



## Device and Terminal Servers

[www.digi.com](http://www.digi.com)

*Making*  
**DEVICE NETWORKING**  
*easy*

© Digi International Inc. 2003, 2004. All Rights Reserved.

The Digi logo, PortServer, Connectware, Digi One, and RealPort are trademarks or registered trademarks of Digi International, Inc.

[www.digi.com](http://www.digi.com)

*Making*  
**DEVICE NETWORKING**  
*easy*

## Chapter 1 Configuration Tasks

Quick Reference for Configuring Features .....	7
Access the Command Line.....	11
Configure RealPort .....	12
Configure an IP Address .....	12
Configure Serial Port Settings .....	13
Configure Wireless Devices .....	27
Configure Network Settings.....	28
Configure Security Features.....	36
Configure Power Over Serial Ports .....	45
Configure User Attributes .....	46
Configure Embedded Modem.....	48
Configuration Management .....	48

## Chapter 2 Command Descriptions

Basic Command Information .....	49
admin.....	51
boot.....	52
close .....	54
connect.....	55
cpconf.....	56
display .....	57
display buffers .....	59
exit.....	61
help.....	62
info.....	63
kill .....	65
mode.....	66
newpass .....	67
ping.....	68
power.....	70
quit.....	72
reconnect.....	73
remove.....	74
revert .....	75
rlogin.....	78

send.....	79
set altip .....	80
set arp.....	81
set auth.....	82
set buffers.....	85
set chat .....	87
set config .....	89
set device .....	94
set dhcp .....	96
set embmodem.....	98
set ethernet.....	99
set filter .....	101
set flow .....	105
set forwarding .....	109
set host.....	113
set ia.....	114
set ippool .....	127
set keys .....	128
set line .....	130
set logins .....	133
set menu.....	136
set modem.....	138
set netlogins .....	140
set ports.....	143
set powerunit .....	149
set radius.....	152
set route.....	154
set script .....	156
set secureaccess.....	162
set service .....	164
set snmp .....	166
set socketid.....	169
set tcpip .....	171
set telnetip .....	173
set terms.....	174
set time .....	176
set trace.....	177
set udpdest.....	181
set udpserial .....	183
set user.....	185
set wlan .....	197
show .....	203

status .....	205
telnet.....	206
traceroute .....	207
uptime.....	208
wan.....	209
who.....	211
<b>Index.....</b>	<b>213</b>



This chapter shows how to perform common device configuration tasks from the command line.

## Quick Reference for Configuring Features

The following table shows common features that can be configured, the device types in which the features are supported, the commands used to configure each feature, and where to find more information in this chapter.

In this table, the “Digi TS Family” includes the following devices:

- Digi One TS
- Digi One TS Wireless
- Digi One RealPort
- Digi One RealPort Wireless
- PortServer TS 2/4
- PortServer TS 2/4 MEI
- PortServer TS 2/4 MEI Wireless
- PortServer TS 8/16
- PortServer TS 1/3 + Modem

And “Digi TS Wireless family” includes the following devices:

- Digi One TS Wireless
- PortServer TS 2/4 MEI Wireless
- Digi One RealPort Wireless

## Quick Reference for Configuring Features

Feature/Task	Device types supported in	Commands	See page
<b>RealPort</b>	Digi TS Family	See User Guide's chapter on setting up RealPort for details on configuring this feature.	
<b>Wireless devices</b>	Digi One TS Wireless PortServer TS 2/4 MEI Wireless	set wlan	27
<b>Point-to-Point Protocol (PPP) connections</b>	Digi One TS PortServer TS 1 + Modem PortServer TS 3 + Modem PortServer TS 2/4 MEI PortServer TS 2/4 MEI Wireless PortServer TS 8/16	set ports set flow set user	13
<b>Modem emulation</b>	Digi One TS PortServer TS 1 + Modem PortServer TS 3 + Modem PortServer TS 2/4 MEI PortServer TS 2/4 MEI Wireless PortServer TS 8/16	set ports dev=pm field AT commands	22 See also the <i>AT Command Reference</i> .
<b>Autoconnection</b>	Digi TS Family	set ports set user	26
<b>IP routing</b>	Digi TS Family	set route set forwarding set user	28

Feature/Task	Device types supported in	Commands	See page
<b>Security / access control features</b>			
Control access to configuration	Digi TS Family	set user	36
Control access to inbound ports	Digi TS Family	set ports - dev field set logins set user	37
Control access to outbound ports	Digi TS Family	set ports - dev field	38
Restrict access to outbound ports	Digi TS Family	set auth	38
Use CHAP authentication for PPP users	Digi TS Family	set user	38
Control user access to the command line	Digi TS Family	<ul style="list-style-type: none"> <li>• Through autoconnect by port: set ports</li> <li>• Through autoconnect by user: set user</li> <li>• Through menus: set menu</li> </ul>	38
Use RADIUS to authenticate users	PortServer TS 8/16	set radius	39
Issue user passwords	Digi TS Family	<ul style="list-style-type: none"> <li>• To enable/disable password for a user: set user</li> <li>• To issue new password to user: newpass</li> </ul>	42
Configure SSH Version 2 for secure communication	Digi TS Wireless Family PortServer TS 8/16 PortServer TS 2/4 MEI	<ul style="list-style-type: none"> <li>• To configure password protection: set user - name and password fields, and newpass command</li> <li>• To use a public key: set user - name and loadkey fields</li> <li>• To make reverse SSH connections to ports: <i>ssh ip_address 2500 + port_number</i></li> </ul>	43
<b>Industrial Automation (IA)</b>	Digi TS Family	set ia	20
<b>Domain Name Server (DNS)</b>	Digi TS Family	set config set host	32
<b>Simple Network Management Protocol (SNMP)</b>	Digi TS Family	set snmp	34

## Quick Reference for Configuring Features

Feature/Task	Device types supported in	Commands	See page
<b>Power Over Ports</b>	PortServer TS 2/4 MEI Digi TS Wireless Family	<ul style="list-style-type: none"> <li>To display status of circuit breaker: display circuitbreaker or set config print</li> <li>To reset circuitbreaker: set config circuitbreaker=reset</li> </ul>	45
<b>Embedded Modem</b>	PortServer TS 1 + Modem PortServer TS 3 + Modem	set ports - dev field, where dev=min, mout, or mio	48
<b>User attributes</b>			
Set common user features	Digi TS Family	set user - name field	46
Assign a password	Digi TS Family	newpass	46
Configure a user for a menu	Digi One TS PortServer TS 2/4 MEI PortServer TS 2/4 MEI Wireless PortServer TS 8/16	set user defaultaccess=menu	46
Automatically connect a user	Digi TS Family	set user autoconnect=on	46
Remove a user from the user table	Digi TS Family	remove	46
Use a RADIUS server to set user attributes	PortServer TS 8/16	set radius	46
<b>Configuration management</b>			
Upgrade firmware	All devices	boot	48
Copy configuration to and from a remote host	All devices	cpconf	48
Reset configuration to defaults	All devices	revert	48

## Access the Command Line

To configure devices using commands, you must first access the command line, either from a locally connected terminal or a Telnet session, and then log on as `root` from the command line.

### From a Locally-Connected Terminal

To access the command line and the configuration from a terminal connected to one of the device server's serial ports, follow these steps.

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`.

### 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 "Configure an IP Address" on page 12.

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. For example

```
telnet 192.3.23.5
```
2. Log on as the `root` user. The default password is `dbps`.

### If You Cannot Access the Command Line

If you cannot access the command line, your user access permissions may be set to disable access to the command line. See Control User Access to the Command Line on page 38.

## Configure 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.

For further configuration details, see the User Guide's chapter on setting up RealPort.

## Configure an IP Address

To configure an IP address, mask, and default gateway for the device server's Ethernet interface, use the set config command.

### 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. Configure an IP address for the Ethernet interface by entering the following command:

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

where *ip-address* is the IP address for the Ethernet interface. For example:

```
set config ip=191.143.2.154
```

3. Configure a subnet mask by entering the following command:

```
set config submask=mask
```

where *mask* is the subnet mask for this subnetwork. For example:

```
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. For example:

```
set config gateway=191.143.2.46
```

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

```
boot action=reset
```

### 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 effect.

