



PortServer TS 8/16

www.digi.com

Making
DEVICE NETWORKING
*easy*TM

© Digi International Inc. 2003.

Digi, Digi International, the Digi logo, the Digi Connectware logo, the Making Device Networking Easy logo, Digi One, PortServer, and RealPort are trademarks or registered trademarks of Digi International, Inc. in the United States and other countries worldwide. All other trademarks are the property of their respective owners.

www.digi.com

Making
DEVICE NETWORKING
easy™

Table of Contents

Chapter 1 Introduction	
Setup Overview	7
About Entering Commands on the Command Line	8
Supported Devices	8
About This Guide.....	8
Other Documents in the Library.....	8
About Configuration Methods.....	9
Configuration Prerequisites	10
Chapter 2 Configuring the IP Address	
Options for Configuring the IP Address and Mask	11
Device Support: Digi Port Authority-Remote and ARP-Ping for IP Address Configuration	11
Configuring the Ethernet Interface with Digi Port Authority-Remote ...	11
Configuring the IP Address Using ARP-Ping.....	12
Configuring the Ethernet Interface from the Command Line	13
Configuring an IP Address using DHCP and RARP.....	14
Chapter 3 Configuring Ports for RealPort	
About RealPort	15
Configuring Ports: Web Interface	15
Chapter 4 Configuring Ports for Printers	
Configuration Considerations	19
Configuring Ports for Printers: Web Interface.....	20
Tips for Telnet and rsh Printing	20
Configuring a Port for Direct-Access Printing	20
Chapter 5 Configuring Ports for Modems	
Tips on Configuring A Modem.....	23
Configuring Ports for Modems: Web Interface	23
Commands for Configuring Ports for Modem Connections.....	24
Related Information	24
Configuring A Hunt Group	24

Chapter 6	Configuring Ports for Terminals and Computers	
	Configuring Ports for Terminals: Web Interface	27
	Commands for Configuring Ports for Terminals	27
	Port Defaults.....	27
	Related Information	27
	About Computer Connections	28
Chapter 7	Configuring PPP	
	Configuring Inbound PPP Connections: Command Line.....	29
	Configuring Outbound PPP Connections: Command Line.....	31
Chapter 8	Configuring Autoconnection	
	About Autoconnection	35
	Configuring a Port for Autoconnection: Web Interface	35
	Commands for Configuring Autoconnection by Port or by User.....	35
	Configuring a User for Autoconnection: Web Interface	35
	Configuring TCP Socket Communication	36
	Configuring UDP Multicast	37
Chapter 9	Configuring IP Routing	
	Configuring Static Routes.....	41
	Configuring Dynamic Routes Using RIP.....	42
	Configuring Proxy ARP.....	43
Chapter 10	Configuring the Digi Device for IA (Industrial Automation)	
	About Modbus	45
	Modbus Configuration Procedure: Web Interface	45
	Configuring the User-Defined Protocol.....	46
Chapter 11	Configuring Security Features	
	Controlling Access to the Configuration	47
	Controlling Access to Inbound Ports	47
	Controlling Access to Outbound Ports.....	48
	Controlling Access to the Command Line	48
	Using RADIUS to Authenticate Users	49
	Issuing User Passwords	52
	Configuring SSH Version 2 for Secure Communication	52
	Controlling Access to Services	53
	SSL Support	54
Chapter 12	Configuring DNS	
	About the Domain Name System	55
	Configuration Procedures.....	56

Chapter 13 Configuring SNMP	
About SNMP and the device server Agent	57
Configuration Procedure: Web Interface	58
Chapter 14 Configuring Users	
About Configuring Users	59
Configuration Methods	59
Common User Features	59
Configuring a User: Web Interface	60
Commands for Configuring a User	60
Chapter 15 Configuring Console Management	
About Console Management	61
Configuring Ports	61
Configuring SSH	61
Accessing Attached Devices	63
Securing Console Access	65
Power Management	66
Configuring Port Buffering	69
Configuring User Menus	69
Chapter 16 Managing the OS and Configuration	
Upgrading the Firmware	71
Copying the Configuration to and from a Remote Host	71
Resetting Device Server Configuration to Defaults	72
Commands for Resetting the Configuration to Defaults	73
Chapter 17 Troubleshooting	
Symptom: PortServer TS 8/16 Does Not Boot	75
Symptom: Cannot Telnet to the PortServer TS 8/16	75
Symptom: Trouble Accessing a Port	76
Procedure: Running the POST Using the LEDs	77
Procedure: Running the POST from a Terminal	77
Verifying TFTP on a UNIX System	78
Troubleshooting TFTP Problems	78
Resetting PortServer TS 8/16 Configuration to Defaults	79
Command Line Procedure	79
Front Panel Procedure	79
Verifying the PortServer TS 8/16 IP Address	79
Checking for Duplicate IP Addresses	80
Pinging an IP Address	80
Verifying the Network Cabling	80
Verifying the RealPort Process: AIX	81

Verifying the RealPort Process: HP-UX	81
Verifying the RealPort Process: Linux	81
Verifying the RealPort Daemon: SCO	81
Verifying the RealPort Process: Solaris.....	82
Verifying the RealPort Service: Windows NT	82
Verifying the RealPort Service: Windows 2000	82
Checking and Changing Port Configuration	82
Digi Contact Information	84
Chapter 18 Specifications	
Specifications	85
FCC Part 15 Class A	88
ICES 003 Class A.....	89
Digi Contact Information	89
Index.....	91

Setup Overview

This section provides an overview of the setup process.

Step A: Plan

Before beginning setup, consider the following:

- How to assign an IP address to the Digi device's Ethernet interface, which can be accomplished in a number of ways. See "Configuring the IP Address" on page 11.
- How to configure serial ports. A key consideration is whether to use RealPort. Other considerations include the type of peripheral that will connect to the port and the peripheral's cabling requirements. See "Configuring Ports for RealPort" on page 15 and the online RealPort driver documentation and Cable Guide, both of which are on the Access Resource CD.
- The various ways that your Digi device can be configured. See "About Configuration Methods" on page 9 and "Configuration Pre-requisites" on page 10 for more information.

Step B: Set Up the Hardware

1. Connect the device to power and to the network.
2. Connect peripherals to serial ports. See the Cable Guide on the Access Resource CD.

Step C: Install and Setup Digi Port Authority-Remote

Digi Port Authority-Remote is a utility that provides one of the ways to configure an IP address and also provides port monitoring. See the *Digi Port Authority-Remote Device Monitor Setup Guide*, which is on the Access Resource CD.

Step D: Configure an IP Address

There are a number of ways to configure an IP address. See "Configuring the IP Address" on page 11 for more information.

Step E: Configure Ports

See the following for more information:

- "Configuring Ports for RealPort" on page 15
- "Configuring Ports for Printers" on page 19
- "Configuring Ports for Modems" on page 23
- "Configuring Ports for Terminals and Computers" on page 27

Step F: Configure Other Features as Required

See the following for information on setting up other features:

- "Configuring PPP" on page 29
- "Configuring Autoconnection" on page 35
- "Configuring IP Routing" on page 41
- "Configuring Security Features" on page 47
- "Configuring DNS" on page 55

About Entering Commands on the Command Line

If you use the command line, you will find the commands needed within each chapter. For detail such as syntax, parameters, range, variables, or applications see the *Digi One/PortServer TS Command Reference* found on the Access Resource CD.

Supported Devices

This manual provides information on the following Digi devices:

- PortServer TS 8
- PortServer TS 16

About This Guide

Purpose

This guide provides the following:

- Configuration and administration procedures
- Configuration examples

Audience

This manual is intended for the person responsible for configuring and administering device server. It assumes that this person has experience configuring network devices and is familiar with networking concepts.

Scope

This manual provides step-by-step instructions for configuring and administering device server's main features. It does not address how to configure every option, provide complete information on commands, or discuss hardware installation. These topics are covered in other documents in the device server library.

Other Documents in the Library

Here is a list of the other documents in the library:

Device Server Quick Start Guide

The guide that comes in the package with the device server covering the first steps necessary to get your device server up and running.

Digi One/PortServer TS Command Reference

This online manual, available on the Access Resource CD, provides complete information on commands.

RealPort Setup Guides

These online manuals provide information on setting up servers for RealPort software.

Digi Port Authority - Remote Device Monitor Setup Guide

This online manual provides information on installing and using Digi Port Authority - Remote software.

Online Help for the Web UI

This context-sensitive online help provides information on configuration fields used with web browser configuration interface.

About Configuration Methods

Use this section to learn about configuration methods.

Configuring the device server from an Attached Terminal

With this method, you cable a terminal or PC running terminal emulation software to a device server port and then use the command line to enter commands. This method allows you to configure all features. It requires, however, that you and the device server be in the same location. Some users find it advantageous to configure the device server IP address this way and then use one of the other methods for the rest of the configuration.

Configuring the device server from a Telnet Session

With this method, you Telnet to the device server and use the command line to complete configuration tasks. The only disadvantage to this method is that you have to configure the device server with an IP address before you can Telnet to it.

Configuring the device server from the Web Interface

The great advantage to this method is ease of use. This method requires that you configure the IP address before you can access the configuration from the web interface, however, some features cannot be configured this way.

Downloading a Configuration File

With this method, you configure a Digi device and then do the following:

1. Download an existing configuration file to a host system.
2. Edit the file with specific configuration using a text editor.
3. Upload the file to the device server.

This an excellent method for maintaining highly similar configuration files for multiple Digi devices. The disadvantage is that the device server requires some configuration steps, such as the IP address, to be completed before it can be used.

Configuration Prerequisites

Accessing the Command Line from a Locally-Connected Terminal

Use this procedure to access the command line and the configuration from a terminal connected to one of the device server's serial ports.

1. Connect a terminal or PC to a serial port on the device server. For a Windows HyperTerminal connection, use the cable that came in the package.
2. Configure the parameters of the terminal or terminal emulation software to work with the Digi serial port. The default port settings are:
 - VT 100 emulation
 - 9600 baud
 - 8-bit character
 - 1 stop bit
 - No parity
3. Log on as the `root` user. The default password is `dbps`.

Log On as Root from the Command Line

1. At the log on prompt, enter `root`.
2. Enter the default password `dbps`.

Accessing the Command Line from a Telnet Session

Use this procedure to access the command line and the configuration from a Telnet session. This procedure assumes that you have configured the Digi device with an IP address already. See "Configuring the IP Address" on page 11.

1. To Telnet to the device server, enter the following command from a command prompt on another networked device, such as a server:

```
telnet ip-address
```

where *ip-address* is the device server's IP address

Example: `telnet 192.3.23.5`

2. Log on as the `root` user. The default password is `dbps`.

Accessing the Configuration from the Web Interface

Use this procedure to access the configuration from the web interface. This procedure assumes that you have configured the Digi device with an IP address already. See "Configuring the IP Address" on page 11.

1. Access the device server from a web browser by specifying the device server's IP address in the URL window.
2. Log on as `root`. The default password is `dbps`.

Options for Configuring the IP Address and Mask

The device server IP address can be configured using the following methods:

- With Digi Port Authority-Remote, a Digi utility
- By updating the ARP table on a server and then pinging the Digi device (called ARP-Ping)
- From the command line using the set config command (Configuring the Ethernet Interface from the Command Line)
- Using a RARP server
- Using a DHCP server

The IP address and mask can also be changed using the web interface. This method, however, does not work for the initial IP address configuration.

Device Support: Digi Port Authority-Remote and ARP-Ping for IP Address Configuration

Not all Digi devices can use Digi Port Authority-Remote and ARP-Ping for IP address configuration. To determine if you can use these features, find the hardware label on your Digi device and then use the table below to determine whether this feature is available:

Device	Part Number	Revision Required
Digi One IA RealPort	50000764-01	F or higher
Digi One RealPort	50000723-01	J or higher
PortServer TS 2	50000723-02	J or higher
PortServer TS 4	50000723-03	G or higher
PortServer TS 8	50001208-01	B or higher
PortServer TS 16 (desktop)	50001207-01	E or higher
PortServer TS 16 (rack-mounted)	50001185-01	C or higher

Configuring the Ethernet Interface with Digi Port Authority-Remote

Use this section to configure an initial IP address, subnet mask, and default gateway using Digi Port Authority-Remote. This procedure cannot be used to change the IP address, but only to assign the initial IP address. It also cannot be used if a DHCP server is active.

Starting Point

This procedure assumes the following:

- That your Digi device supports this feature. See "The IP address and mask can also be changed using the web interface. This

method, however, does not work for the initial IP address configuration." on page 11.

