mode* form and set the mode to *server*. After you submit the change, the Tunnel menu will change and offer server specific forms.

To set up the server, select the *Tunnel – Server Config* form. The first item in the form is were the port number is selected. This is the UDP port that clients tunnels will connect to. The default is 22, but you may select any number in the 1 to 65535 range. When you setup the client PMT-6601s, you will specify this same port number in their configuration.

The next two items, *Tunnel Subnet* and *Tunnel Subnet Mask* sets the virtual subnet to be used for the tunnels. You must use a valid subnet. In other words, the subnet address must fall on a valid boundary for the given mask. Also, there must be at least 4 addresses in the subnet. An example would be 10.60.192.0 / 255.255.255.0

The *Tunnel – Tunnel Users* form is where you configure the authentication credentials and set an IP address for each client PMT-6601. Each sitename and IP address must be unique. See the help screens for the valid characters and length limits for both the sitename and password. The client's IP address should be chosen from an address in the Tunnel Subnet, but do not choose either of the first two addresses as these are used by the server to form a virtual point-to-point link.

Tunnel Setup – Client

To place the PMT-6601 in client mode, select the *Tunnel – Mode* form and set the mode to *client*. After you submit the change, the Tunnel menu will offer client specific forms.

To setup the client, select the *Tunnel – Client Config* form. The fields on this form correspond directly to settings in the Server's configuration.

- The *Connect to Server* field is set to the Server's LAN-1 IP address.
- The *Connect to Port* field is set to the Server's *Listen to Port*.
- The *Sitename* and *Password* is set to a corresponding entry in the Server's *Tunnel Users* table.

The *Port Forwarding* and *Virtual Server* forms are where you specify the mapping of services to individual computers on the remote network. These tables map the Server assigned IP address, as specified in the

Tunnel Users table, and a port number to a remote IP address and port number. So, for example, if you want to forward port 5900 to 172.16.10.2, you would configure the following entry:

```
enable tcp 5900 --> 172.16.10.2 5900
```

If you wanted to forward port 5901 to 172.16.10.3 port 5900, you would configure the following entry:

```
enable tcp 5901 --> 172.16.10.3 5900
```

Virtual Servers is a simplified form of Port Forwarding. Protocols, such an Netbios and FTP use multiple ports. By specifying a Virtual Server entry, Netbios or FTP traffic can be directed to a particular machine without having to enter multiple rules in the Port Forwarding table. The Default Server is a special case of Port Forwarding. It directs all traffic, not directed by another Port Forward or Virtual Server entry, to the indicated address. In other words, the Default Server will get everything else.

Static Routing Rule – Server Side

In order to have computers on your network communicate with the devices on the machine networks you will need to install a static routing rule to the Tunnel Subnet. The route needs to specify that the PMT-6601's LAN-2 interface is the gateway for the Tunnel's virtual LAN. Using the above diagram as an example, you would need to specify a route of:

```
target 10.60.192.0 netmask 255.255.255.0 gateway 10.60.70.10
```

The easiest way to handle this is to put the static route in your primary gateway router. In the above diagram, that would be the firewall router. When a computer on your network tries to communicate with a remote device, it will send the request to your gateway router. The gateway router will forward the packet to the PMT-6601. The gateway router will then send a redirect command to the computer giving it the above routing information.

Another way to handle this is to put the static routing entry in every computer that needs access to the remote devices. The disadvantage of this method is that you must enter this in every computer that needs it. However, the advantage is that only computers configured with this static route may access the remote devices. For Windows XP this is done with the following command. Again, referring to the diagram as an example, the command would be:

```
route -p add 10.60.192.0 mask 255.255.255.0 10.60.70.10
```

Static Routing Rule – Client Side

Computers out on the remote end of the network will need to have their default gateway address set to the PMT-6601's IP address. Which address you use depends on the interface. Referring to the diagram as an example, computers on the LAN-2 would have their gateway address set to 172.16.10.1 and computers on LAN-3 would have their gateway address set to 172.16.11.1.

- LAN-1 will need an IP address, netmask, and upstream gateway address on either the customer's internal or external network. If the customer is running a DHCP server, LAN-1 may be configured to obtain this information automatically. If the PMT-6601 is placed on the customer's internal network, the firewall must allow outbound UDP connections on port 22 (or the port you choose to use when you set up the server).
- LAN-2 will need an IP address and netmask compatible with the machine network.
- LAN-3 will need an IP address and netmask compatible with the machine network. Use of this interface is optional. However, if you choose to use it, it must not overlap with LAN-2's configuration. LAN-2 and LAN-3 are isolated from each other, thus broadcasts traffic will not traverse between these interfaces.
- Note about LAN-2 and LAN3 – It is important that the subnets on these interfaces not overlap with the customer's subnet on LAN-1.