```
set config ip=192.150.150.10 submask=255.255.255.0 dhcp=off
```

```
set config gateway=192.150.150.11
```

```
boot action=reset
```

### See also

For more information, see these command descriptions:

- set config on page 89
- boot on page 52

## Configure Serial Port Settings

Configuring serial port settings involves setting the following options for a port:

- Point-to-Point (PPP) connections
- Industrial automation (IA)
- Modem emulation
- TCP socket communication
- UDP Multicast communication
- Autoconnection

## Configure PPP Connections

Configuring Point-to-Point Protocol (PPP) connections includes:

- Configuring inbound PPP connections
- Configuring outbound PPP connections
- Using filters on the PPP connections, as needed

## Configure Serial Port Settings

### Configure Inbound PPP Connections

To configure simple inbound PPP connections from the command line, follow these steps.

For information on fine-tuning PPP connections, see the `set user` command.

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

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.

For 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.

For example:

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

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.

For 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 to the PPP user. For 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 *set ippool* on page 127.

For 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. For example:

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

## Configure Serial Port Settings

### Example

This example shows a very simple PPP inbound configuration with the following properties:

- 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
```

### See also

For more information, see these command descriptions:

- [set ports on page 143](#)
- [set flow on page 105](#)
- [set line on page 130](#)
- [set user on page 185](#)

## Configure Outbound PPP Connections with Filters

To configure outbound-only PPP connections with filters, or the outbound portion of bidirectional connections with filters, follow these steps.

Note: For dialout outbound connections to a non-Digi device, select authentication type=none. CHAP authentication works between two Digi devices.

1. To set the filter for the outbound connection, enter:

```
set filter name="<filter name>" s1="dst/<IP Address>/<Subnetmask>
```

2. To set the flow control to hardware, enter:

```
set flow range=1 ixon=off ixoff=off rts=on cts=on
```

Note: PortServer TS 1/3+Modem flow control default is Hardware.

3. To configure the user for the outbound PPP connection:

```
set user name="<username>" protocol=ppp
```

4. To set up the user for the PPP environment (the local IP address, the devices, the telephone number, etc) enter the following commands:

```
set user name="<username>" ipaddr=negotiated
ipmask=255.255.255.255
```

```
set user name="<username>" defaultaccess=netservice autoport=513
password=on
```

```
set user name="<username>" outgoing=on autoservice=default
```

```
set user name="<username>" bringup="<filter name>"
```

```
set user name="<username>" device="gendialer"
```

5. To assign the dialscript to which the port the modem is connected, enter the following command:

```
set device name="gendialer" baud=no dialer=genmdm chat=no port=1
```

6. To set up routing for the PPP connection enter the following commands:

```
set forwarding state=active splithorizon=off poisonreverse=off
```

```
set route net=<IP Address> mask=<Subnetmask> metric=1
wanname="<username>"
```

Note: The wanname command must match the set username command. In this example the username is "<username>" as in step 2.

7. To enable the new wan interface, enter the following command:

```
set user name="<username>" dialout=on
```

Note: If you change a filter type after an initial configuration, you must reboot for the filter to take effect.

## Configure Serial Port Settings

### Example

The following example shows a simple outbound PPP configuration with filters and the following properties:

- The port is set up for outbound connections .
- Flow control is set to Hardware (for the PortServer TS 1/3+Modem default is Hardware.)
- Default device and scripts are used

```
set filter name="<filter name>" s1="dst/<IP Address>/<Subnetmask>"
set flow range=1 ixon=off ixoff=off rts=on cts=on
set user name="<username>" protocol=ppp
set user name="<username>" ipaddr=negotiated
    ipmask=255.255.255.255
set user name="<username>" defaultaccess=netservice autoport=513
    password=on
set user name="<username>" outgoing=on autoservice=default
set user name="<username>" bringup="<filter name>"
set user name="<username>" device="gendialer"
set device name="gendialer" baud=no dialer=genmdm chat=no port=1
set forwarding state=active splithorizon=off poisonreverse=off
set route net=<IP Address> mask=<Subnetmask> metric=1
    wanname="<username>"
set user name="<username>" dialout=on
```

**Note:** If you do not require filters for your outbound PPP connection, you may use this example by omitting step 1. If there is no filter, when the dialout connection is turned on, the device will automatically dial out.

## Filters for PPP Connections

Filters are used to manage and control PPP connections. You can design a filter to do any of the following:

- Bring up a connection
- Allow certain types of packets to use the connection and keep certain types of packets from using it
- Keep a connection up
- Send a message to the log file when a specified event occurs on the connection

You might, for example, develop a filter that brings up a connection on an outbound port only when device server handles a packet carrying a particular destination IP address.

The set user command has fields that define how a filter functions, that is, whether it is the type of filter that accepts or blocks packets, brings up a connection, keeps up a connection, or sends a message to the log file. The following table describes each of the set user fields related to filtering.

For more information about using filters see "set filter" on page 101.

set user Field	Description	Example
passpacket	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.
keepup	Causes the idletimeout timer to be reset and a connection maintained.	Filter that causes the connection to be maintained as long as there is any packet traffic except RIP packets.
bringup	Causes the Digi device to establish a connection.	Filter that causes an outgoing connection to be initiated whenever a packet specifying a particular IP address is handled.
logpacket	Causes the Digi device to send a message to the log file.	Filter that notifies the log anytime an ICMP packet is handled.

### See also

For more information, see these command descriptions:

- set user on page 185
- set filter on page 101

## Configure Serial Port Settings

### Configure Industrial Automation (IA)

To configure how devices in an industrial automation (IA) environment communicate, use the following command:

```
set ia
```

The syntax for `set ia` varies according to the IA device being configured: serial port-connected devices, network-based masters, network-based slaves, and serial master routes. The `set ia` command description on page 114 shows these syntax variations, the effects of the command fields for each variation, and examples of configuring several IA devices. See `set ia` on page 114 for command syntax, field descriptions, and examples.

### Protocols for IA Devices

IA devices can use either of the following communication protocols:

- Modbus protocol
- A “user-defined” protocol

Following are guidelines on configuring devices to use each protocol.

### Modbus Configuration Guidelines

When using the `set ia` command to configure devices that will run the Modbus protocol, follow these guidelines:

- 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.

**User-Defined Protocol Configuration Guidelines**

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.

When using the `set ia` command to configure devices that will run the user-defined protocol, follow these guidelines:

- 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.

## Configure Serial Port Settings

### Configure Modem Emulation

Modem emulation enables a system administrator to configure a networked Digi device server to act as a modem. The Digi device server emulates modem responses to a serial device and seamlessly sends and receives data over an Ethernet network instead of a PSTN (Public Switched Telephone Network). The advantage for a user is the ability to retain legacy software applications without modification and use a less expensive Ethernet network in place of public telephone lines.

To use a Digi device server for modem emulation, do the following:

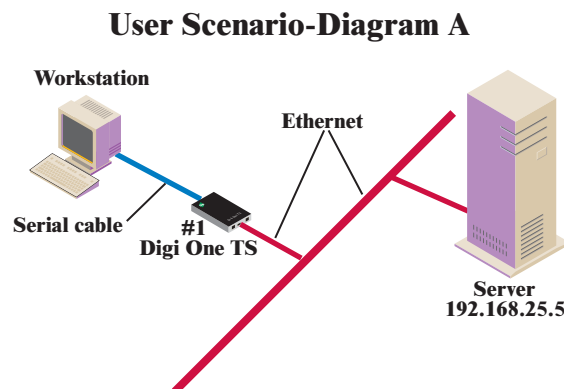
- Use a cable with the correct wiring pinouts (see "Modem Emulation Cable Signals" on page 24).
- Configure the serial ports and device type with the Web Interface.

Note: Before AT commands are accepted, DSR must go high on the Digi device server.

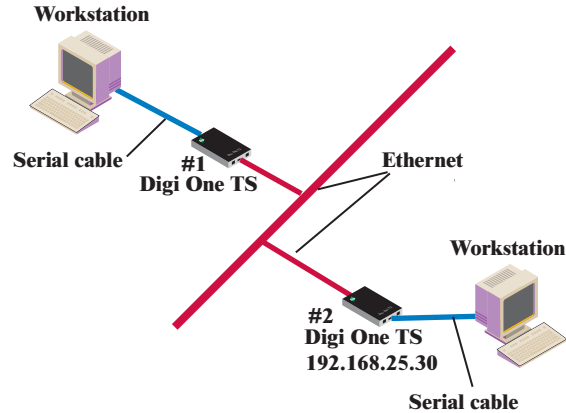
The AT commands used with modem emulation are described in the AT Command Reference.

### Common User Scenarios

The Digi device server in modem emulation mode allows for the easy replacement of modems in almost any environment where there is a LAN or WAN.



In Diagram A, the Digi One TS replaces a modem connected to a workstation running an application. The Digi One TS allows for the use of software applications without modification by responding to all the AT commands configured in the workstation application. The Digi One TS connects to the IP Address of the server when an `ATDT ipaddress:port` (`ATDT 192.168.25.5:50001`) command is issued. Once the remote device establishes the TCP connection, a `CONNECT` message is sent to the serial port and only then does the Digi device server switch from AT command mode to data mode. Using the modem escape sequence or dropping DTR on either side terminates the connection. A `DISCONNECT` message will be sent to the application if the remote side closes the TCP connection.