- That your Digi device is connected to the Ethernet network.
- That the Digi device has DHCP client turned on. This is the default setting and it will be on unless it was turned off.
- That you do **not** have a DHCP server to serve IP address. If you do, use the DHCP procedure. See "Configuring an IP Address using DHCP and RARP" on page 14.
- That you have installed Digi Port Authority-Remote version 2.01.11 or later. For information on installing Digi Port Authority-Remote, see the *Digi Port Authority Remote Device Monitor Setup Guide*, which is on the Access Resource CD.

Procedure

1. Run Digi Port Authority-Remote.
2. If Digi Port Authority-Remote is not set for ADDP, choose ADDP as the Discovery Protocol.
3. Click Discover.

A list of Digi devices appears. Systems with IP addresses of 0.0.0.0 need IP addresses.

4. Select a device from the list and then click Configure.
5. Supply an IP address, subnet mask, and default gateway and then choose OK.

Digi Port Authority-Remote configures the IP address, subnet mask, and default gateway.

Configuring the IP Address Using ARP-Ping

Use this section to configure an IP address by manually updating a server's ARP table and then pinging the Digi device.

Note: The ARP-Ping command assigns the IP address you designate but also assigns default subnet mask and gateway addresses. It is necessary to change the subnet mask and gateway addresses.

Starting Point

This procedure assumes the following:

- That your Digi device supports this feature. See "The IP address and mask can also be changed using the web interface. This method, however, does not work for the initial IP address configuration." on page 11.
- That your Digi device is connected to the Ethernet network

Procedure

1. Record the MAC address of the Digi device. It's on the back of the unit.
2. Access a server on the same subnet as the Digi device.

3. Manually update the server's ARP table using the Digi device's MAC address and the IP address you want assigned to the Digi device. The following is an example of how this is done on a Windows NT 4.0 system:

```
arp -s 143.191.2.1 00-00-9d-22-23-60
```

4. Ping the Digi device using the IP address just assigned. The following is an example:

```
ping 143.191.2.1
```

The ping will probably time out before there is a response from the Digi device.

5. Wait a few seconds and then ping the Digi device again.

The Digi device replies to the ping, indicating that the IP address has been configured.

Configuring the Ethernet Interface from the Command Line

This section discusses how use the command line to configure an IP address, mask, and default gateway for device server's Ethernet interface.

Manual Configuration Procedure

1. To ensure that the IP address you configure is permanent, turn DHCP off by entering the following command:

```
set config dhcp=off
```

2. To configure an IP address for the Ethernet interface, enter the following command:

```
set config ip=ip-address
```

where *ip-address* is the IP address for the Ethernet interface

Example to Set IP Address

```
set config ip=191.143.2.154
```

3. To configure a subnet mask, enter the following command:

```
set config submask=mask
```

where *mask* is the subnet mask for this subnetwork

Example to Set Subnet Mask

```
set config submask=255.255.255.0
```

4. To configure a default gateway, enter the following command:

```
set config gateway=ip-address
```

where *ip-address* is the IP address of the default gateway

Example to Set Gateway Mask

```
set config gateway=191.143.2.46
```

5. Reboot the Digi device at the prompt using the following command:

```
boot action=reset
```

Manual Configuration Example

In this example set config commands configure the Ethernet interface and

the boot command reboot the Digi device, which is required for the address change to take affect.

```
set config ip=192.150.150.10 submask=255.255.255.0 dhcp=off
set config gateway=192.150.150.11
boot action=reset
```

Configuring an IP Address using DHCP and RARP

About DHCP and RARP

When the device server boots, it transmits a DHCP request and a RARP request. This continues until an address is assigned.

Procedure

To use RARP or DHCP follow these steps:

1. Set up an entry for an address on a DHCP or RARP server. If you intend to use RealPort, do the following:
 - Reserve a permanent IP address.
 - Record the IP address. You will need it when you configure the RealPort driver.
2. Power on the device server.

The DHCP or RARP server assigns the device server an IP address.

About RealPort

This section provides a brief introduction to RealPort.

What is RealPort?

RealPort is a feature that allows network-based host systems to use the ports of the device server as though they were the host system's own ports, appearing and behaving as local ports to the network-based host.

RealPort Advantages

RealPort provides the following advantages:

- It expands the number of ports available to the host system.
- It enables device server ports to be treated as if they were directly connected to the host, which means they use all standard operating system interfaces that control baud rate, parity, stop bits, and flow control.
- It enables host administrators to do most of the required configuration on the host, the system with which the administrator is most familiar.
- It dramatically reduces host CPU overhead because multiple terminal or printer sessions are multiplexed over the same TCP/IP connection.

Configuring the RealPort Software

You must install and configure RealPort software on each host that will use RealPort ports. See the RealPort documentation for more information.

Configuration Options

You can configure the device server for RealPort using the web interface. For information on using the web interface, see "Configuring Ports: Web Interface" on page 15.

Configuring Ports: Web Interface

Use this procedure to configure a port from the web interface.

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`.

The default password is `dbps`.



3. From the main menu, select Setup Wizards > RealPort.



4. To complete configuration, choose Next and then follow the prompts.
5. To return to the main Ports menu, choose Ports from the Menu again.

6. To complete RealPort setup, install and configure the RealPort driver.
See the appropriate RealPort setup guide on the Access Resource CD.
To configure Secure RealPort, see set config securerealport in Digi One/
PortServer TS Command Reference.

Configuration Considerations

You should be aware of the following considerations if you intend to configure device server to handle printers.

Using RealPort

RealPort, a feature that allows network-based host systems to use the ports of the device server as though they were the host system's own ports, is an easy and efficient way for printers to use device server ports. For information on this option, see "Configuring Ports for RealPort" on page 15.

Flow Control Tips

Here are some tips to ensure that your printer performs as expected:

- If flow control is necessary, ensure that the printer and device server use the same flow control scheme.
- Some printers that use hardware flow control issue the DTR (data terminal ready) signal when they are ready for data. If so, the DTR pin on the cable from the printer must be wired to an input on the device server port (usually CTS) that can be used for flow control.

Using the lpd Protocol

Here are some tips for configuring the print spooler on your UNIX system when you intend to print using the lpd protocol to a printer attached to device server:

- The number of copies option with lpr is not supported.
- Banner pages are not supported.
- The device server's DNS name or IP address is the remote system's name.
- Queue names must conform to the following conventions:
 - Begin the queue name with one of the following character strings: (a) Use ASCII if you want device server to substitute carriage return and line feed characters for each line feed the system sends. (b) Use raw if no substitution should be performed.
 - After the queue name, insert an underscore character and the number of the device server port to which the printer is attached.
 - If you want to use either of the following options, specify an additional underscore and then the letter that identifies the option: (a) Use **f** to append a form feed character to the end of each file in a print job (b) Use **d** to add a Ctrl-d to the end of each file in a print job. (This is often required by PostScript printers.)

Examples

String	Result
ascii_1	Prints to port 1 and translates CR to CR/LF.
ascii_8_f	Prints to port 8, translates CR to CR/LF and prints a form feed at the end of the job.
raw_1_d	Prints to port 1 with no translation and appends a Ctrl-d to the end of the print job.

Configuring Ports for Printers: Web Interface

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. From the main menu, click Configure > Ports.
4. Choose the port from the port column.
5. Ensure that the Device Type is Printer.
6. Make other changes to the configuration as required. Use the online help for information.
7. If you want to apply this configuration to multiple ports, choose Clone, select the ports for this configuration, and then choose Continue.
8. Click Submit.
9. To return to the main Ports menu, choose Ports from the left navigation bar.

Tips for Telnet and rsh Printing

Here are some tips for handling Telnet and rsh printing:

- If line feed and carriage return problems occur, try supplying a set line command that specifies `onlcr=on`. This converts carriage returns to carriage return/line feeds.
- If you want tab characters (ASCII character 9) converted to 8 spaces, use a set line command that specifies `otab=on`.

Configuring a Port for Direct-Access Printing

Direct access printing allows Telnet users on the LAN to access a port and to issue print commands directly to the printer. This section describes the two ways users can access a printer directly and explains how to configure the port to support each method.

Method 1: Specifying Port Numbers in the Telnet Command

This method allows users to issue Telnet commands that identify the correct port by using TCP port numbers. Users identify the type of connection and port number by specifying one of the following:

For this connection type...	Identify the port by specifying...
Telnet	2000 plus the number of the port. Example: 2002 for port 2.
Raw	2100 plus the number of the port. Example: 2102 for port 2.

User Command Example 1

In this example, a user from the host server, specifies a standard Telnet connection on port 2 of a device server using IP address 199.250.38.15.

```
cat myfile | telnet 199.250.38.15 2002
```

User Command Example 2

In this example, a user, from the host server, specifies a raw Telnet connection on port 2 of a device server using IP address 199.250.38.15.

```
cat myfile | telnet 199.250.38.15 2102
```

- **Note:** To specify a hunt group in the command instead of an individual port, use the group number specified on the `group` field of the `set ports` command that configured the port. See the *Digi One/PortServer TS Command Reference*.

Method 1 Configuration

There is no special configuration required to set up a port for this type of direct access. Simply configure the port for a printer. See "Configuring a Port for Direct-Access Printing" on page 20 for more information.

Method 2: Using Alternate IP Addresses

This method provides similar functions to method 1, except it assigns an IP address to a port.

Method 2 Configuration

To configure an alternate IP address, do the following:

- Configure the port for a printer. See *Configuring a Port for Direct-Access Printing* on page 20 for more information.
- Supply a `set altip` command that specifies the following:

```
set altip group=port-number ip=ip-address
```

where

- *port-number* is the actual port number of a device server port
- *IP-address* is the unique IP address of a port on the device server

Command Line Example

```
set ports range=2 dev=prn
set line range=2 baud=9600 csize=8 stopb=1 parity=n
set flow range=2 cts=on rts=on ixon=off ixoff=off
```

```
set altip group=2 ip=199.250.38.17
```

The following example displays a file on port 2 whose unique IP address is 199.250.38.17:

```
cat myfile | telnet 199.250.38.17
```

Tips on Configuring A Modem

Here are some tips on configuring modems to work with device server:

- Configure the modem so that DCD goes high when it receives an incoming connection request.
- Configure the modem to answer an incoming call only when DTR is high, and to drop the line when DTR goes low.
- For bidirectional connections, it is advisable to configure the non-volatile parameters in the modem for incoming calls. Also configure the modem to reset to these parameters when DTR is dropped.
- Configure the modem to lock the serial line speed at the highest baud rate the modem will accept for reliable data transfer because the device server cannot switch the baud rate of the serial line on a per call basis without reconfiguration.

Note: You may want to consider connecting modems using RealPort, a feature that allows network-based host systems to use the ports of the device server as though they were the host system's own ports. It is an easy and efficient way for modems to use device server ports. For information on this option, see "About RealPort" on page 15.

Configuring Ports for Modems: Web Interface

Use this procedure to configure a port for a modem from the web interface.

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. From the main menu, click `Configure > Ports`.
4. Click the port from the port column.
5. Configure the correct device type. Click `Modem in` for inbound modem connections, `Modem out` for outbound connections, and `Modem` for bidirectional connections.
6. Make other changes to the configuration as required. Use the online help for information.
7. If you want to apply this configuration to multiple ports, click `Clone`, select the ports for this configuration, and then click `Continue`.
8. Click `Submit`.
9. To return to the main `Ports` menu, click `Ports` from the menu again.

Commands for Configuring Ports for Modem Connections

For configuring ports for modem connections use the following commands found in the *Digi One/PortServer TS Command Reference* :

- set ports
- set line
- set flow

Related Information

- If you intend to run PPP traffic over this modem connection, see "Configuring PPP" on page 29.
- For information on setting up the port for autoconnection, see "Configuring Autoconnection" on page 35 of this manual and the set ports command in the *Digi One/PortServer TS Command Reference*.
- If you do not know the operating parameters required by the modem, see the modem documentation.
- For correct cable information of the connection between the device server serial ports and modems, see the *Digi One/PortServer Cable Guide*.
- For more information on configuring dialer and login scripts, see the set script command in the *Digi One/PortServer TS Command Reference*.

Configuring A Hunt Group

A hunt group is a group of ports sharing one common IP address and differs from altip where one port has its own unique IP address. A hunt group is desirable when you have many ports, but do not have the available IP addresses or simply prefer to use one IP address for a group of ports. When a user Telnets into the hunt group's IP address and the first port is busy, the user is seamlessly bumped to the next available port.

In configuring the PortServer for a hunt group, the port numbering must start higher than the total number of PortServer serial ports available.