**User Scenario-Diagram B**

In Diagram B, two Digi device servers will replace modems on both sides of the connection. The initiation of the connection occurs with either of the Digi device servers. If both ends are Digi device servers, the TCP listening port number is 50001 for port 1. An example of the connection command is `ATDT 192.168.25.30:50001`. Upon establishing a successful TCP connection, a `CONNECT` message is sent to the serial port and only then does the Digi device server switch from AT command mode to data mode. After the `CONNECT` is received, the transmission of data begins. Using the modem escape sequence or dropping DTR on either side terminates the connection.

Modem emulation has the ability to communicate to an infinite number of other devices.

## Configure Serial Port Settings

### Modem Emulation Cable Signals

Use the following signal assignments to make a cable connecting the Digi device server to a serial device.

Note: DSR and DTR on the serial device side are connected to the DSR signal of the Digi device server.

Serial Device		Digi Device Server
CTS (in)		RTS (out)
RTS (out)		CTS (in)
DSR (in)		DSR (in)
DTR (out)		
DCD (in)		DTR (out)
TX (out)		RX (in)
RX (in)		TX (out)
GND		GND

**Originating,  
Answering, and  
Disconnecting  
Calls****Originating Calls**

To send data to a Digi device server, enter the following information for your application replacing the telephone number with the Digi device server's IP address and TCP port number. Enter the following command:

```
ATDT ipaddress:tcp_port#
```

For example:

```
ATDT 146.135.13.5:50001
```

**Answering Calls**

The Digi device server listens on a pre-defined TCP port to receive data. When the Digi device server receives a call notification (RING) through a serial port to begin a TCP connection, it needs to reply with an ATA or a pre-configured Auto-Answer to answer the call.

Note: The TCP ports assigned to the serial ports are as follows:

Serial port 1 listens on TCP port 50001

Serial port 2 listens on TCP port 50002

Serial port 3 listens on TCP port 50003

Serial port 4 listens on TCP port 50004

**Disconnecting Calls**

The TCP connection disconnects by either dropping the DTR signal on the serial port or sending the escape sequence <P>+++<P> to the Digi device server. <P> represents a one second pause.

**Disconnecting Calls-Digi Device Server**

The Digi device server sends a NO CARRIER response to the serial port when the network connection is dropped.

## Configure Serial Port Settings

### Configure 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.

To configure TCP socket communications, use the sockets field on the set config command. See set config on page 89.

### Configure UDP Multicast Communications

UDP multicast is used to send serial data over an Ethernet cable to one or many hosts at the same time.

To configure UDP multicast communications, use the set udpdest command. See set udpdest on page 181.

### Configure 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. Once the user is authenticated, an automatic connection to a host is made.

To configure autoconnection, either by port or by user, use the following commands:

- set ports - auto, autoservice, dest, dev, and dport fields. See set ports on page 143.
- set user - name, autoconnect, autohost, autoport, and defaultaccess fields. See set user on page 185.

## Examples

### Configure an autoconnect port

In this example, the set ports command configures the port so that all incoming users are automatically connected via Telnet to the host specified on the dest field. The port is also available for outgoing connections.

```
set ports range=1 auto=on dest=199.125.123.10 dev=mio dport=23
```

### Configure an autoconnect user

In this example, the set user command configures user4 to be automatically connected via Telnet to a host at address 199.193.150.10.

```
set user name=user4 autoconnect=on autohost=199.193.150.10  
autoport=23 defaultaccess=autoconnect
```

## Configure Wireless Devices

To configure wireless devices, use the `set wlan` command. See `set wlan` on page 197. Configuring a wireless device involves specifying:

- The authentication used for the device
- Whether the device automatically detects available Set Service Identifiers (SSIDs).
- The country code for the device's radio
- The number of access points in the vicinity
- The antenna choice for transmit and receive
- Whether the device uses encryption, and if so, which kind
- The encryption key, if encryption is used
- The fragmentation boundary for directed messages
- The number of bytes used for the RTS/CTS handshake
- The desired SSID for the device

### Example

```
set wlan ssid="homeBase" encryption_mode=128
encryption_key=ab1F793f01578ebf567afeb567
set wlan ssid="homeBase" em=128 ek=ab1F793f01578ebf567afeb567
```

## Configure Network Settings

Configuring network settings involves the following:

- IP routing
- Domain Name Server (DNS)
- Simple Network Management Protocol (SNMP)

## Configure IP Routing

Configuring IP routing involves these tasks:

- Configure static routes using the `set route` command
- Configure dynamic routes using the `set forwarding` command
- Configure Proxy ARP using the `set forwarding` command

## Configure Static Routes

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

- `net` 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.
- `gateway` is the IP address of the device that is the next hop to the destination.

For more information, see `set route` on page 154.

**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  
wannname=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
```

## Configure Network Settings

### Configure Dynamic Routes Using RIP

To configure the device server for dynamic routing using the Routing Information Protocol (RIP), enter the following command:

```
set forwarding
```

For more information, see `set forwarding` on page 109.

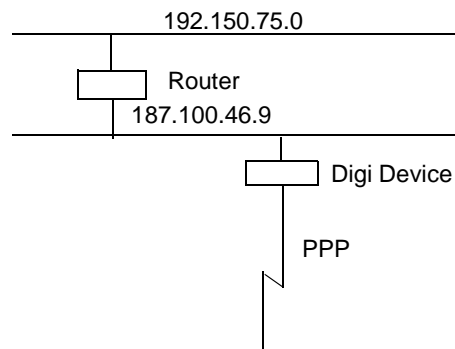
#### Procedure

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.

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

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
```

## Configure Proxy ARP

To configure the device server for Proxy ARP, enter the following command:

```
set forwarding
```

For more information, see `set forwarding` on page 109.

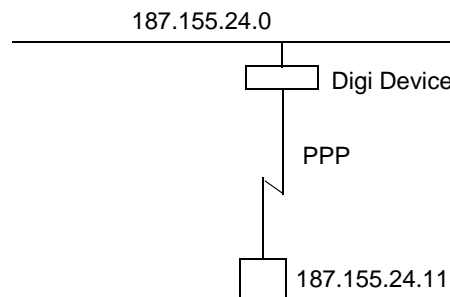
### Procedure

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.

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 the device server for Proxy ARP by supplying a `set forwarding` command that specifies the following:
  - `state=passive`
  - `proxyarp=on`

### Example

In this example, the 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
```

### Configure Domain Name System (DNS)

The domain name system (DNS) maps domain names to information associated with these names, such as IP addresses. Configuring the DNS involves the following tasks:

- Configure a DNS server
- Configure the host table

### 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 do the following:
  - 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.

### Name Server Types

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

Following 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`.

**Configure a  
DNS 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

For example:

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

For more information, see `set config` on page 89.

**Configure the  
Host Table**

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

For example, the following commands configure three IP address-to-name mappings:

```
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
```

For more information, see `set host` on page 113.

### Configure SNMP

Simple Network Management Protocol (SNMP) is the network management protocol that governs the exchange between nodes and stations.

### 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).

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.

### 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.

### MIBs

The SNMP management 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)

**Supported Trap Messages**

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

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

- Cold starts (device server initializes)
- Authentication failures
- Login attempts

**Command for Configuring SNMP**

To configure SNMP, enter the following command:

```
set snmp
```

For more information, see `set snmp` on page 166 .

**Example**

The following command configures SNMP with all trap options

```
set snmp run=on trap_dest=190.175.178.73 auth_trap=on  
cold_start_trap=on link_up_trap=on curr_thresh_exc_trap=on  
temp_thresh_exc_trap=on
```

## Configure Security Features

From the command line, you can configure several security-related features to do the following:

- Control access to the configuration
- Control access to inbound ports
- Control access to outbound ports
- Restrict access to outbound ports
- Use CHAP authentication for PPP users
- Control user access to the command line
- Use RADIUS to authenticate users
- Issue user passwords
- Configure SSH Version 2 for secure communication

### Control Access to the Configuration

Access to the configuration can be controlled by either of the following methods:

- Through user attributes; that is through various fields on the set user command
- Through network settings; that is, through the network field on the set user command

Controlling access of the 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. For information on the limitations placed on regular users for each command see set user on page 185.

## Control Access to Inbound Ports

An inbound port is one defined on the `dev` field of the `set ports` command for one of the following device types:

- `term`, for terminal connections
- `min`, for incoming modem connections)
- `mio`, for bi-directional modem connections)
- `hdial`, `hio`, for computer connections)

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

The login and password requirement for inbound ports can be changed by configuring either of the following:

- 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.

For more information, see `set ports` on page 143.

### Change 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
```

For example:

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

For more information, see `set logins` on page 133.

### Change a User's Access Requirements

To configure a user so that they do 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.