To configure a group of ports for a hunt group, do the following:

1. Enter the following command to create the hunt group:

```
set ports range=range group=port_number
```

2. Enter the following command to set the IP address for the hunt group:

```
set altip group=port_number ipaddress
```

Command Line Examples

The following example displays the configuration for 16 serial ports in a hunt group with their collective IP address being 199.250.38.37.

```
set ports range=1-16 group=65
set altip group=65 ip=199.250.38.37
```

A user who Telnets to this IP address is automatically connected to the first

available hunt group port.

Configuring Ports for Terminals: Web Interface

Use this procedure to configure a port from the web interface.

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. From the main menu, choose `Configure > Ports`.
4. Choose the port from the port column.
5. Ensure that the Device type is set to Terminal.
6. Make changes to the configuration as required. Use the online help for information.
7. If you want to apply this configuration to multiple ports, choose `Clone`, select the ports for this configuration, and then choose `Continue`.
8. Choose `Submit`.
9. To return to the main Ports menu, choose `Ports` from the Menu again.

Commands for Configuring Ports for Terminals

- `set ports`
- `set line`
- `set flow`

Port Defaults

- VT-100 emulation
- 9600 baud
- 8-bit characters
- 1 stop bit
- No parity
- Software flow control

Related Information

- For information on the `set line`, `set ports`, and `set flow` commands, see the *Digi One/PortServer TS Command Reference*.
- For information on configuring terminal ports for autoconnections, see, "Configuring Autoconnection" on page 35.

Note: The set line settings must match the settings of the attached terminal or

device.

About Computer Connections

Configuring computer connections is very similar to configuring terminal connections, which is discussed on page 27. Consequently, this section simply discusses the differences between these connection types.

Starting Point

This section assumes that

- You are logged on as root
- You know the attributes, such as baud rate and parity, of the PC that will be connected to this port

Configuring Typical PC Connections

To configure a port for a directly-connected PC, where the PC always initiates the connection, configure the connection as you would a terminal connection, except on the set ports command do the following:

- Specify dev=min if you have a 10-pin null modem cable to support this type of connection.
- Specify dev=term if you do not have a 10-pin null modem cable

Consider defining the serial connection as a PPP link. See "Configuring PPP" on page 29 for more information.

Configuring Inbound PPP Connections: Command Line

Use this section to configure simple inbound PPP connections from the command line. For information on fine-tuning PPP connections, see the set user command in the *Digi One/PortServer TS Command Reference*.

Note: CHAP authentication works between two Digi devices. CHAP will be negotiated to PAP for all other connections

Procedure

1. To configure the port for a modem, enter the following command:

```
set ports range=range dev=device
```

where *range* is the port or ports and *device* is one of the following:

- min for inbound only modem connections
- mio for bidirectional modem connections.

See the set ports command in the *Digi One/PortServer TS Command Reference* for more information.

Example: `set ports range=3 device=min`

2. To configure flow control for the ports, enter the following command:

```
set flow range=range flow-control=scheme
```

where *range* is the port or ports and *flow-control=scheme* is the flow control required for this connection. Typically, for modem connections RTS and CTS are on.

Example:

```
set flow range=3 ixon=off ixoff=off rts=on cts=on
```

See the set flow command in the *Digi One/PortServer TS Command Reference* for more information.

3. To configure the baud rate for this connection, enter the following command:

```
set line range=range baud=bps
```

where *range* is the port or ports to configure and *bps* is the line speed in bits-per-second. Typically, you can set this to 115000 bps for modem connections.

Example:

```
set line range=3 baud=115000
```

4. To create an inbound PPP user, enter the following command:

```
set user name=name protocol=ppp netservice=on  
    defaultaccess=netservice
```

where *name* is a name to assign the PPP user

Example:

```
set user name=pppin protocol=ppp netservice=on
defaultaccess=netservice
```

5. To configure an IP address for the remote PPP user, enter the following command:

```
set user name=name ipaddr=ip-address
```

where

- *name* is the user's name
- *ip-address* is one of the following: (a) A standard IP address in dotted decimal format. (b) 0.0.0.0, which means the remote user will supply the IP address. (c) *ippool*, which means that the user will be assigned an IP address from an IP address pool. See the `set ippool` command in the *Digi One/PortServer TS Command Reference*.

Example:

```
set user name=pppin ipaddr=ippool
```

6. If you used the IP address pool option in the previous step, specify the following subnetwork mask using the following command: (a mask of 255.255.255.255 is required)

```
set user ipmask=255.255.255.255
```

7. To configure an IP address for the local end of the PPP connection, enter the following command:

```
set user name=name localipaddr=ip-address
```

where *name* is the user's name and *ip-address* is the IP address to assign to the local end of the PPP connection. This address must be unique. That is, no other user can be assigned this address and it cannot be the IP address for the Ethernet interface.

Example:

```
set user name=pppin localipadr=199.1.1.2
```

Configuring Inbound PPP Connections: Example

This example shows a very simple PPP inbound configuration. Here are some points on this configuration:

- The port is set up for inbound connections (`dev=min`).
- RTS and CTS are used for flow control.
- The baud rate has been set to 115000 bps.
- The user has been configured to use an IP address pool

```
set ports range=3 device=min
set flow range=3 ixon=off ixoff=off rts=on cts=on
set line range=3 baud=115000
set user name=pppin protocol=ppp netservice=on
defaultaccess=netservice
set user name=pppin ipaddr=ippool
set user name=pppin localipadr=199.1.1.2
```

Configuring Outbound PPP Connections: Command Line

This section describes how to configure outbound PPP connections. Use it to configure outbound only connections or to configure the outbound portion of bidirectional connections.

Note: CHAP authentication works between two Digi devices. CHAP will be negotiated to PAP for all other connections

Procedure

1. To configure the port for a modem, enter the following command:

```
set ports range=range dev=device
```

where *range* is the port or ports and *device* is one of the following:

- mout for outbound only modem connections
- mio for bidirectional modem connections.

See the set ports command in the *Digi One/PortServer TS Command Reference* for more information.

Example: `set ports range=3 device=mout`

2. To configure flow control for the ports, enter the following command:

```
set flow range=range flow-control=scheme
```

where *range* is the port or ports and *flow-control=scheme* is the flow control required for this connection. Typically, for modem connections RTS and CTS are on.

Example:

```
set flow range=3 ixon=off ixoff=off rts=on cts=on
```

See the set flow command in the *Digi One/PortServer TS Command Reference* for more information.

3. To configure baud rate for this connection to the modem, enter the following command:

```
set line range=range baud=bps
```

where *range* is the port or ports to configure and *bps* is the line speed in bits-per-second. Typically, you can set this to 115000 bps for modem connections.

Example:

```
set line range=3 baud=115000
```

4. If you do not want to use the Digi-supplied dialer script (genmdm) and login script (loginscript), which work for most applications, use the set script command to create your own scripts.

See the set script command in the *Digi One/PortServer TS Command Reference* for more information.

5. If you do not want to use the Digi-supplied outbound device (gendialer), which works for most applications, enter the following command:

```
set device name=name ports=ports dialer=name
```

where

- name=*name* is the name for this device
- *ports* are the ports to associate with this device

- `dialer=name` is the name of a dialer script, either the Digi-supplied script or a user-created one

6. To create a PPP user, enter the following command:

```
set user name=name protocol=ppp
```

where *name* is the name of the PPP user

Example

```
set user name=pppout protocol=ppp
```

7. To configure this user for outbound connections, enter the following command:

```
set user name=name outgoing=on device=device
```

where *device* is either the Digi-supplied device or the outbound device created earlier in this procedure

Example:

```
set user name=pppout outgoing=on device=gendialer
```

8. To configure an IP address for the local end of the PPP connection, enter the following command:

```
set user name=name localipaddr=ip-address
```

where *name* is the user's name and *ip-address* is one of the following:

- 0.0.0.0. , which means that the user will request an IP address from the remote server.
- A specific IP address, which means that the Digi device will attempt to use this IP address. The remote server must agree to this request.

Example:

```
set user name=pppout localipadr=0.0.0.0
```

9. To configure a telephone number to dial to reach the outbound user, enter the following command:

```
set user name=name n1=telephone-number
```

where *name* is the user's name and *telephone-number* is the number to dial to reach the user. You can enter this number as digits only, with dashes (-) separating digits, or with commas.

Example:

```
set user name=pppout n1=4452624
```

Example

This example shows a very simple outbound PPP configuration. Here are some points on this configuration:

- The port is set up for outbound connections (`dev=mout`).
- Flow control is set to Hardware.
- Default device and scripts are used

```
set ports range=3 device=mout
```

```
set flow range=3 ixon=off ixoff=off rts=on cts=on
```



```
set line range=3 baud=115000
set user name=pppout protocol=ppp
set user name=pppout dialout=on outgoing=on device=gendialer
set user name=pppout localipadr=0.0.0.0
set user name=pppout n1=4452624
```

set user Field	Description	Example
pass-packet	Causes a packet to be passed or blocked	Filter causes incoming packets from an IP address to be accepted and packets from all other IP addresses to be blocked
logpacket	Causes the Digi device to send a message to the log file	Filter that notifies the log anytime an ICMP packet is handled

Packet Type	Type Identifier
Echo reply	0
Destination unreachable	3
Source quench	4
Redirect	5
Echo request	8
Time exceeded for a datagram	11
Parameter problem on a datagram	12
Timestamp request	13
Timestamp reply	14
Address mask request	17
Address mask reply	18

About Autoconnection

The autoconnection feature allows you to configure a user to access the device server and then be automatically connected to a host on the LAN. You can implement autoconnection in the following ways:

- By port where all port users are automatically connected to the same host. The device server is completely transparent to them.
- By user where a user is required to log on and may be required to supply a password, but once the user is authenticated, an automatic connection to a host is made.

Configuring a Port for Autoconnection: Web Interface

This section describes how to configure a port for autoconnection from the web interface.

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. Select Configure and then Autoconnect from the menu.
4. Configure the port as required. Use the online help for more information.
5. To return to the main Ports menu, choose Ports from the Menu again.

Commands for Configuring Autoconnection by Port or by User

See the complete list of commands in the *Digi One/PortServer TS Command Reference*. The commands needed for autoconnection either by port or by user will be under the following commands in the Command Reference on your Access Resource CD.

- `set ports`
- `set user`

Configuring a User for Autoconnection: Web Interface

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. Select Configure and then Users from the menu.
4. Choose Add User.
5. Enter a name and then choose Submit
6. Choose the new user from the Name column.

7. Configure the user. Be sure to specify the following: (1) Default Access: Autoconnect (2) Enable Autoconnect (3) The IP address that will be the destination for the autoconnect user (4) A Destination TCP port number, which determines the type of connection for this user (such as 23 for Telnet).
8. Choose Submit.
9. To return to the main User menu, choose User from the Menu again.

Note:

Configuring TCP Socket Communication

TCP socket communication enables serial devices to communicate with each other over an Ethernet network as though they were connected by a serial cable.

This section describes how to use the web interface to configure this Digi device for the following:

- Inbound connections, that is, connections that are initiated by the device on the other side of the network
- Outbound connection, that is, connections that are initiated by the device connected to the serial port

Procedure for Configuring Inbound Socket Communication

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. From the main menu, choose Configure > Port.
4. From the Port configuration screen, set the Device type to Printer, adjust other serial port communication parameters as required by the connected device, and then choose Submit.
5. Choose Advanced, check Binary Mode and then choose Submit.

Procedure for Configuring Outbound Socket Communication

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. From the main menu, choose Configure > Port.
4. From the Port configuration screen, set the Device type to Modem In, adjust other serial port communication parameters as required by the connected device, then choose Submit.

Note: The Terminal type field does not matter.

5. To configure the port to launch an automatic connection, choose Advanced.
6. Choose Enable Autoconnect
7. Specify the IP address of the slave.

8. Specify a TCP port to use for this connection. If this is a connection to a serial port on another Digi device and you have not changed the base socket service, use the following conventions to specify a TCP port number:

For This Type of Connection...	Specify ...	Example
Telnet	2000 + port number	To specify port 1, use 2001
Raw connection	2100 + port number	To specify port 2, use 2102

9. If you want the autoconnection to launch immediately, choose Force DCD.
10. Choose Binary Mode.
11. When you complete the configuration process, choose Submit.

Note: For more flexible base socket configuration, see socket parameter in set config in Digi One/PortServer TS Command Reference.

Configuring UDP Multicast

The Digi One and PortServer TS devices are devices capable of UDP multicast. UDP multicast is used to send serial data over an Ethernet cable to one or many hosts at the same time. UDP is a connectionless protocol, meaning UDP does not need a protocol, but is sending data without any form of acknowledgement or error correction. Up to 64 devices can receive a UDP multicast at one time. Both the transmitting and receiving devices must be configured properly for UDP multicast to work.

This section describes how to use the web interface to configure this Digi device for the following:

- Inbound connections, that is, connections that are initiated by the device on the other side of the network
- Outbound connection, that is, connections that are initiated by the device connected to the serial port

Procedure for Configuring Outbound Socket Communication

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the Digi One/PortServer TS as `root`. The default password is `dbps`.
3. From the main menu, choose Configure > Port.
4. From the Port configuration screen, set the Device type to Printer, adjust other serial port communication parameters as required by the connected device, and then choose Advanced.

Note: The serial parameters for two connecting devices must match meaning if one device is set for 9600 bps, the other device must be set for the same rate.

- Choose UDP serial... at the bottom of the page. The UDP Serial Configuration page is displayed.

Delimiting string configuration

Forward buffer when the following string is found

- CR (carriage return)
- CR/LF (carriage return/line feed)
- Custom string

Strip string before forwarding

Timer/idle delay settings

Forward buffer after the following number of milliseconds

ms (1-60000)

- System default
- Disabled

Buffer settings

Forward buffer after the following number of bytes

bytes (1-4k)

- System default

Destination list:

Description	IP Address	UDP Port
<input type="button" value="Add destination"/> <input type="button" value="Submit"/> <input type="button" value="Help"/>		

- Fill in the requested information and choose Add destination at the bottom of the page. See the Help section for additional information on the settings.
- Scroll to the bottom of the page. Under Description, choose updstest1.
- Enter the requested information and choose Submit. You can change the Description as desired. The IP address is the destination device server's address and the UDP port uses a base socket number of 2100 for UDP. The first port would be port number 2101.
- Repeat these steps until you have added the necessary destinations.

Procedure for Configuring Inbound Socket Communication

- Access the web interface by entering the Digi One/PortServer TS IP address in a browser's URL window.
- Log on to the Digi One/PortServer TS as `root`. The default password is `dbps`.
- From the main menu, choose Configure > Port.

4. From the Port configuration screen, set the Device type to Printer, adjust other serial port communication parameters as required by the connected device, and then choose Submit.

Configuring Static Routes

This section describes how to configure device server for static routes.

Related Information

See the `set route` command in the *Digi One/PortServer TS Command Reference*.

Procedure

To configure a static route over a PPP link, enter the following command:

```
set route net=addr mask=mask metric=hops wanname=interface
      gateway=gateway
```

where

- *addr* is either the IP address of a system to be reached over this route or the network address of the subnet that is to be reached on this route
- *mask* is the mask to use for interpreting the IP address.
- *metric* is the number of hop to the destination
- *interface* is either `ether` if this route is over the Ethernet interface or the name of a user if the route is over a PPP link
- *gateway* is the IP address of the device that is the next hop to the destination

Example: Route Using the Ethernet Interface

In this example, a route to a subnet is created over the Ethernet interface. Key features include the following:

- The address on the `net` field is a subnetwork address, not the IP address of a specific device
- The `wanname=ether`, indicating that this route is over the Ethernet interface
- The `metric` field indicates that packets to this subnet will pass through two routers
- The `gateway` field indicates that all packets using this route are to be forwarded to the device at IP address 191.21.21.2.

```
set route net=199.21.33.0 mask=255.255.255.0 metric=2
      wanname=ether gateway=199.21.21.2
```

Example: Route Using a PPP Link

In this example, a route to a subnet is created over a PPP interface. Key features include the following:

- The address on the net field is IP address of a specific device, not a subnetwork address
- The wan name is the name of a PPP user.
- The metric field indicates that packets to this subnet will pass through two routers
- The gateway field indicates that all packets using this route are to be forwarded to the device at IP address 191.21.21.2.

```
set route net=199.21.33.44 mask=255.255.255.255 metric=2
  wannname=ppp1 gateway=199.21.21.2
```

Configuring Dynamic Routes Using RIP

This section describes how to configure device server for dynamic routing.

Related Information

See the set forwarding command in the *Digi One/PortServer TS Command Reference*.

Starting Point

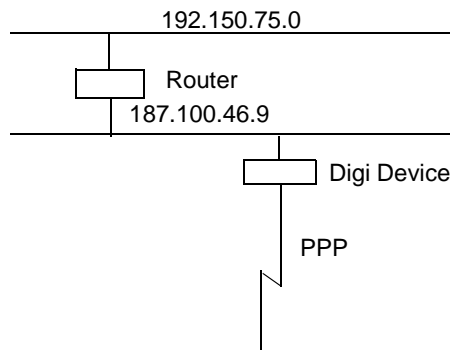
This procedure assumes that you have signed on as root and have or will configure modems, modem scripts, devices, and filters for routes that use serial lines.

Procedure

1. Configure the links over which routed packets and RIP updates will be sent.
 - To enable routing over the LAN to which device server is attached, no routing-specific configuration is required.
 - To enable routing over PPP links be sure to use the netrouting field on the set user command to configure how device server handles RIP updates. You can configure the link so that device server does any of the following with RIP updates:
 - Both sends and receives them (netrouting=both)
 - Sends them only (netrouting=send)
 - Receives them only (netrouting=receive)
 - Neither sends nor receives them (netrouting=off)
2. Configure the device server for dynamic routing with a set forwarding command that specifies state=active.

Example: Dynamic Routes

In this example, which shows only those commands and command fields pertinent to routing, device server is configured for dynamic routing using RIP. But to prevent RIP updates from being sent across the PPP link, the set user command that defines the link specifies netrouting=off.



```
set forwarding state=active poisonreverse=on splithorizon=on
set user name=link1...netrouting=off
```

Configuring Proxy ARP

This section describes how to configure device server for Proxy ARP.

Related Information

See the set forwarding command in the *Digi One/PortServer TS Command Reference*.

Starting Point

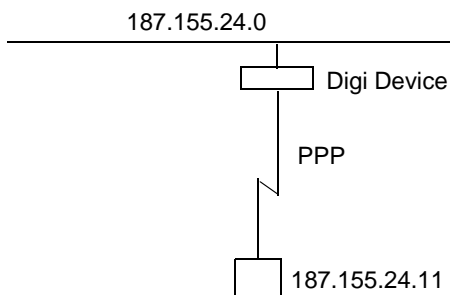
This procedure assumes that you have signed on as root and have or will configure modems, modem scripts, devices, and filters for routes that use serial lines.

Procedure

1. Configure the links over which packets will be routed using a set user command. This command must specify (on the ipaddr field) a specific IP address for the remote system using the Proxy ARP service.
2. Configure device server for Proxy ARP by supplying a set forwarding command that specifies the following:
 - state=passive
 - proxyarp=on

Example

In this example, device server provides Proxy ARP services to a remote host.



```
set user name=link1...ipaddr=187.155.24.11
set forwarding state=passive proxyarp=on
```


About Modbus

Modbus is a protocol that defines how devices in an industrial automation (IA) environment communicate. It specifies that a controlling unit, called a master, manages one or more units, called slaves. The protocol specifies that only the master may initiate communication. Slaves may only respond.

The protocol defines the structure of Modbus messages, determines how the master requests information from the slave or specifies an action for the slave to take, defines how the slave is to respond, specifies addressing conventions, and deals with many of the other details required for communication to occur. Modbus defines two encoding schemes, Modbus ASCII and Modbus RTU. Each Modbus device uses one or the other.

Designed to function over a serial communication cable, Modbus has been extended in recent years to function over an Ethernet network using Modbus/TCP, which defines a method of encapsulating Modbus ASCII or Modbus RTU messages in IP packets for transport over the network.

The extremely flexible Digi implementation includes support for Modbus ASCII, Modbus RTU, Modbus/TCP, and two other methods of transport over a network, TCP socket and UDP socket communication. The implementation enables multiple network-based masters to concurrently initiate communication with serial-based slaves using any of the supported network protocols.

Modbus Configuration Procedure: Web Interface

1. Access the web interface.
2. Sign in as root. The default password is `dbps`.
3. Choose Setup Wizard > Industrial Protocols.
4. Use the wizard to complete configuration tasks. Here are a few tips:
 - Configure the serial port for the serial communication parameters (baud rate, data bits, parity and stop bits) required by the connected IA device.
 - Choose Modbus ASCII or Modbus RTU as the serial port protocol, depending on the requirements of the IA device connected to the port.
 - If you configure the port for a slave, you do not have to configure a network-based master. Communication with the master just works. (If the master is connected to a serial port, it must be configured, however.)

- If you configure a port for a master and the slaves are located on the network, TCP sockets, UDP sockets, and Modbus/TCP are all supported. Use the protocol required by the master.

Configuring the User-Defined Protocol

Digi One\PortServer TS 2/4 MEI devices support what Digi calls the “user-defined” protocol, which is any IA serial-port protocol with the following attributes:

- All message packets are bounded by fixed header and trailer strings.
- Each protocol request is followed by a single response.

Procedure

1. Access the web interface.
2. Sign in as root. The default password is `dbps`.
3. Choose Setup Wizard > Industrial Protocols.
4. Use the wizard to complete configuration tasks. Here are a few tips:
 - Configure the serial port for serial communication parameters (baud rate, data bits, parity and stop bits) required by the connected IA device.
 - Choose User-defined as the serial-port protocol.
 - If you configure the port for a slave, you do not have to configure a network-based master. Communication with the master just works. (If the master is connected to a serial port, it must be configured, however.)
 - If you configure a port for a master and the slaves are located on the network, TCP sockets and UDP sockets are supported options.

Controlling Access to the Configuration

Controlling access of device server restricts access to the configuration by defining the following types of users:

- The root user, who has unlimited access to device server commands. He or she can view any configuration table and change any configuration parameter. The root is identified by the user name `root` and must supply a password to be authenticated. The default root password is `dbps`. You should change this password immediately.
- Regular users, who have much more restricted access to device server commands. Regular users can view some configuration tables and can change some configuration parameters related to their own sessions and passwords. See the *Digi One/PortServer TS Command Reference* for information on the limitations placed on regular users for each command.

Controlling Access to Inbound Ports

This section describes methods of controlling access to inbound serial ports. An inbound port is one defined on the `dev` field of the `set ports` command for one of the following device types:

- `term` (used to define terminal connections)
- `min` (used to define incoming modem connections)
- `mio` (used to define bi-directional modem connections)
- `hdial`, `hio` (used to define computer connections)

Default Access Restrictions

The default configuration for inbound ports is that a login and password are required to access them.

Options for Removing Access Restriction

The login and password requirement for inbound ports can be changed by configuring

- The port so that it does not require a login and password. In this case, no one is required to supply a login or password.
- Specific users so that they do not require a password. In this case, some users do not supply passwords, and others are required to.

Procedure for Changing a Port's Access Requirements

To configure a port so that no one has to login or specify a password,

supply a set logins command that specifies the following:

```
set logins range=range login=off passwd=off
```

Example:

```
set logins range=1-2 login=off passwd=off
```

Procedure for Changing a User's Access Requirements

To configure a user so that he or she does not have to specify a password when accessing an inbound port, supply a set user command that specifies the following:

```
set user name=name password=off
```

where *name* is a name to identify the user

Example:

```
set user name=user1 password=off
```

Controlling Access to Outbound Ports

This section describes methods for controlling access to outbound serial ports. An outbound port is one defined on the dev field of the set ports command for one of the following device types:

- prn (used to define printer connections)
- mout (used to define outbound modem connections)
- mio (used to define bi-directional modem connections)
- host (used to define host connections)

Default Access

The default for outbound ports is unlimited access.

Restricting Access to Outbound Ports

Use the set auth command to restrict access to outbound ports. See the description of the set auth command in the *Digi One/PortServer TS Command Reference* for more information.

CHAP Authentication for PPP Users

CHAP authentication can be used to restrict PPP user access to outbound ports. For more information on CHAP configuration, see the set user command in the device server *Command Reference*.

Controlling Access to the Command Line

This section describes how to restrict access to the device server command line.

Method 1 Autoconnection

The autoconnection feature allows you to configure a user to access the

device server but then be automatically connected to a host on the LAN. You can implement autoconnection in the following ways:

- By port where all port users are automatically connected to the same host. The device server is completely transparent to them.
- By user where a user is required to login and may be required to supply a password, but once the user is authenticated, an automatic connection to a hosts made.

For information on configuring autoconnection, see "Configuring Autoconnection" on page 35.