For example:

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

For more information, see `set user` on page 185.

### Control Access to Outbound Ports

An outbound port is one defined on the dev field of the set ports command for one of the following device types:

- prn, for printer connections
- mout, for outbound modem connections
- mio, for bi-directional modem connections
- host, for host connections)
- ia, for industrial automation devices

The default for outbound ports is unlimited access.

### Restrict Access to Outbound Ports

Use the set auth command to restrict access to outbound ports.

### Use 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.

### Control User Access to the Command Line

You can restrict user access to the device server command line through the following methods:

- Using the autoconnection feature
- Using menus

#### Using the Autoconnection Feature

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. Use set ports command, with the auto, autoservice, dest, dev, and dport fields. See set ports on page 143.
- 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 host is made. Use the set user command, with the name, autoconnect, autohost, autoport, and defaultaccess fields. See set user on page 185.

#### Using Menus

Menus select destination systems without having to access the device server command line. Menus are created using the set menu command. For information on configuring menus, see set menu on page 136.

## Use RADIUS to Authenticate Users

The RADIUS feature is available on PortServer 8/16 devices only.

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.

The device server can be configured 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.

### 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.

### How RADIUS Works

When a device server is configured for RADIUS, the authentication process is as follows:

- A user logs into device server.
- The 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.

### The `set radius` Command

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)

For example:

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

For more information, see `set radius` on page 152.

**Using a Secondary RADIUS Server**

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 Table Key**

The numbers in the following tables have the following meaning:

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

### Issue User Passwords

To establish passwords for users, and issue them to users, use the following commands:

- `set user`, with the password field - To require a password of a user. See `set user` on page 185.
- `newpass` - To create or change a user's password. See `newpass` on page 67.

### Procedure

This procedure assumes that you have signed on as root and already used the `set user` command to configure the user to whom you will be issuing a password.

The Advanced tab under User allows you to set Escape characters for Connect, Telnet, Rlogin, and Kill as well as an SSH Public Key. Click **Apply** to save the settings.

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.

## Configure SSH Version 2 Encryption for Secure Communication

Users can be configured to use SSH version 2 encryption for secure communication. SSH keys need to be generated from your SSH client.

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

### Devices support for SSH

SSH version 2 encryption is only available for the following devices.

Device	Required Hardware	Required Firmware
Digi One TS	50000771-01A or higher	82000747a or higher
PortServer TS 2 MEI	50000771-02A or higher	
PortServer TS 4 MEI & Wireless	50000771-03A or higher	

### Configure Password Protection for an SSH User

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. For example:

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

For more information, see `set user` on page 185, and `newpass` on page 67.

### Use 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. SSH keys need to be generated from your SSH client.

For example:

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

See `set user` on page 185 for more information.

### Make 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. For example:

- Reverse SSH connection to Port 1: `ssh 192.1.2.3 2501`
- Reverse SSH connection to Port 4: `ssh 192.1.2.3 2504`

## Configure Security Features

### Control Access to Services

You can disable services, such as Telnet and Rlogin, for inbound users, which means that users 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.

To control access to services for inbound users, use the `set secureaccess` command. See `set secureaccess` on page 162.

#### Services that Can Be Disabled

The following services can be disabled:

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

#### Service Levels

The service levels, or levels of secure access, are as follows:

- Secure, which means that SSH is the only service available to inbound users
- High, which means that SSH, HTTP, 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.

#### Examples

##### Disable inbound Telnet connections

```
set secureaccess telnet=off
```

##### Disable all services except SSH

```
set secureaccess level=secure
```

## Configure Power Over Serial Ports

Power over serial ports is only available for the following devices:

- PortServer TS 2/4 MEI
- Digi TS Wireless Family

Power over serial ports is a hardware feature. Enabling this feature involves changing a jumper inside the device. See the TS Family User Guide's chapter on power over ports for more details.

From the command line, the only power-related task you can perform is to reset the circuit breaker.

### Reset the Circuit Breaker

1. Display the status of the circuit breaker by entering:

```
display circuitbreaker
```

or

```
set config print
```

2. Reset the circuit breaker by entering:

```
set configuration circuitbreaker=reset
```

For more information, see `display` on page 57, and `set config` on page 89.

## Configure User Attributes

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

- 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

### Commands for Configuring a User

User attributes are configured by the following commands:

To:	Use this command:
Set common user-related features	set user (name=) Common user-related features are described in "Common Configurable User Features" on page 47.
Assign a password to a user	newpass
Configure a menu to be automatically displayed for a user	set user defaultaccess=menu
Automatically connect a user	set user autoconnect, autoconnect, autohost, autoport, autoservice fields
Defines the number of outbound ports a user connected over the LAN can access at one time.	maxsessions
remove a user from the user table	remove
Use a RADIUS server to set user attributes	set radius

## Common Configurable User Features

The following table describes common user-related features that can be configured by fields on the set user command. For a complete list of features, see the set user on page 185.

Feature	Description	set user Field
accesstime	Determines the times and days the user can access the device server.	accesstime
autoconnect	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.	autoconnect autohost autoport autoservice
Default access type	Defines the type of access the user is restricted to. Menu, command line, autoconnect, and outgoing and netservice are the types.	defaultaccess
Menu access	Defines the menu that is to be presented to a user with menu access.	menu
Port access	Defines the number of outbound ports a user connected over the LAN can access at one time.	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

## Configure Embedded Modem

Configure the embedded modem with the `set embmodem` command. For more information see `set embmodem` on page 98.

The embedded modem feature can be configured from the Web Interface (enter the IP address in the URL address bar of your browser, and log in with user name `root` and password `dbps`).

## Configuration Management

Configuration management tasks performed from the command line include:

- Upgrading firmware
- Copying the configuration to and from a remote host
- Resetting the configuration to defaults

### Upgrade Firmware

To upgrade firmware, use the following command:

```
boot
```

See `boot` on page 52.

### Copy the Configuration to and from a Remote Host

To use the command line to copy the configuration to and from a remote host, use the following command:

```
cpconf
```

See `cpconf` on page 56.

### Reset the Configuration to Defaults

To reset the configuration to factory defaults or the latest version stored in NVRAM, use the following command:

```
revert
```

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.

See `revert` on page 75.

This chapter provides the following:

- Basic information that applies to all commands, including navigation and editing keys, displaying online help, abbreviating commands, and syntax conventions.
- A description of each command.

## Basic Command Information

### Navigation and Editing Keys

Use the keys listed in the table to navigate the command line and edit commands:

Action	Keys
Move the cursor back one space	Ctrl b
Move the cursor forward one space	Ctrl f
Delete the character to the left of the cursor	Back space or Ctrl h
Delete the character under the cursor	Delete
Scroll back through commands	Ctrl p
Scroll forward through commands	Ctrl n
Execute the command	Enter

### Displaying Online Help

Help is available for all commands. The table describes how to access it.

For information on ...	Type
All commands	? (with no additional parameters)
A specific command	The command and then ? <b>Example:</b> info ? <b>Example:</b> set user ?

### Abbreviating Commands

All commands can be abbreviated. Simply supply enough letters to uniquely identify the command.

## Syntax Conventions

Presentation of command syntax in this manual follows these conventions:

- Brackets ([]) surround optional material.
- Braces ({}), surround entries that require you to choose one of several options, which are separated by the UNIX pipe (|).
- Non-italicized text indicates literal values, that is, fields or values that must be typed exactly as they appear. Yes and no options are examples of literals.
- Italicized text indicates that a type of information is required in that field. For example, *filename* means that the name of a file is required in the field.

## admin

<b>Purpose</b>	Used to temporarily access commands reserved for administrators (root) when logged in as a normal (non-root) user. After issuing the admin command, the following occurs: <ol style="list-style-type: none"><li>1. A prompt requesting the root password appears.</li><li>2. You enter the root password.</li><li>3. If the password is accepted, the device displays the root prompt, indicating that you can issue commands reserved for administrators. If the password is not accepted, the device displays the message, "Incorrect password."</li></ol>
<b>Required privileges</b>	Only normal users can use the admin command.
<b>Syntax</b>	<code>admin</code>
<b>Example</b>	<code>admin</code>
<b>See also</b>	For information on ending temporary root sessions, see the following commands: <ul style="list-style-type: none"><li>• <code>exit</code> on page 61</li><li>• <code>quit</code> on page 72</li></ul>

boot

## boot

<b>Purpose</b>	Performs the following functions: <ul style="list-style-type: none"><li>• Reboots the device server.</li><li>• Restores the configuration to defaults.</li><li>• Loads new POST code from a TFTP server.</li><li>• Loads a new firmware into flash ROM from a TFTP host.</li></ul>
<b>Device support</b>	Users of Digi One RealPort, Digi One IA RealPort, and PortServer TS 2/4 devices must be very careful with the load option. If this operation fails and then you reboot, the unit may not work. To ensure success, do the following: <ol style="list-style-type: none"><li>1. Attempt to boot from a remote firmware image before issuing the boot load command. See set config on page 89 for more information.</li><li>2. After issuing the boot load command, ensure that you receive the message “The image in flash now appears valid.” If you do <b>not</b> receive this message, do <b>not</b> reboot. Call technical support for instructions on what to do next.</li></ol>
<b>Required privileges</b>	Root privileges are required to use this command.
<b>Syntax</b>	<p><b>Reboot the device server</b> <code>boot action=reset</code></p> <p><b>Restore configuration defaults</b> <code>boot action={eewrite   factory   reset} switch={factory   user}</code></p> <p><b>Load new firmware from a TFTP host</b> <code>boot load={host-ip-address   host-name}:[load-file]</code></p> <p><b>Load new POST code (Digi One and PortServer TS 2/4 only)</b> <code>boot load-post=tftp-server-ip:filename</code></p> <p><b>Load new boot code (PortServer TS 8/16 only)</b> <code>boot load-post=tftp-server-ip:filename</code></p>
<b>Fields</b>	<p><b>action</b> The action to be performed.</p> <p><b>eewrite</b> Resets all but the network-related parts of the configuration to defaults. Ports, users, passwords, and most other features are reset. This option does <b>not</b> apply to the PortServer TS 8/16.</p> <p><b>factory</b> Resets the entire configuration to defaults. For PortServer TS 8/16, this option also reverts to the factory EOS.</p>

**reset**

Reboots the device.

**load**

The firmware to be loaded.

**{*host-ip-address* / *host-name*}**

The IP address or host name of a host with new firmware, which is then burned into flash ROM. The host must be running TFTP.

**[*file*]**

The firmware file.

**load-post**

The POST or boot code to be loaded.

***tftp-server-ip***

The IP address of a server running TFTP.

***post-file-name***

The file that holds the new POST or Boot code.

**switch**

Determines the firmware to use on reboot. This option applies to PortServer TS 8/16 only.

**factory**

The firmware that shipped with the device.

**user**

The most recent firmware upgrade.

**Examples****Reload firmware and reset configuration to defaults**

```
boot action=factory
```

**Reset all-but the network-related parts of the configuration to defaults**

This example does **not** apply to PortServer TS 8/16.

```
boot action=eewrite
```

**Reboot device and use current firmware and configuration**

```
boot action=reset
```

**Load firmware using a boot host**

The command loads the firmware stored on the host into flash ROM. A reboot is required to use the new firmware.

```
boot load=198.150.150.10:os-1
```

**See also**

- `cpconf` on page 56 for information on saving the current configuration to a host prior to restoring the configuration to defaults.
- `revert` on page 75 for information on restoring configuration defaults to the latest configuration stored in NVRAM.

close

## close

### Purpose

Closes active Telnet, Rlogin, and connect sessions.

The close command is associated with the sessions displayed by the status command. That is, you can only close sessions that are displayed by the status command by issuing a close command, and not by the kill command.

A close command issued without options closes the current connection.

To issue the close command, you must escape the active session. Do this by pressing the escape key defined for your session type. The following table lists default escape keys.

Session Type	Default Escape Keys
Connect	Ctrl [ Enter
Rlogin	~ Enter
Telnet	Ctrl ] Enter

### Required privileges

Anyone can use this command.

### Syntax

```
close [{* | connection-number}]
```

### Fields

\*

Closes all active sessions.

#### ***connection-number***

Identifies the session to close by its session number.

### Examples

#### **Close a session identified by number**

```
close 1
```

#### **Close the current session**

```
close
```

### See also

- kill on page 65. The kill command has a broader effect than close, and lets you kill connections from the global list; that is, it is not limited to sessions associated with the current connection.
- set user on page 185 for information on defining escape keys for Telnet, Rlogin, and connect sessions.
- status on page 205 for information on displaying status information on active sessions.

## connect

### Purpose

Initiates a local connection on a port.

There are several ways of using the connect command:

- To make multiple connections, issue multiple connect commands.
- To temporarily suspend a connection, escape the active session by pressing the escape character defined on the set user command. The default escape character is Ctrl [ (Control key and left bracket).
- To temporarily suspend a connection and return to the command line, press the escape character and then the Enter key.
- To switch between active sessions (without first escaping to the command line), press the escape character and then the number of the session you wish to enter. Pressing the connect escape character twice causes the next session to appear, enabling you to easily page through sessions.

### Required privileges

Anyone can use this command.

### Syntax

```
connect {serial_port | hunt_group | id-name}
```

### Fields

#### ***serial\_port***

The number of the port on which to establish a connection.

#### ***hunt\_group***

Identifies a hunt group, which is defined by the set ports group command.

#### ***id-name***

The name (defined on the set ports command) of the port on which to establish a connection.

### Example

The following command creates a connection to port 1:

```
connect 1
```

### See also

- close on page 54 for information on ending a session.
- reconnect on page 73 for information on reestablishing a port connection.
- set user on page 185 for information on defining an escape character.
- set ports on page 143 for information on defining a hunt group.

cpconf

## cpconf

### Purpose

Used to:

- Restore the configuration from a remote host.
- Copy the configuration to a remote host.
- Display the configuration on a terminal.

### Required privileges

Root privileges are required to use this command.

### Syntax

```
cpconf {fromhost=host[:file] | tohost={host[:file] | term}}
```

### Fields

#### fromhost

Copies the configuration from the host and file specified. Be sure to:

- Identify the host by either its IP address or DNS name.
- Separate host and file fields by colons.

If you do not specify a file, the default, config.ps3, is used.

#### tohost

Copies the configuration to the host and file specified. Be sure to:

- Identify the host by either its IP address or DNS name
- Separate the host and file information by a colon.

If the filename is not specified, config.ps3 is used.

TFTP must be running on the host. For transfers to the Digi device, the file must be in the TFTP directory and assigned read-write permissions for all users.

#### term

Displays the configuration file on the terminal that issued the command.

### Examples

#### Copy configuration from a host

```
cpconf fromhost=190.150.150.10:ps-cnfg1
```

#### Copy configuration to a host

```
cpconf tohost=190.150.150.10:ps-cnfg1
```

#### Copy configuration to a terminal

```
cpconf term
```

## display

### Required privileges

Used to:

- Display the status of the EIA-232 signals on serial ports.
- Display a list of errors.
- Clear the errors list.
- Display information on Digi devices that use dip switch settings to enable multiple electrical interface (MEI) on serial ports.
- Display power information for the Digi devices that support the powered Ethernet feature.

To display the contents of a port buffer, use the `display buffers` command instead. See `display buffers` on page 59.

### Required privileges

Anyone can use this command to display information. Root privileges are required to clear the errors list.

### Syntax

#### Display information

```
display {port range=port-port | error | power | switches
|circuitbreaker}
```

#### Clear errors

```
display error clear
```

### Fields

#### circuitbreaker

Displays status of the circuit breaker.

#### clear

Clears the errors list.

#### error

Does one of the following:

- Clears all errors from the errors list when the clear option is specified.
- Displays a list of errors when the clear option is **not** specified.

#### port

Displays signal state for the ports specified on the range option. There is only one port on the SP/IA.

#### power

Displays status of power sources for the Digi devices that support the powered Ethernet option. This option does not apply to PortServer TS 8/16 and some Digi One and PortServer TS 2/4 devices.

#### range

A range of ports. There is only one port on the SP/IA.

#### switches

Displays dip switch settings for devices supporting MEI.

display

**Examples**

**Display configuration information on a port**

```
display port range=1
```

**Display configuration information on a range of ports**

```
display port range=1-2
```

**Display a list of errors**

```
display error
```

**Display information on dip switch settings**

```
display switches
```

**Display power information**

```
display power
```

**Clear errors**

```
display error clear
```

**See also**

display buffers on page 59 to display the contents of a port buffer.

## display buffers

### Purpose

Used to:

- Display the contents of a port buffer.
- Transfer the contents to a server running TFTP.
- Configure the screen parameters.

### Device support

The following table lists the devices to which this command applies:

Device	Required Hardware	Required Firmware
Digi One RealPort	Not supported.	Not supported.
Digi One IA	Not supported.	Not supported.
Digi One TS Digi One TS Wireless	50000771-01A or higher	82000747a or higher
PortServer TS 2 MEI PortServer TS 2 MEI Wireless	50000771-02A or higher	
PortServer TS 4 MEI PortServer TS 4 MEI Wireless	50000771-03A or higher	
PortServer TS 8	All levels	82000684c or higher
PortServer TS 16	All levels	

### Required privileges

Root privileges are required to use this command.