Method 2: Menus

Menus select destination systems without having to access the device server command line. For information on configuring menus, see the description of the set menu command in the *Digi One/PortServer TS Command Reference*.

Using RADIUS to Authenticate Users

This section provides a description of RADIUS and explains how to configure device server to use RADIUS. Digi device and terminal servers are capable of authenticating reverse Telnet users with RADIUS. The Service-Type attribute of the RADIUS server must be defined correctly for the Digi devices to grant access.

What is RADIUS?

RADIUS (remote authentication dial-in user service) is a method of maintaining a database of profiles of dial-in users. These profiles can include login and password information, as well as other user attributes.

RADIUS Components

RADIUS requires two components, an authentication host server and client protocols. The device server implements the client protocol. A host must implement the authentication server application.

RADIUS Table Key

The numbers in the following tables have the following meaning:

#	Meaning
0	This attribute must <u>not</u> be present.
0+	Zero or more instances of this attribute may be present.
0-1	Zero or one instance of this attribute <u>may</u> be present.
1	Exactly one instance of this attribute <u>must</u> be present.

RADIUS Attributes (RFC 2138) Supported

The following attributes are supported in the Digi device server RADIUS

client implementation.

Request	Accept	Reject	Challenge	#	Attribute
1	0	0	0	1	User-Name
0-1	0	0	0	2	User-Password
0-1	0	0	0	3	CHAP-Password
0-1	0	0	0	4	NAS-IP-Address
0-1	0	0	0	5	NAS-Port
0-1	0-1	0	0	6	Service-Type
0-1	0-1	0	0	7	Framed-Protocol
0-1	0-1	0	0	8	Framed-IP-Address
0-1	0-1	0	0	9	Framed-IP-Netmask
0	0-1	0	0	10	Framed-Routing
0	0+	0	0	11	Filter-Id
0	0-1	0	0	12	Framed-MTU
0+	0+	0	0	13	Framed Compression
0+	0+	0	0	14	Login-IP-Host
0	0-1	0	0	15	Login-Service
0	0-1	0	0	16	Login-TCP-Port
0	0-1	0	0-1	27	Session-Timeout
0	0-1	0	0-1	28	Idle-Timeout

RADIUS Accounting Attributes (RFC 2139)

The following RADIUS accounting attributes are supported in the Digi device server.

#	Attribute	#	Attribute
0-1	User-Name	0-1	Login-TCP-Port
0	User-Password	0-1	Session-Timeout
0	CHAP-Password	0-1	Idle-Timeout
0-1	NAS-IP-Address	1	Acct-Status-Type
0-1	NAS-Port	0-1	Acct-Delay-Time
0-1	Service-Type	0-1	Acct-Input-Octets
0-1	Framed-Protocol	0-1	Acct-Output-Octets
0-1	Framed-IP-Address	1	Acct-Session-Id
0-1	Framed-IP-Netmask	0-1	Acct-Authentic
0-1	Framed-Routing	0-1	Acct-Session-Time
0+	Filter-Id	0-1	Acct-Input-Packets
0-1	Framed-MTU	0-1	Acct-Output-Packets
0+	Framed-Compression	0-1	Acct-Terminate-Cause
0+	Login-IP-Host	0-1	Port-Limit
0-1	Login Service		

How RADIUS Works

Here is how authentication works when device server is configured for RADIUS:

- A user logs into device server.
- device server collects login information and then checks to see if the user is in the local database of users.
- If the user is in the local database, device server handles authentication.
- If the user is not in the local database, device server submits an authentication request to the RADIUS server.
- The RADIUS server does one of the following:
 - If the user is validated, it passes this information to other devices and the user is permitted access.
 - If the user is not validated, the RADIUS server returns an access reject message to device server, which then denies access to the user.

Configuring RADIUS: Web Interface

Use this section for information on configuring device server as a RADIUS client from the web interface.

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. From the main menu, choose `Configure > RADIUS`.
4. Configure the RADIUS client as required. Use the online help for information on configuration fields.
5. When you complete configuration, choose `Submit`.

Configuring RADIUS: Command Line

To configure device server to function as a RADIUS client, supply a `set radius` command that specifies the following:

- `run=on`
- The IP address of the primary RADIUS server (on the `primary` field). The primary server is the first server to which authentication requests are sent.
- A password (on the `secret` field)

Note To use a secondary RADIUS server, supply a second `set radius` command that specifies `run=on`, the IP address of the secondary server (on the `secondary` field) and another password for the secondary server (on the `secret` field).

RADIUS Command Line Configuration Example

```
set radius run=on primary=199.123.15.129 secret=J9CxegpP
```

Issuing User Passwords

This section discusses how to issue user passwords.

Related Information

See the `newpass` and `set user` commands in the *Digi One/PortServer TS Command Reference*.

Starting Point

This procedure assumes that you have signed on as root and already configured the user to whom you will be issuing a password.

Procedure

1. Issue a `newpass` command that identifies the user (on the name field) to whom this password will be issued.
2. When the system prompts you for a new password, type in the password and then press Enter.
3. When the system prompts you to enter the new password again, type it in and then press Enter.

Configuring SSH Version 2 for Secure Communication

This section discusses how to configure a user for SSH version 2 encryption.

Password Protection

To configure simple password authentication for an SSH user, no SSH-specific configuration is required. Simply configure a user by entering the following commands:

```
set user name=name password=on
newpass name=name
```

where *name* is a user name

Example

```
set user name=ssh-user1
newpass name=ssh-user1
```

Using a Public Key

To enable public key authentication and to associate a public key with a user, enter the following command:

```
set user name=name loadkey=host:key
```

where

- *name* is the name of a user
- *host* is either an IP address or DNS name of a host running TFTP that holds

- *key* is the name of a file that contains the DSA public key. If your host's implementation requires a complete path to the file, specify the path here as well.

Example:

```
set user name=secure loadkey=143.191.2.34:ssh-file
```

Making Reverse SSH Connections to Ports

The convention used to identify a port for a reverse SSH connection to a Digi device is to use 2500 + the port number. See the examples that follow for more information.

Note: Only PortServer TS 8/16 supports reverse SSH version 2 server.

Example: Reverse SSH Connection to Port 1

```
ssh 192.1.1.2.3 2501
```

Example: Reverse SSH Connection to Port 4

```
ssh 192.1.1.2.3 2504
```

Controlling Access to Services

This section describes how to disable services, such as Telnet and Rlogin, for inbound users, which means that they cannot access the Digi device using those services. This feature allows you to turn off individual services or to specify a security level, which means that all services not included in that level are turned off.

Services that Can Be Turned Off

The following services can be turned off.

- HTTP
- HTTPS
- RealPort
- Reverse TCP
- Reverse Telnet
- Remote login
- Remote shell
- SSL
- SNMP
- SSH
- Telnet

Service Levels

These are the secure access levels:

- Secure, which means that SSH is the only service available to inbound users
- High, which means that SSH, HTTP, HTTPS, SNMP, and RealPort services are available to inbound users
- Normal, which means all services are available
- Custom, which means you can select services to turn off.

The default service level is normal, which means that all services are available.

Procedure

Use this topic for information on using the web interface to turn services off.

1. Access the device server from a web browser by entering the Digi device's IP address in the URL window.
2. Log on as `root`. The default password is `dbps`.
3. From the main menu, choose Secure Access.
4. Use the wizard to disable services that you do not want to make available to inbound users. Use the context sensitive help for information on configuration fields.

SSL Support

Introduction

The device server supports communication over the Secure Socket Layer (SSL). Applications running on networked systems and devices can initiate secure communication with a device connected to a Digi serial port by using the SSL TCP port.

Setting Up for SSL Connections

No device server configuration is required to use SSL unless the application cannot use the default SSL TCP port, which can be changed using the sockets field on the set config command. See the *Digi One/PortServer TS Command Reference* for more information.

Initiating an SSL Connection with a Digi Device

The formula for determining the correct TCP port is the following: **base socket + port + 600**. See the following examples, which use the default base socket (2000), to clarify how this works.

To Connect to ...	Use This Command ...	Example
Port 1	telnet <i>ip-address</i> 2601	Telnet 192.2.2.1 2601
Port 2	telnet <i>ip-address</i> 2602	Telnet 192.2.2.1 2602

About the Domain Name System

This section discusses key concepts of the domain name system.

Purpose of DNS

The domain name system maps domain names to information associated with these names, such as IP addresses.

DNS Components

DNS components include:

- A distributed database consisting of domain names and associated information
- A hierarchical system of domain name servers that maintain the database and use it to respond to requests for information about a particular domain name, such as its IP address
- Domain name resolvers that
 - Accept requests from users
 - Satisfy information requests by building and submitting properly formulated queries to one or more name servers or by retrieving information from a local host file
 - Return information to users
 - Cache information for future use

Types of Name Servers

There are two types of name servers in the domain name system:

- Local servers maintain information for resources within a local zone. It is up to individual network administrators to determine the scope of a local zone.
- Root servers maintain information in higher-level domains than do local servers.

Typically, when a user requires information about a domain name, the resolver queries a local server. If local servers cannot provide the information, root servers are queried next.

Naming Conventions

Each node in the domain name system has a globally unique domain name that consists of its own name, which is called a label, and the labels of all superior nodes.

DNS Name Example

Here is an example of a domain name. Note that labels are separated by

periods:

```
mn07.amalgamated.com
```

In this example, mn07 is part of the higher-level domain called amalgamated.com.

Configuration Procedures

Procedure for Using a Name Server

To configure a DNS server, enter the following command:

```
set config domain=domain myname=name dns=ip-address
```

where

- *domain* is the domain in which the device server will reside
- *name* is a DNS name for device server
- *ip-address* is the IP address of a name server

Example:

```
set config domain=digi.com myname=poe dns=204.221.1.4
```

Procedure for Using a Host File

Use this section to configure the host table, which maps IP addresses to host names.

Enter the following command

```
set host name=name ip=ip-address
```

where

- *name* is the name the host
- *ip-address* is the IP address of the host

Example

In this example, three IP address-to-name mappings are configured

```
set host name=poe ip=204.221.110.200  
set host name=gary ip=204.221.110.202  
set host name=toni ip=204.221.110.203
```


About SNMP and the device server Agent

This section introduces SNMP and network management in TCP/IP networks, and it describes the device server agent. It discusses the following:

- Network management components
- The SNMP agent
- SNMP traps
- The device server agent's MIB support
- The device server agent's supported traps

Network Management Components

The TCP/IP network management architecture contains the following components:

- Managed nodes such as host systems, routers, terminal and communications servers (such as device server) and other network devices
- One or more network managers (also called network management stations), which are the points from which the network is managed
- Agents that reside on managed nodes and retrieve management information and communicate this information to network managers
- The network management protocol, SNMP, which governs the exchange of information between the nodes and stations
- Management information, which is the database of information about managed objects. This database is called the management information base (MIB).

SNMP Management Agent

Each managed node contains at least one agent—a component that responds to requests from the network manager—that retrieves network management information from its node and notifies the manager when significant events occur.

SNMP Traps

A mechanism defined by SNMP is called a trap, which is a report or “alarm” from a managed node to an SNMP manager that a significant event has occurred.

MIB Support

The agent supports the following MIBs:

- Read-write for MIB II (RFC 1213), which is an Internet-standard MIB, consisting of managed objects from the systems, interfaces, IP, ICMP, TCP, UDP, transmission, and SNMP group
- Read-write for the character-stream devices using SMIv2 MIB (RFC 1658)
- Read-write for the RS-232-like hardware devices MIB (RFC 1659)
- Read-write for the device server IP Network Control Protocol of the Point-to-Point Protocol MIB (RFC 1473)

Message Support

The SNMP agent supports the Set, Get, GetNext, and Trap messages as defined in RFC 1157. These messages are used as follows:

- Set, which means set the value of a specific object from one of the supported MIBs
- Get, which means retrieve the value of a specific object from one of the supported MIBs
- GetNext, which means retrieve the value of the next object in the MIB
- Trap, which means send traps to the manager when a particular type of significant event occurs

Supported Traps

The agent can send traps when any of the following occur:

- Cold starts (device server initializes)
- Authentication failures
- Login attempts
- Current threshold for power management
- Temperature threshold for power management
- Link up

Configuration Procedure: Web Interface

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as **root**.

Note: The default password is **dbps**, which should be changed. See the `newpass` command in the *Digi One/PortServer TS Command Reference* for information on changing passwords.

3. Select Configure and then SNMP from the menu.
4. Fill in the configuration fields and then click Submit.

For additional information, see the *Digi One/PortServer TS Command Reference* `set snmp`.

About Configuring Users

Although it is not required, the device server is often configured to accommodate the requirements of particular users. Typical configurable user attributes include the following:

- Whether the user is required to supply a password
- Autoconnection attributes, such as the system to which the user should be automatically connected at login
- The interface the device presents the user, such as a menu or command line
- Whether the user has access to outbound ports

For information on configuring PPP users, see "Configuring PPP" on page 29.

Configuration Methods

You can configure users in the following ways:

- With the web interface.
- With the set user command. See the set user command in the *Digi One/PortServer TS Command Reference*.
- With a RADIUS server. See the set radius command in the .

Common User Features

This section discusses common user-related features. For a complete list, see the set user command in the *Digi One/PortServer TS Command Reference*.

Feature	Description	set user Field
accesstime	Determines the times and days the user can access the device server. This feature is not configurable from the web interface.	accesstime
auto connect	Automatically connects the user to the host specified on the autohost field using the service (TCP port) defined on the autoport or autoservice fields. Autoconnection can also be implemented by port instead of by user. This feature is configurable from the web interface.	autoconnect autohost autoport autoservice

Default access type	Defines the type of access the user is restricted to. Menu, command line, autoconnect, and outgoing and net service are the types. This feature is configurable from the web interface.	defaultaccess
Menu access	Defines the menu that is to be presented to a user with menu access. This feature is configurable from the web interface.	menu
Port access	Defines the number of outbound ports a user connected over the LAN can access at one time. This feature is not configurable from the web interface.	maxsessions
PPP	Defines PPP-related parameters for the user.	There are too many fields to list here. See the set user command for more information.
Routing updates	Defines whether RIP routing updates are forwarded over the link to this user.	netrouting

Configuring a User: Web Interface

Use this section to configure users with from the web interface.

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as **root**. The default password is **dbps**.
3. Select Configure and then Users from the menu.
4. Choose Add User.
5. Enter a name and then choose Submit
6. Choose the new user from the Name column.
7. Configure the user as required.
8. Click Submit.
9. To return to the main User menu, click User from the Menu again.

Commands for Configuring a User

Use the commands listed below as well as find specific examples and complete parameters from the *Digi One/PortServer TS Command Reference*.

- set user (name=)
- newpass to assign a password
- default access=menu to configure a user for a menu
- autoconnect to automatically connect a user
- remove to remove a user from the user table

About Console Management

The device server can be configured to remotely manage network devices, such as routers, switches, power units, and servers, which usually provide EIA-232 serial ports for management. Using the device server and TCP/IP utilities like reverse Telnet and SSH2, network administrators can access consoled serial ports from a single station over the LAN. Power management also enables the network administrator to control and monitor power units and the devices attached to them from a single location. The SSH2 feature secures access to ports and devices as defined by the network administrator.

To set up Console Management for the PortServer 8/16, you will do the following:

- configure the serial ports
- configure SSH2 to control access to ports and devices
- configure power units and accessibility
- configure port buffering
- configure user menus

Configuring Ports

The device server serial ports must be configured properly before they will support console management. To configure the serial ports for console management, do the following:

1. From a web browser, login to the Portserver TS as root (default password is dbps). Make the following changes from the Configure > Ports page.
2. For each port connected to a device that will be managed, change the device type setting for the port to Printer (prn).
Default device type setting for all ports: terminal (term)
3. Ensure that the port and the device to be managed are using the same flow control scheme and other port parameters.
Default settings are: software flow control, 9600 bps, 8 bits, None for parity, 1 stop bit.

Configuring SSH

The device server supports SSH version 2. Users can connect using a variety of SSH clients that are available. There are three authentication options you can choose from to validate users. These options are local authentication, SSH authentication, and RADIUS authentication. There is no special configuration for local authentication. For how to configure your

device for RADIUS authentication, see the chapter on Configuring RADIUS. See the following section on how to configure SSH for authentication.

If you want to use SSH2 connections and use an SSH public key for authentication, do the following:

Device	Firmware Version
PortServer TS 8	82000684c or higher
PortServer TS 16	

- enter the following command

```
set user name=name loadkey=host:key
```

where

- *name* is the name of a user
- *host* is either an IP address or DNS name of a host running TFTP
- *key* is the name of a file that contains the DSA public key. If your host's implementation requires a complete path to the file, specify the path here as well.

Example:

```
set user name=secure loadkey=143.191.2.34:ssh-file
```

Note: Use the table to determine whether your Digi product supports SSH2 connections using a public key for authentication.

Example: SSH2 and Menu Access

In this example, a Digi device is configured to use an SSH2 public key, and it presents a menu to the administrator, from which he or she will select a device to manage.

Key aspects of this configuration include the following:

- Two ports to which the managed devices are connected specify `dev=prn`, a device type that does not spawn a login from the Digi device.
- A menu specifies connect commands, which when selected provide connections to ports 1 and 2 and the managed systems. The menu also specifies a menu table index number of 6 (on the range parameter), which is then linked to a user with the `set user` command

```
set ports dev=prn range=1-2
set line baud=19200 range=1-2
set menu name=menu1 t1="Console Management Menu" range=6
set menu name=menu1 range=6 m1="Connect to System 1" c1="connect
  1"
set menu name=menu1 range=6 m2="Connect to System 2" c2="connect
  2"
set user name=admin1 defaultaccess=menu menu=6 password=on
  outgoing=on
set user name=admin1 loadkey=142.191.2.34:ssh-file1
newpass name=admin1
```

Accessing Attached Devices

Telnet

Telnet is a direct connection to another device on the network. Once a user is connected to the device with a telnet session, they can connect to a specific port. Use the following procedure to initiate a telnet session:

```
telnet ipaddress
```

An example is:

```
telnet 192.168.5.24
```

At the command prompt, the user can connect directly to a port by entering the following command:

```
connect portnumber
```

An example is:

```
connect 4
```

This command initiates a telnet session on port 4. Other methods for accessing ports using a telnet session are through Custom Menus and Autoconnect.

Telnet Direct to a Port (Reverse Telnet)

Where Telnet is a direct connection to a device, reverse telnet is a direct connection to a device's serial port from the network. In the example below,

a user connects directly to serial port 4 on a PortServer. Reverse telnet uses a socket numbering scheme starting with 2000 plus the port number.

```
telnet 192.1.2.3 2004
```

A reverse telnet session can be authenticated on a Digi device with a RADIUS server.

Note: Ports must be configured for console management before they can be used for reverse telnet or reverse ssh. See "Configuring a Port for Autoconnection: Web Interface" on page 35.

SSH Direct to a Port (Reverse SSH)

Reverse ssh is the same as a reverse telnet session except the communication session is encrypted. Reverse ssh uses the socket numbering scheme of 2500 + the port number. In the example below, the user establishes a connection to port 12 on a Digi device.

```
ssh 192.1.2.3 2512
```

Users on a Linux system should use the following example for reverse ssh.

```
ssh -lroot -p2512 192.1.2.3
```

Alternate IP Addresses

If you want to simplify access to the ports, do the following to access a port from a workstation on the LAN. You can assign IP addresses to each port that will be connected to a managed device, which allows the administrator to Telnet directly to the port without specifying a TCP port number. See the set altip command in the *Digi One/PortServer TS Command Reference* for more information.

Configuration

In this example, the device server is configured with

- Alternate IP addresses using set altip commands, which assign IP addresses to ports 1 and 2. This enables direct access to one of these ports with a Telnet command that specifies one of the IP addresses.
- Password protection on ports 1 and 2. This is done with the set auth command that leaves all hosts to login by specifying the ip address as 0.0.0.0.

```
set ports dev=prn range=1-2
set line baud=19200 range=1 unrestricted=name ip=0.0.0.0
  mask=0.0.0.0
set auth login=1-2 range=2
set altip group=1 ip=119.180.33.50
set altip group=2 ip=119.180.33.51
```

User Command

In this example, a user Telnets to port 1 using an IP address. The user will be required to log in before access to the port is granted.

```
telnet 119.180.33.50
```

Securing Console Access

The device server provides the user with the ability to obtain secure and reliable access to console ports. Access to ports can be restricted in three ways:

1. User

Users can be setup with menu access, whereby the user is limited to the options presented in the menu. A port can also be assigned a spe-

cific User ID (UID). Access to the port is then restricted to that particular user.

2. Protocol

Protocols supported by the device server can be turned off to restrict the ways users can access ports. For example services such as telnet and http can be turned off with SSHv2 being the only method available to access.

3. Source IP

Ports can also be restricted by the source IP of the computer wanting access.

For details on configuring these options, refer to Chapter 11, or the see description of the following commands in the *Digi One/PortServer TS Command Reference*.

- set ports uid=
- set secureaccess
- set auth

Power Management

The web interface provides a quick, easy method for adding and configuring remote power control units to the PortServer TS 8/16. The PortServer TS 8/16 gives an administrator access to remote power units on the network enabling the administrator to reset a device(s) or turn them on or off. Once a power unit has been added, it can be configured and managed in three different ways. Users, console groups, and device names are the three different ways to manage the power units. Individual users are authorized to manage one or more outlets. Users assigned to a console group manage one or more ports and the power units attached to those ports. Users assigned by device name manage all devices having a specific name such as router or Cisco. The three management options a user has are to turn a device on, off, or reset a device or devices.

Configuring Power Units

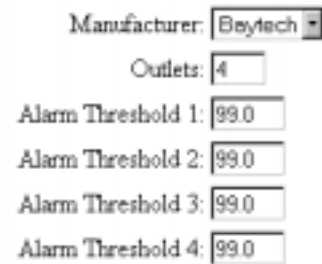
To add and configure a power unit on a Digi PortServer TS 8/16, do the following:

1. Enter the device server's IP address in a browser's URL address bar. Use the username `root` and the default password `dbps` to login.
2. From the menu, choose Configure > Power > select the Add Power Unit button.
3. Fill in the requested fields for port number, power unit manufacturer, number of outlets, and choose Submit. The power unit has been added and you are returned to the Power Unit Configuration page.
Note: The port number entered is the port on the PortServer TS which is connected to the power unit.

4. To configure the power unit, choose Edit Power Unit hyperlink under the power unit you have added.
5. Choose the manufacturer, enter the number of outlets, and set the alarm thresholds. Choose Submit.
The power unit is configured.

Note: The alarm threshold monitors the electric current on an outlet. It warns the user by sounding an audible warning when a specific amperage level is reached on an outlet.

Devices Supported: The Digi PortServer TS 8/16 supports the following Baytech power units: RPC 4, 6, 10, 12, 16, 18, 22, 27, and 28. See the Baytech website for further details at: <http://www.baytech.net>.



Manufacturer:

Outlets:

Alarm Threshold 1:

Alarm Threshold 2:

Alarm Threshold 3:

Alarm Threshold 4:

Configuring Users

Individual users must already be entered in the system before they can be assigned to the power units. You can add users by going to Configure > Users and filling in the required fields. To assign a user to a power unit, do the following:

1. From the menu, choose Configure > Power > and the Outlet you are configuring. The Outlet is listed in the Plugged Into column.
2. In the Power Management Users section, select Assign User.
3. From the drop down menu, choose the user you want to assign to manage the power unit.

4. Choose Submit to save your configuration.

Configuring Console Groups

To assign groups to the power units, do the following:

1. From the menu, choose Configure > Power > and the Outlet you are configuring. The Outlet is listed in the Plugged Into column.
2. A configuration screen appears. In the Console Group field select a group from the pull down menu to assign the group to the Outlet. The Device Name and Plugged Into fields are already filled by the configuration utility.
3. In the Power Management Users section, check the boxes to assign control either by the device name, the console group, or both. If none are selected, users assigned to this device may only manage this device, rather than a group of devices.
The Power Management options become accessible only when a Console Group or Device Name have been assigned.

Choose Submit to save your configuration.

For additional console settings, see set powerunit in the Digi One/PortServer TS Command Reference.

Configuring Device Names

1. From the menu, choose Configure > Power > and the Outlet you are configuring. The Outlet is selected from the Plugged Into column.
2. Enter the name you want to assign to control the Outlet in the Device Name field.
If information is already present in the field, highlight the field and enter the new information.
3. In the Power Management Users section, check the boxes to assign control either by the device name, the console group, or both.
If none are selected, users assigned to this device may only manage this device, rather than a group of devices.

The Power Management options become accessible only when a Console Group or Device Name have been assigned.

4. Choose Submit to save the configuration.

Select the outlet that the device's power is plugged into and the Console Group that the device's console port is connected to. Select which users have authority to manage this device.

Device Name:

Plugged Into:

Console Group:

Power Management Users

The following users have power management authority on this device.