### Syntax

```
display buffers [range=range] {screen [lines=number]
[tail=number] / tftp=server:filename}
```

### Fields

#### lines

The number of lines of data to display at a time when the screen option is specified. Use 0 to indicate continuous flow.

#### range

The port or ports to which the command applies.

#### screen

Displays the port buffer contents on the screen.

#### tail

The total number of lines in the buffer to be displayed. The number is calculated from the end of the buffer counting back.

#### tftp

##### server

The IP address or DNS name of a server running TFTP to which buffer information should be transferred.

display buffers

***filename***

The name to use for the file that will be transferred to the TFTP server.

**Examples**

**Display port buffering information on the screen**

```
display buffers range=2 screen lines=32 tail=30
```

**Output buffering information to a TFTP server**

```
display buffers range=2 tftp=stambrose:port_ouput
```

**See also**

- set buffers on page 85
- set wlan on page 197

## exit

**Purpose**

Used to terminate either of the following sessions:

- Your current session.
- A temporary root session. If you are in a root session, the exit command returns you to a regular session.

**Required privileges**

Anyone can use this command.

**Syntax**

```
exit
```

**Example**

```
exit
```

**See also**

- admin on page 51 for information on starting a temporary root session.
- quit on page 72 for an alternate method of ending a root session.

help

## **help**

**Purpose** Displays information on commands.

**Required privileges** Anyone can use this command.

**Syntax** help

**Example** help

**See also** "Displaying Online Help" on page 49.

## info

**Purpose** Displays or clears statistics, including protocol, interface, IA, serial, and UDP over serial. The statistics displayed are those gathered since the statistics tables were last cleared.

**Required privileges** Normal users can view statistics tables. Root privileges are required to clear them.

**Syntax**

**Clear statistics**

```
info clear {protocol | network | serial:port | ia:protocol
| sou:range}
```

**Display statistics**

```
info {protocol | {network | serial:port | ia:protocol /
sou:range}
```

**Fields**

**info clear**  
Clears all the statistics tables. This command resets all the counts in the statistics tables to zero.

**info {*protocol* | network | serial:*port* / ia:*protocol* / sou:*range*}**  
Displays one or more statistics tables, depending on the option specified. The following table describes the syntax options and results:

Syntax	Result	Example
info clear	All statistics are cleared.	info clear
info <i>protocol</i> where <i>protocol</i> is one of the following: wlan, frame, modbus, ip, icmp, ethernet tcp, or udp.	wlan, frame, modbus, ip, icmp, tcp, or udp tables are displayed.	info ip
info network	All network interface statistics are displayed.	info network
info serial: <i>port</i> where <i>port</i> the port number.	Port statistics are displayed. For descriptions of these statistics, see About the port statistics displayed by info serial on page 64.	info serial:1
info ia: <i>protocol</i> where <i>protocol</i> is one of the following: Compoway/F, df1fullduplex, df1halfduplex, fins, hostlink, modbus, userdefined.	IA protocol statistics are displayed.	info ia:fins
info sou: <i>range</i> where <i>range</i> is the port or ports.	Serial over UDP statistics associated with a serial port are displayed.	info sou:2

**About the port statistics displayed by info serial**

When you enter an info serial command, the statistics displayed and their meanings are as follows. Note that these statistics are the *number* of changes for each statistic. They are not a *value* of the statistics themselves. The numbers on these statistics will only increase from their previous counts, unless you set the count back to zero by issuing an info clear command.

Statistic	Description
rbytes	The number of bytes received.
tbytes	The number of bytes transmitted.
sigchange	The number of times the signals have changed states.
norun	The number of times FIFO has overrun.
noflow	The number of times the Received buffer has overrun.
nframe	The number of framing errors detected.
nparity	The number of parity errors detected.
nbreak	The number of breaks detected.

**Examples****Display the IP table**

```
info ip
```

**Display Modbus information**

```
info ia:modbus
```

**Display serial over UDP statistics for port 1**

```
info sou:1
```

**Clear all network statistics tables**

```
info clear
```

## kill

### Purpose

Clears or resets sessions on ports.

The kill command is associated with the connections displayed by the who command. That is, you can only close connections that are displayed by the status command by issuing a kill command, and not by the close command.

### Required privileges

Root privileges are required to use this command.

### Syntax

```
kill {tty=tty-number | tty=tty-range} | tty-number |  
tty-range}
```

### Fields

#### **tty=tty-number**

A port on which to clear a session. Number = 1.

#### **tty=tty-range**

A range of ports on which to clear sessions. Range = 1.

#### **tty-number**

An alternate method of specifying the number of the port on which to clear a session. Number = 1.

#### **tty-range**

An alternate method of specifying a range of ports on which to clear sessions. Range = 1.

### Examples

#### **Kill a session on a specific port**

```
kill tty=1
```

#### **Kill a session on a range of ports**

```
kill tty=1-2
```

### See also

- close on page 54, to close sessions for the current connection.
- who on page 211, for information on determining current users.

mode

## mode

**Purpose** Changes or displays the operating options for a current Telnet session.

**Required privileges** Anyone can use this command.

**Syntax** **Change Telnet options**  
`mode [bin={on|off}][crmod={on|off}][crlf={on|off}]`

### Display Telnet options

`mode`

## Fields

### bin

Specifies whether binary mode is enabled.

#### on

Turns on binary mode, which means that all transmitted and received characters are converted to binary during this Telnet session.

#### off

Turns off binary mode off for this Telnet session. The default is off.

### crmod

Specifies whether line feeds are added to received carriage returns.

#### on

Specifies that line feeds are added to received carriage returns.

#### off

Specifies that line feeds are **not** added to received carriage returns. The default is off.

### crlf

Specifies whether line feeds are added to transmitted carriage returns.

#### on

Specifies that line feed characters are added to transmitted carriage returns.

#### off

Specifies that line feed characters are **not** added to transmitted carriage returns. The default is off.

## Examples

### Turn on binary mode

```
mode binary=on
```

### Add line feed characters

```
mode crmod=on crlf=on
```

### Display operating options

```
mode
```

## newpass

- Purpose** Used to create or change your own password (if you are logged in under your own name); the root password, or another user's password (if you are logged in as root).  
When you enter the newpass command, a series of prompts guide you through the process of changing a password.
- Required privileges** Anyone can change his or her own password. Root privileges are required to change someone else's password or the root password.
- Syntax** `newpass [name=username]`
- Field** **name**  
The name of the user (configured with the set user command) whose password will be created or changed. This option is available only if you have root privileges.
- Example** The following command initiates a dialog that changes the user's password:  
`newpass`
- See also** See set user on page 185 for information on configuring users.

ping

## ping

### Purpose

Tests whether a host or other device is active and reachable.

### Required privileges

Anyone can use this command.

### Syntax

```
ping [continuous][fill=char] {hostname | ip-addr} [intv=msec]  
[loose_srout=ip-addr, ip-addr...] [npkts=num] [pktsiz=bytes]  
[record_route] [strict_srout=ip-addr, ip-addr...] [verbose]
```

### Fields

#### **continuous**

Specifies that pings be sent continuously until stopped. (Press the interrupt keys to stop continuous pings. The default interrupt keys are <Ctrl-C>.)

#### **fill**

Specifies characters to include in the data portion of the echo reply.

#### **intv**

The interval in milliseconds between pings. The range is -1 to 60,000. The default is 1000 milliseconds (one second). A value of -1 means that echoes will be continuously sent until the value in the npkts field is reached.

#### ***ip-addr* | *hostname***

Identifies the target of the ping by an IP address or domain name.

#### **loose\_srout**

Specifies that the ping should pass through the routers indicated on its way to the target host. These routers are identified by their IP addresses.

#### **npkts**

The number of packets to include with each ping. The range is 1 to 30,000. The default is 1.

#### **pktsiz**

The size of the ping packet in bytes. The range is 0 to 20000. The default is 56.

#### **record\_route**

Specifies that routers handling the ping include their IP addresses in the echo reply.

#### **strict\_srout**

Specifies that the ping pass through the routers indicated—and only those indicated—on its way to the target host. Routers are identified by their IP addresses.

#### **verbose**

Specifies that echo replies include statistics associated with the ping, such as round-trip time and number of packets transmitted and received.

**Examples****Specify a simple ping**

The ping command determines whether the specified host can be reached.

```
ping 199.150.150.10
```

**Specify loose source routing**

The command specifies that the ping must pass through the routers identified on the loose\_srout option but may pass through additional routers as well.

```
ping 199.150.150.10 loose_srout=199.150.160.10,190.150.161.10
```

**Specify strict source routing**

The command specifies that the ping pass through the routers identified on the strict\_srout field and only those routers. If it cannot reach the destination along this path, the destination is regarded as unreachable.

```
ping 199.150.150.10 strict_srout=199.150.160.10,190.150.161.10
```

power

## power

### Purpose

The power command can be used to perform the following actions:

- Control the power state of specific ports on the PortServer TS 8/16 or devices connected to the ports.
- Display the power state of specific ports on the PortServer TS 8/16.
- Display the status of a power unit.