[Assign User](#)

Apply these authorities to all devices using device name 'outlet1_1'

No console group has been assigned to apply all authorities to all devices using that console group.

Configuring Port Buffering

Note: Port buffering is supported on PortServer TS 2/4 MEI and PortServer TS 8/16 devices only.

Serial ports store data or information in what are called buffers. Buffers are helpful to administrators who use them to monitor events on a system. If a system unexpectedly goes down, the administrator can look in a logfile (buffer) to find out what caused the system to go down. The buffers serve to diagnose network and device problems.

To configure a port for port buffering, do the following:

1. From the web interface, choose Configure > Port Buffering.
2. Select the port you want to configure.

Choose On to turn on buffering, select the size of the buffer, and choose Submit.

Note: Buffers can only be viewed by administrators from the web interface page.

Configuring User Menus

The web interface configuration utility provides an easy method for configuring user menus. The menus can be designed to give users access to specific devices or ports. To configure a menu from the web browser, login to the Digi device server as root (default password is dbps) and choose Configure > Menus.

Upgrading the Firmware

This section describes how to upgrade the firmware, which can be done from the web interface using HTTP or FTP.

HTTP or TFTP Upgrade Procedure

If your hardware is okay, make sure you are running the latest firmware version available. Check the Digi Support site (<http://ftp.digi.com/support/firmware>) for the latest firmware and/or POST updates for your device

1. Download a copy of the firmware file.
2. Access the Digi device server's web interface by entering the Digi device server's IP address in a browser's URL window and log on (User Name `root`, Password `dbps`).
3. Choose Update Firmware from main menu.
4. Browse to the location on your system where the firmware has been saved, select the correct file, and click Update.
5. Reboot the device when prompted.
6. Access the Digi device server's web interface and verify on the Information Page that the Firmware version has been successfully updated.

Do not leave your browser until you are prompted to reboot.

Command Line

If you want to use the command line to upgrade firmware, use the `boot` command. See the *Digi One/PortServer TS Command Reference* for more information.

Copying the Configuration to and from a Remote Host

This section discusses copying the configuration to a remote host and from a remote host, which means you can configure the Digi device remotely by entering commands in a text file and then copying the file to the Digi device.

When To Use Remote Configuration

Typically, you use remote configuration when you have several device servers with similar configurations and want to keep a master configuration on a remote host, from which you can easily create variations for downloading to individual device servers.

Rules for Editing a Configuration file

Here are some rules for editing a configuration file on a remote host:

- Edit the file with any text editor.

- Each line of the file must start with a set command, such as set user or set line. In other words, do not let commands wrap to the next line if your editor supports this function.

HTTP Procedure

1. Access the web interface by entering the device server IP address in a browser's URL window.
2. Log on to the device server as `root`. The default password is `dbps`.
3. From the main menu, choose Admin > HTTP CpConf.
4. To copy a file from the host you are on do the following:
 - Choose Browse, select the file, and then choose Submit.
 - Follow the prompts to complete this procedure.
5. To copy a file to a remote host, do the following:
 - Right click on the Download current config link.
 - Choose Save Target as
 - Specify a file name and then choose Save.
6. Follow the prompts to complete this task.

TFTP Procedure

1. Ensure that TFTP is running on the remote host.
2. Access the web interface by entering the device server IP address in a browser's URL window.
3. Log on to the device server as `root`. The default password is `dbps`.
4. From the main menu, choose Admin > TFTP CpConf.
5. Choose either Copy configuration to a TFTP server or Copy configuration from a TFTP server.
6. Specify an IP address and a file name and then choose Submit.
7. Follow the prompts to complete this task.

Command Line

If you want to use the command line to copy the configuration to and from a remote host, use the `cpconf` command. See the *Digi One/PortServer TS Command Reference* for more information.

Resetting Device Server Configuration to Defaults

Use this topic to reset the device server configuration to defaults.

Note: This procedure causes the device server to lose all configuration changes. If you have a complex configuration, contact Digi before performing for information on saving your configuration.

Procedure

1. Use a pen, the point of a paper clip, or some other device to press the recessed button on the front panel.
2. While holding down the button, power on the device server.

3. When the 1-5-1 LED pattern is displayed, release the button.
The device boots up.

Commands for Resetting the Configuration to Defaults

Use the revert command to reset the configuration to factory defaults or the latest version stored in NVRAM. See the *Digi One/PortServer TS Command Reference* for complete information.

Note: You can also use the range field on this command to define a range of ports with the serial, port, line, flow, keys and login options.

Symptom: PortServer TS 8/16 Does Not Boot**Introduction**

Use the information provided in this discussion when PortServer TS 8/16 will not complete the boot cycle.

Procedures

Things to Try	See ...
Check for hardware problems.	<ul style="list-style-type: none"> "Running PortServer TS 8/16 Hardware Diagnostics" on page 76 "Running PortServer TS 8/16 POST" on page 77
Check for TFTP problems if PortServer TS 8/16 is booting from a TFTP host.	<ul style="list-style-type: none"> "Verifying TFTP on a UNIX System" on page 78 "Troubleshooting TFTP Problems" on page 78
Resetting the device to configuration defaults.	"Resetting PortServer TS 8/16 Configuration to Defaults" on page 79
If you cannot resolve the problem, contact Digi.	"Digi Contact Information" on page 84

Symptom: Cannot Telnet to the PortServer TS 8/16**Introduction**

Use the information provided in this discussion to troubleshoot network problems.

Assumptions

This discussion assumes that the PortServer TS 8/16 itself is working, that is, that it completes the boot cycle.

Procedures

Things to Try	See ...
Verify the IP address. This procedure ensures that you are using the right IP address to Telnet to the PortServer TS 8/16.	"Verifying the PortServer TS 8/16 IP Address" on page 79
Check for duplicate IP address. This procedure ensures that two devices are not using the same IP address.	"Checking for Duplicate IP Addresses" on page 80

Things to Try	See ...
See if you can ping the IP address. If you can ping the address, but cannot Telnet to it, you probably have a firewall problem. See the Firewall documentation for more information.	"Pinging an IP Address" on page 80
Verify the network cabling.	"Verifying the Network Cabling" on page 80
If you cannot resolve the problem, contact Digi.	"Digi Contact Information" on page 84

Symptom: Trouble Accessing a Port

Introduction

Use this procedure if you are having trouble accessing a PortServer TS 8/16 port. The specific problem might be that you cannot logon from a terminal or the printer or modem is not working properly. The Digi Port Authority-Remote utility is helpful in the troubleshooting process for determining the port signal status. See *Configuring the Ethernet Interface with Digi Port Authority-Remote*.

Assumptions

This discussion assumes the following:

- That the PortServer TS 8/16 itself is working, that is, that it completes the boot cycle. If it is not, see "Symptom: PortServer TS 8/16 Does Not Boot" on page 75.
- That the network is working. This is only pertinent if all ports are not working and the malfunctioning ports are RealPort ports. The discussion in "Symptom: Cannot Telnet to the PortServer TS 8/16" on page 75 goes through the steps of validating the network connection.

Procedures

Things to Try	See
If this is a RealPort port and all ports are not working, ensure that the RealPort process is running.	"Verifying the RealPort Process: AIX" on page 81
Verify PortServer TS 8/16 port settings.	"Checking and Changing Port Configuration" on page 82
Verify the cabling to the peripheral	See the Digi One/PortServer Cable Guide for information.

Running PortServer TS 8/16 Hardware Diagnostics

Use this topic to run hardware diagnostic procedures to validate the

PortServer TS 8/16.

1. Connect a terminal to a PortServer TS 8/16 port.
2. If the port is still using the default configuration, configure the terminal to use the following settings (Otherwise, configure the terminal to match the port configuration):
 - VT-100 emulation
 - 9600 baud
 - 8-bit characters
 - 1 stop bit
 - No parity
3. Reboot the PortServer TS 8/16.
4. When the front panel LEDs are all lighted, hold the Reset button and press the v key. You may release the button when the serial port begins to output test results.
5. When the Hardware Diagnostics Menu appears, select a test to perform.

Running PortServer TS 8/16 POST

Use these topics to run PortServer TS 8/16 power on self test to validate the PortServer TS 8/16 hardware.

Procedure: Running the POST Using the LEDs

1. Power on the PortServer TS 8/16.
2. Use the following table to interpret the output from the LEDs.

If ...	Then ..
The power LED blinks immediately after POST	A DHCP error has occurred and the PortServer TS 8/16 was not assigned an IP address.
Any of the other four LEDs blink immediately after POST	A hardware component failed.

Procedure: Running the POST from a Terminal

1. Connect a terminal to the first serial port on the PortServer 8/16.
2. If the port configuration was changed, configure the terminal to match the port settings. If the port is still using the default configuration, configure the terminal to use the following settings:
 - VT-100 emulation
 - 9600 baud
 - 8-bit characters
 - 1 stop bit
 - No parity

3. Reboot the PortServer TS 8/16 and press v when the LEDs begin to blink.

POST output appears on the terminal screen.

Verifying TFTP on a UNIX System

Use this procedure to verify that TFTP is working correctly on your UNIX host.

Note: This procedure, which uses a TFTP transfer of the Digi Device's boot image between two UNIX hosts, enables you to compare the size of the boot image before and after it is transferred, enabling you to determine if TFTP is working properly.

1. Access a root prompt on the UNIX host.
2. Make sure that you are not in the /tftpboot directory.
3. Enter this command:

```
tftp ipaddress
```

where *ipaddress* is the IP address of the UNIX host.

A TFTP prompt appears.

4. At the prompt, enter the following command:

```
binary
```

5. Enter this command at the TFTP prompt:

```
tftp > get tftp_file_name
```

where *tftp_file_name* is the name of the Digi Device's boot image in the /tftpboot directory.

6. Enter this command at the TFTP prompt to exit TFTP:

```
tftp quit
```

7. Compare the size of the original file against the transferred file using this command:

```
ls -l tftp_file_name /tftpboot/tftp_file_name
```

If the file sizes match, TFTP is working properly.

Troubleshooting TFTP Problems

Here are some things to check if you encounter TFTP problems.

- Verify that the /tftpboot directory exists and has read, write and execute (777) permissions with this command: `ls -l /tftpboot`
- If necessary, use this command to create the directory:

```
mkdir /tftpboot
```

- If necessary, use this command to change permissions of the directory to read, write and execute:

```
chmod 777 /tftpboot
```

- Verify that the file /tftpboot/ftp_file_name exists and has read and execute permissions with this command:

```
ls -l /tftpboot/ftp_file_name
```

where *ftp_file_name* is the name of the firmware boot image

- If necessary, use this command to change permissions of the file to read and execute:

```
chmod 666 /tftpboot/ftp_file_name
```

- Verify that the `inetd.conf` file is properly configured for `tftp` by displaying the file `/etc/inetd.conf`. An entry similar to this should be uncommented:

```
tftp dgram udp something
```

where *something* will vary with each operating system.

- For controlled TFTP access, make sure that the file `/etc/tftpdaccess.ctl` exists and verify that it only allows access to public directories. If this file is not present, `tftp` will allow full access. A sample file is located in the directory `/usr/lpp/tcpip/samples`.
- Restart the `inetd` process with these two commands:

```
ps -ef | grep inetd
```

This will report back the `inetd` process number.

```
Kill -1 inetd_PID
```

Where *inetd_PID* is the process number for the `inetd` process reported by the previous command.

Resetting PortServer TS 8/16 Configuration to Defaults

Use this topic to reset the PortServer TS 8/16 configuration to defaults.

Note: This procedure causes the PortServer TS 8/16 to lose all configuration changes. If you have a complex configuration, see the `cpconf` command in the *Digi One/PortServer TS Command Reference* for information on backing up your configuration. The PortServer also resets to the DHCP default setting and loses its IP address during the reset process. Use DPA-Remote to find and configure your device. DPA-Remote can be found under Software on the Software and Documentation CD or from www.support.digi.com under Support Tools. You will need to re-assign an IP address after the reset and reboot procedure.

Command Line Procedure

1. Log on to the PortServer TS 8/16 as root.
2. Issue the following command:

```
boot action=factory
```

Front Panel Procedure

1. Power on the PortServer TS 8/16
2. While the PortServer TS 8/16 is still booting, press and hold (for about 10 seconds) the white button on the front panel.

Verifying the PortServer TS 8/16 IP Address

Use this procedure to check the IP address on the PortServer TS 8/16.

1. Connect a terminal to a PortServer TS 8/16 port.
2. If the port is still using the default configuration, configure the terminal to use the following settings (Otherwise, configure the terminal to match the port configuration):
 - VT-100 emulation
 - 9600 baud

- 8-bit characters
 - 1 stop bit
 - No parity
3. Press Enter to get a logon prompt from the PortServer TS 8/16.
 4. Log on to the PortServer TS 8/16.
 5. Use the set config command to verify the PortServer TS 8/16 IP address.

Checking for Duplicate IP Addresses

Use this procedure to ensure that the PortServer TS 8/16 and another device are not using the same IP address.

1. From another system on the network, use the ping command to determine if the IP address is in use. The following is the command syntax:

```
ping ip-address
```

2. Do one of the following:
 - If there is no response to the ping, exit this procedure and return to the symptoms section of this section. Two devices using the same IP address is probably not a problem.
 - If there is a response, continue with this procedure.
3. Turn the PortServer TS 8/16 off and then ping again.
4. Do one of the following:
 - If there is a response to the ping, there is another device using that IP address, so assign one of the devices a new IP address.
 - If there is no response, turn the PortServer TS 8/16. Another device is not using the IP address assigned PortServer TS 8/16.

Pinging an IP Address

Use this procedure to determine if a system can be reached from across a network.

Attempt to ping the PortServer TS 8/16 from another system on the network. Here is the format of the command:

```
ping ip-address
```

Verifying the Network Cabling

Use this procedure to troubleshoot network cabling problems.

1. Check the Ethernet cable. Verify the following:
 - The Ethernet cable is connected securely at both ends.
 - The Ethernet cable is pinned correctly.
 - The quality of the cable is sufficient for the cable length and the cable environment. Common Category 5 Unshielded Twisted Pair cabling can generally be run 300 meters at a speed of 10 Mbps and

150 meters at higher speeds. Consult an Ethernet cable manufacturer for a recommended cable for your configuration.

2. Verify your Ethernet hub. See your Ethernet hub manual.

Verifying the RealPort Process: AIX

1. Type the following:

```
lsdev -Cc nts
```

2. If the sa devices are not in an available state, type the following from the AIX prompt:

```
mkdev -l sa#  
cfgmgr
```

where # is the number of the Digi Device.

Verifying the RealPort Process: HP-UX

1. Verify that RealPort is running on the HP-UX operating system by entering:

```
ps ef| grep drp
```

If you see an entry for each Digi Device similar to the following, the RealPort process is running.

```
root 2254 1 0 Dec 13 ? 0:03/sbin/drpd 1 199.86.0.1 root 2049 1 0  
Dec 13 ? 0:01/sbin/drpd 1 199.86.5.1
```

2. If the daemon is not running, enter this command at a root prompt:

```
/usr/sbin/drpadmin
```

3. Answer the prompts as appropriate.

Verifying the RealPort Process: Linux

The RealPort daemon (process) controls communication between the RealPort driver module and your Digi Devices across the network. One daemon must remain in the background for each Digi Device, maintaining the communication link. You should not need to start the daemon by hand. The `dgrp_cfg_node` program does this automatically.

However, to determine whether any RealPort daemons are currently running on your system, as well as to determine which Digi Device each daemon is communicating with, you can execute the following command:

```
ps ax | grep drpd
```

For more information about the RealPort daemon, see the `drpd` man page that is installed with the driver package.

Verifying the RealPort Daemon: SCO

Use this topic to verify that the RealPort daemon is running on a SCO Unix or SCO OpenServer operating system.

1. At the root prompt, enter the following command:

```
ps ef| grep ncxd
```

If the RealPort Daemon is running, you should see an entry for each Digi Device similar to the following.

```
root 2254 1 0 Dec 13 ? 0:03/etc/necd -d /dev/cts0 -n
root 2049 1 0 Dec 13 ? 0:01/etc/necd -d /dev/cts0 -n
```

2. If you do not see this information, restart the daemon by doing the following:
 - a. Modify the `/etc/rc2.d/S86ncxa` file with the appropriate IP addresses.
 - b. Reboot the server.

Verifying the RealPort Process: Solaris

Use this topic for information on verifying that the RealPort process is running on a Solaris system.

1. Type the following command:

```
ps -ef|grep ncx
```
2. If the information that appears is not correct, do the following:
 - a. Modify the `/etc/rc2.d/S26realport` file with the appropriate IP addresses.
 - b. Reboot the UNIX server.

Verifying the RealPort Service: Windows NT

Use this procedure to verify the RealPort service on Microsoft Windows NT.

1. From the Start menu, choose Settings > Control Panel > Devices > Digi RealPort.
2. If the RealPort service has not been started, choose Start.

Verifying the RealPort Service: Windows 2000

Use this procedure to verify the RealPort service (process) on Microsoft Windows 2000.

1. Right-click on My Computer, choose Properties > Hardware tab > Device Manager.
2. Expand the Multi-port Serial Adapters list if necessary and select Digi PortServer.
3. If the RealPort Service (process) is not enabled, right-click and choose Enable.

Checking and Changing Port Configuration

Use this topic to ensure that PortServer TS 8/16 serial port configuration is correct. You can display and change port configuration from either the command line or the web interface. This topic addresses the command line only. For information regarding the web interface, access the port from the web interface and then use the online help.

RealPort

- Specify
`set ports dev=rp` to define a device type.
- Configure serial line attributes on the RealPort host.
- Configure flow control on the RealPort host.

Printer

- For most printers, specify
`set ports dev=prn`
- Use the set line command to configure serial line attributes that are consistent with peripheral requirements.
- Use the set flow command to configure flow control attributes that are consistent with peripheral requirements.

Incoming Modem

- For most incoming modem connections, specify
`set ports dev=min`
- Use the set line command to configure serial line attributes that are consistent with peripheral requirements.
- Use the set flow command to configure flow control attributes that are consistent with peripheral requirements.

Outgoing Modem

- For most outgoing modem connections, specify
`set ports dev=mout`
- Use the set line command to configure serial line attributes that are consistent with peripheral requirements.
- Use the set flow command to configure flow control attributes that are consistent with peripheral requirements.

Two-way Modem

- For both incoming and outgoing modem connections, specify
`set ports dev=mio`
- Use the set line command to configure serial line attributes that are consistent with peripheral requirements.
- Use the set flow command to configure flow control attributes that are consistent with peripheral requirements.

Terminal

- For most terminal connections, specify
`set ports dev=term`
Also, if you have configured the port for autoconnection, ensure that the destination IP address and TCP port (dport) are correct.
- Use the set line command to configure serial line attributes that are consistent with peripheral requirements.

- Use the set flow command to configure flow control attributes that are consistent with peripheral requirements.

Digi Contact Information

Digi International
11001 Bren Road East
Minnetonka, MN 55343
U.S.A

Customer Service and Support	
World Wide Web:	http://support.digi.com
email	support@digi.com
Telephone (U.S.)	1-800-344-4273
Telephone (other locations)	(+011) 952-912-3444

Specifications

LEDs

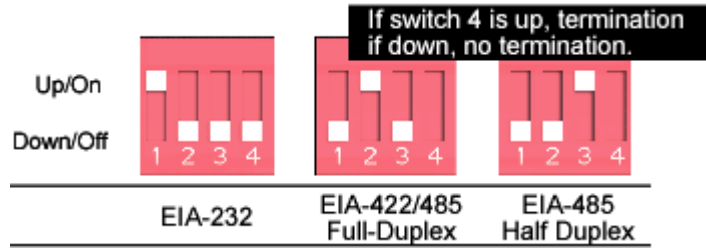
LED	Color	State	Indicates
Power	Green (labeled PWR)	On	Power detected
		Steady blinking	Waiting for an IP address.
		Blinking 1-1-1	Starting the EOS
		Blinking 1-3-1	Starting the TFTP process
		Blinking 1-5-1	Configuration returned to factory defaults
		Off	No power detected
Radio Signal Strength	Yellow	Varying brightness	Signal strength relates to brightness or dimness of the light
Status (Link)	Green	On	Physical network detected
		Off	No physical network detected
ACT	Yellow	On	Bad initialization
		Off	Ready
		Blinking	Network activity

LED Diagnostics

LED Activity	Indication
1-1-1 pattern	Starting the EOS.
1-3-1 pattern	TFTP boot process started
1-5-1 pattern	Tells you that configuration has been return to the factory configuration. See "Managing the OS and Configuration" on page 71.
Steady blinking	Device seeking an IP address from DHCP server. If a static IP address has been set, go to Configure Network, click Submit, and reboot the device.
Solid	On Digi One RealPort and PortServer TS 2/4 devices, this means the boot completed sucessfully.

Device Server EIA 232/422/485 Switch Settings

Function	Switch Settings			
	1	2	3	4
EIA-232	Up	Down	Down	Down
EIA-422/485 Full-duplex	Down	Up	Down	If up, termination. If down, no termination
EIA-485 half-duplex	Down	Down	Up	





DB9 Pinouts

DB9 Pin	EIA-232	EIA-422/485 Full-Duplex	EIA-485 Half-Duplex
1	DCD	CTS-	Not used
2	RxD	RxD+	RxD+
3	TxD	TxD+	TxD+
4	DTR	RTS-	Not used
5	GND	GND	GND
6	DSR	RxD-	RxD-
7	RTS	RTS+	Not used
8	CTS	CTS+	Not used
9	NA	TxD-	TxD-


WARNING: To prevent electric shock, do not remove the cover of this module while unit is powered up. There are no user-serviceable parts inside. Refer servicing to qualified personnel.

CAUTION: This unit has two power inputs. For total isolation from electrical shock and energy hazard, disconnect both power inputs. The device is intended to be mounted in an indoor only type system.

Standard Models Specifications

Power Requirements (Standard Models)	
2-contact barrel connector 	+9 to +30 VDC 525 mA (max) external power supply
RJ-45 Powered Ethernet 	+30 to +60 VDC 100 mA (max)
Environmental	
Ambient temperature	0 to 50° Celsius 32 to 131° Fahrenheit
Relative humidity	5% to 90% non-condensing
Altitude	0 to 12,000 feet 0 to 3,658 meters
Mechanical	
Length	13.33 centimeters 5.25 inches
Width	8.25 centimeters 3.25 inches
Height	1.90 centimeters .75 inches
Weight	.227 Kilos 8 ounces

Specifications for Extended Temperature Models

Power Requirements (Extended Temperature Models)	
2-contact barrel connector 	+9 to +30 VDC 525 mA (max) external power supply
Environmental	
Ambient temperature	-35 to 70 °Celsius -31 to 158 °Fahrenheit
Relative humidity	5% to 90% non-condensing
Altitude	0 to 12,000 feet 0 to 3,658 meters
Mechanical	
Length	13.33 centimeters 5.25 inches
Width	8.25 centimeters 3.25 inches
Height	1.90 centimeters .75 inches
Weight	.227 Kilos 8 ounces

FCC Part 15 Class A

Radio Frequency Interference (RFI) (FCC 15.105)

This equipment has been tested and found to comply with the limits for Class A digital devices pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Labeling Requirements (FCC 15.19)

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications (FCC 15.21)

Changes or modifications to this equipment not expressly approved by Digi may void the user's authority to operate this equipment.

Cables (FCC 15.27)

Shielded cables *must* be used to remain within the Class A limitations.

ICES 003 Class A

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Digi Contact Information

Digi International
 11001 Bren Road East
 Minnetonka, MN 55343
 U.S.A.

Digi Contacts	
World Wide Web:	http://digi.com
email	digi.info@digi.com
Telephone (U.S.)	1-952-912-3444
Telephone (other locations)	(+011) 952-912-3444

Index

C

- command line
 - configuring access to 48
- computer connections
 - configuring 28
- configuration
 - remote 71

D

- DB9 pinouts 86
- DNS
 - configuring a host file 56
 - introduction to 55
- Domain Name System
 - introduction to 55
- domain name system
 - configuring a host file 56

E

- Ethernet interface, configuring 13

I

- inbound ports
 - configuring access to 47
- IP address, configuring the Ethernet interface 13

L

- line interface, setting 86

M

- MEI switch settings 86

N

- newpass command 52

O

- operating system
 - updating 71
- OS
 - updating 71
- outbound ports
 - configuring access to 48

P

- passwords
 - issuing 52
- pinouts, DB9 86
- PPP
 - configuring 29
- printers
 - configuration considerations 19
- Proxy ARP

- configuring 43

R

- RealPort
 - features 15
- remote configuration 71
- routing
 - configuring dynamic routes 42
 - configuring static routes 41

S

- security
 - configuring access to inbound ports 47
 - configuring access to outbound ports 48
 - configuring access to the command line 48
 - using RADIUS 49
- setting the line interface 86
- SNMP
 - introduction to 57