This command is context-sensitive. The action specified will determine whether it applies to a power unit or a device connected to a power unit.

### Device support

This command applies to PortServer 8/16 devices only.

### Required privileges

Root privileges, users with command line access or users with specific menu access on ports are required to view or change states.

### Syntax

```
power [action={clear|on|off|reboot|show}] [range=(port#)]  
[outlet=outlet#)] [id=powerdeviceid] [group=group#)]
```

An outlet can be specified either by entering an outlet number or by using the id and/or group fields.

### Fields

#### action

Used in conjunction with range, outlet, id, or group fields. This field can be set to the following values:

#### clear

Clears the maximum detect current parameter of the specified power control unit.

#### on

The outlet or outlets configured to the device will receive power.

#### off

The outlet or outlets configured to the device will not receive power.

#### reboot

The outlet or outlets configured to the device will be power cycled with a 10 second wait until the user is prompted again. This command only works if the outlets are already receiving power.

#### show

Displays the status of the unit and/or devices connected for the specified range.

#### range

Performs the specified action on the power unit with the specified index.

#### outlet

Performs the specified action on the device with specified index.

#### id

Performs the specified action on the device unit with the specified ID. This field must be used with the action field.

**group**

Performs the specified action on an outlet with the specified group number.

**Examples****Display outlet status**

In this example, the power command displays the status of the outlets, including whether they are on or off, their IDs, and the group number.

```
power action=show range=2 outlets=3
```

Or:

```
power power range=2 outlet=3
```

**Display power unit status**

This example displays the status of two remote power control devices connected to PortServer. The items to be displayed include:

- Remote Power Control Unit ID (or which port it is on)
- Average Power
- Apparent Power
- True RMS Voltage
- True RMS Current
- Maximum Current Detected
- Internal Temperature
- Outlet Circuit Breaker Status
- Alarm Threshold

```
power action=show range=7-8
```

**Control power to a port**

This example turns off the power to all outlets affiliated with group 3.

```
power group=3 action=off
```

**Clear the maximum current detected**

This example clears the maximum current detected variable for the power unit on port 8.

```
power action=clear range=8
```

**Control a device with a device range**

This example turns on the power to the device on the unit 2 connected to the outlet 3.

```
power action=on range=2 outlet=3
```

**Control a device with an ID**

In this example, the power to all outlets affiliated with a device named "Router" will be rebooted. This command will only work if the outlets are all currently on.

```
power action=reboot id=Router
```

quit

## quit

### Purpose

Used to end the following types of sessions:

- The current session. If you are in a regular or root session, quit closes the session.
- A temporary root session. If you are in a root session started with the admin command, quit returns you to a regular session.

### Required privileges

Anyone can use this command.

### Syntax

```
quit
```

### Example

```
quit
```

### See also

See admin on page 51 for information on temporarily accessing commands reserved for the administrator.

## reconnect

**Purpose** Reestablishes a previously established connection.

**Required privileges** Anyone can use this command.

**Syntax** `reconnect [{serial-port | p=serial-port | s=session}]`

**Fields** ***serial-port***  
The serial port to which this command applies.

**p=*serial-port* | s=*session***  
The serial port or session to which this command applies.

**Example** **Reconnect to the last port used**

```
reconnect
```

**See also**

- connect on page 55 for information on establishing a connection on a selected port
- close on page 54 for information on ending a connection
- status on page 205 for information on gathering status on current connections

remove

## remove

**Purpose** Removes entries from configuration tables.

**Required privileges** Root privileges are required to use this command.

**Syntax** `remove table-name {range=range | name=name | ip=ip-address}`

### Fields

#### **ip=ip-address**

Removes an entry from a configuration table based on the IP address specified. This form of the command works only on entries that can be identified by an IP address, such as entries in the auth or altip tables.

#### **name=name**

Removes an entry from a configuration table based on the name specified. This form of the command works only on entries that can be identified by name, such as entries in the user table.

#### **range=range**

Removes entries from one of the device server configuration tables based on the range of table index entries

#### **table-name**

One of the following configuration table names:

- altip
- arp
- auth
- chat
- device
- filter
- host
- ippool
- menu
- powerunit
- route
- script
- service
- telnetip
- term
- user

### Examples

#### **Remove an entry from user table by name**

```
remove user name=martymertz
```

#### **Remove an entry from altip table by IP address**

```
remove altip ip=143.191.2.120
```

#### **Remove an entry from altip table by index number**

```
remove altip range=3
```

## revert

**Purpose** Restores the configuration to defaults or to the latest configuration stored in NVRAM.

The revert command does not restore **network-related parts of the configuration** to defaults.

**Required privileges** Root privileges are required to use this command.

**Syntax** `revert option={factory | nvram} [range]`

**Fields** ***option*={factory | nvram}**

Sets one of the configuration options either to the factory defaults or to the latest version of the configuration stored in NVRAM.

A revert nvram command is only useful if a set conf save=off command was previously issued to the device. See the command examples for more information.

The following table lists the allowable values for *option*, and their effect on the configuration.

option	Then this part of the configuration reverts ...
all	Entire configuration, except network connectivity parameters.
altip	set altip configuration
arp	set arp configuration
auth	set auth configuration
config	set config configuration
filter	set filter configuration
flow	set flow configuration
host	set host configuration
ia	set ia netmaster, set ia netslave, set ia serial, and set iaroute configuration
ianetmaster	set ia netmaster configuration.
ianetslave	set ia netslave configuration.
iaroute	set ia route configuration.
iaserial	set ia serial configuration.
keys	set keys configuration
line	set line configuration
login	set login configuration
menu	set menu configuration

revert

option	Then this part of the configuration reverts ...
network	altpip, arp, host, route, snmp, tcpip, and telnetip configuration. Not related to network connectivity.
port	set ports configuration
powerunit	set powerconfig. This option applies to PortServer TS 8/16 only.
radius	RADIUS configuration. This option applies to PortServer TS 8/16 only.
routed	Routing configuration
script	set script configuration
secureaccess	set secureaccess configuration
security	set auth, set logins, set radius, and set secureaccessconfiguration
serial	set flow, set line, set ports configuration, set power configuration (PortServer TS 8/16 only)
service	set service configuration
snmp	SNMP configuration
system	set config, set ethernet, set keys, set menu, set service, set terms, set trace, and set user configuration
tcpip	set tcpip configuration
telnetip	set telnetip configuration
terms	set terms configuration
trace	Trace settings
users	set user configuration

**range**

A range of ports to which the command applies. This field is valid when used with serial, port, line, flow, keys and login options.

## Examples

### Reset the port configuration to defaults

```
revert port=factory range=1
```

### Reset network-related settings

The configuration is reset to the latest user configuration saved in NVRAM.

1. First, turn off saving configuration changes to NVRAM by issuing the following command:

```
set config save=off
```

2. Change the baud rate of port 8 to 115200:

```
set line baud=115200 ra=8
```

3. Run a test of serial port 8 at 115200 baud.

4. Once testing is complete, return port 8 to normal:

```
revert line=nvram
```

5. Turn on saving configuration changes:

```
set config save=on
```

rlogin

## rlogin

**Purpose** Performs a login to a remote system, also referred to as an rlogin.

**Required privileges** Anyone can use this command.

**Syntax**  
`rlogin [esc=(char)] {hostname/host-ip-addr}  
[ {user=user-name | -l user-name} ]`

**Fields**  
**esc**  
A different escape character than the ~ (tilde) character, which will be used for the current Rlogin session. This character is used for suspending a session from the remote host to return to the device server command line.

**hostname**  
The name of a host to log into.

**host-ip-addr**  
The IP address of a host to log into.

**user=user-name | -l user-name**  
The user name to use on the remote system. If you do not specify a name, your device server user name will be used. The -l user-name option is for compatibility with the UNIX rlogin command.

**Examples** **Remote login using a host name**

```
rlogin host1
```

**Remote login using an IP address**

```
rlogin 192.192.150.28
```

**Remote login using a host name and user name**

The rlogin command establishes an Rlogin session using a host name. The command also supplies the name that identifies the user on the host.

```
rlogin host1 user=fred
```

**See also** See set user on page 185 for information on configuring a user-specific Rlogin escape character.

## send

**Purpose** Sends a control command to a Telnet peer.

**Required privileges** Anyone can use this command.

**Syntax** `send {ao|ayt|brk|ec|el|escape|ga|ip|nop|synch}`

### Fields

**ao**

Sends the “abort output” signal to discard output buffered on the peer.

**ayt**

Sends the “are you there” signal to test whether a host is still active.

**brk**

Sends the “break” signal to interrupt the executing application.

**ec**

Sends the “erase character” to delete the previous character.

**el**

Sends the “erase line” signal to delete the entire current line.

**escape**

Sends the “escape” character.”

**ga**

Sends the “go ahead” signal.

**ip**

Sends the “interrupt process” signal to terminate the program running on the peer.

**nop**

Sends the “no option” signal to the peer.

**synch**

Sends the “synchronize process” signal to the peer.

### Examples

**Send an “interrupt process” signal**

```
send ip
```

**Send an “are you there” signal**

```
send ayt
```

### See also

See telnet on page 206 for information on establishing Telnet sessions.

set altip

## set altip

### Purpose

Configures a serial port or group of serial ports with an alternate IP address, or displays current entries in the alternate IP addresses (altip) table.

Alternate IP addresses enable routing of traffic from the LAN to serial ports or group of ports using IP addresses. By associating ports with IP addresses, Telnet users on the LAN can use IP addresses, rather than port numbers, to specify a port or range of ports in their Telnet calls.

Up to 64 alternate IP address entries are permitted.

### Required privileges

Normal users can display altip information. Root privileges are required to change altip settings.

### Syntax

#### Configure alternate IP address

```
set altip group={port# / group#} ip=ip-addr mode={raw | telnet}
```

#### Display altip table entries

```
set altip [range=range]
```

### Fields

#### group

A port or group of ports.

#### ip

Assigns an IP address to the ports or group of ports (hunt group) specified on the group field.

#### range

A range of index entries in the altip table.

#### mode

Either raw or Telnet, which is used to determine a connection type for reverse Telnet connections.

### Examples

#### Display entire altip table

```
set altip
```

#### Display several entries in altip table

```
set altip range=1-4
```

#### Configure an entry in altip table

```
set altip ip=198.150.150.10 group=65
```

### See also

See set tcpip on page 171 (the sockets option) for information on configuring the base option.

## set arp

<b>Purpose</b>	<p>Manually configures an entry in the Address Resolution Protocol (ARP) table, or displays the contents of the ARP table.</p> <p>The ARP table contains the Ethernet-to-IP address mappings of other devices on the LAN, which is required to communicate with these devices. The ARP protocol updates this table automatically, so manual modification is seldom required.</p>
<b>Required privileges</b>	<p>Normal users can display information. Root privileges are required to change ARP table entries.</p>
<b>Syntax</b>	<p><b>Configure ARP table entries</b></p> <pre>set arp ether=<i>etaddr</i> ip=<i>ipaddr</i> [<i>tim2liv=time</i>]</pre> <p><b>Display ARP table entries</b></p> <pre>set arp [<i>range=range</i>]</pre>
<b>Fields</b>	<p><b>ether</b> The Ethernet address of a device.</p> <p><b>ip</b> The IP address of a device.</p> <p><b>range</b> A range of table entries, which are identified by the index field in the ARP table.</p> <p><b>tim2liv</b> The time, in seconds, to keep an entry in the ARP table. The range is 0 to 1200 seconds. The default is 0, which means the entry will never time out.</p>
<b>Examples</b>	<p><b>Display a range of entries in ARP table</b></p> <pre>set arp range=1-4</pre> <p><b>Display all entries in ARP table</b></p> <pre>set arp</pre> <p><b>Configure an entry in ARP table</b></p> <pre>set arp ip=198.150.150.10 ether=08:00:20:05:0b:da tim2liv=900</pre>

set auth

## set auth

### Purpose

Configures or displays access permissions to serial ports for LAN users.

The set auth command is a very powerful tool for limiting LAN users' access to ports. To produce the intended configuration results, follow these principles:

- The default for a port is unrestricted access. This means that all IP addresses have unrestricted access to a port unless you use the set auth command to place restrictions on port use.
- You can configure a new default by removing the default entry in the auth table (the entry that specifies an IP address of 0.0.0.0 and mask of 0.0.0.0). Then, the default becomes no access for any IP address. You can then use the command to permit access for particular IP addresses.
- In addition to unrestricted access, there are three types of restricted access:
  - Login access. The user of an IP address must log in before access to the port is granted.
  - RealPort access. Only the RealPort application can use the port.
  - No access. The user of the IP address cannot access the port.
- The most reliable way to use the command for configuration is to explicitly specify the type of access for each port on each command. In the examples that follow, which use an 8-port device, the “right” command accounts for all ports, and the “wrong” one does not:

Right: `set auth ip=192.10.10.10 realport=1-3 login=4-5  
unrestricted=6-8`

Wrong: `set auth ip=192.10.10.10 realport=1-3 login=4-5`

- When the only option specified on the set auth command is an IP address, that IP address loses all access rights to all outbound ports.
- When you use the set auth command to change access permissions for a particular IP address (or range of addresses), all other IP addresses are unaffected by the command.
- The mask field extends the scope of the set auth command to a range of IP addresses. In each mask position that a binary 1 appears, the incoming address must match perfectly with the address specified on the ip field.

The auth table is limited to 20 entries.

### Required privileges

Normal users can display information. Root privileges are required to change auth table entries.

**Syntax****Configure access permissions**

```
set auth ip=ipaddress [login={range | none}] [mask=mask]
[realport={range | none}] [unrestricted={range | none}]
```

**Display access permissions**

```
set auth [range=range]
```

**Fields****ip**

The IP address of the device to which this set auth command applies.

**login**

Requires that users of the IP address specified log in. A value of none indicates that users of the IP address specified have login access to none of the ports.

**mask**

Specifies an IP mask used to extend the scope of this set auth command to a range of IP addresses. The following table provides examples of how the mask field works:

IP Address	Subnet Mask	set auth mask	Result
143.191.0.0	255.255.0.0	255.255.0.0.	All users on this class B network are included in the restrictions applied to the outbound ports.
192.10.10.0	255.255.255.0	255.255.255.0	All users on this class C network are included in the restrictions applied to the outbound ports.
192.10.10.0	255.255.255.240	255.255.255.240	All users on this subnetted class C network are included in the restrictions applied to the outbound ports.

**range**

Specifies a range of auth table entries, identified by an index number, to which this command applies.

**realport**

Configures port access for RealPort running on the devices identified by the ip and mask fields. Use this option to grant access to RealPort but restrict access to other users of the IP address.

**unrestricted**

Configures unrestricted access for the IP address specified to the range of ports specified.

set auth

## Examples

### Display entire auth table

```
set auth
```

### Display a range of entries in auth table

```
set auth range=1-2
```

### Configure no access for an IP Address

```
set auth ip=199.150.10.12 mask=255.255.255.255 login=none  
realport=none unrestricted=none
```

### Configure mixed access

In this example, an 8-port device server is configured for mixed access.

```
set auth ip=199.150.10.12 mask=255.255.255.255 realport=1-4  
login=5-6 unrestricted=7-8
```

### Configure access for two IP addresses

This example requires three set auth commands:

- The first removes the default entry from the auth table, which changes the default setting from unrestricted access to all 8 ports for all IP addresses to no access to any ports for any IP addresses.
- The second and third commands restore unrestricted access to all ports for the IP addresses specified.

```
set auth ip=0.0.0.0 rauth=on  
set auth ip=199.22.33.4 realport=none login=none unrestricted=1-8  
set auth ip=199.22.33.8 realport=none login=none unrestricted=1-8
```

### Use the mask field to extend the command

In this example of a TCP/IP Class C network, the set auth commands configure RealPort running on any host on network 199.150.150.0 with access to ports 1 and 2. The other ports are not available to users of the IP address specified.

```
set auth ip=199.150.150.10 mask=255.255.255.0 realport=1-2 logon=none  
unrestricted=none
```

## See also

- set ports on page 143 for information on defining ports.
- set user on page 185 for information on configuring a user for outbound port access.

## set buffers

**Purpose** Configures buffering parameters on a port, or displays the port buffer configuration on all ports.

**Device support** The following table lists the devices to which this command applies:

Device	Required Hardware	Required Firmware
Digi One RealPort	Not supported.	Not supported.
Digi One IA	Not supported.	Not supported.
Digi One TS Digi One TS Wireless	50000771-01A or higher	82000747a or higher
PortServer TS 2 MEI PortServer TS 2 MEI Wireless	50000771-02A or higher	
PortServer TS 4 MEI PortServer TS 4 MEI Wireless	50000771-03A or higher	

**Required privileges** Root privileges are required to use this command.

**Syntax**

**Configure port buffering**

```
set buffer [clear] [range={number}] [size={number}]
[state={on | off | pause}]
```

**Display the port buffering configuration**

```
set buffer [range=range]
```

**Fields**

**clear**

Clears the contents of the specified buffer.

**range**

The port or ports to which the command applies.

**size**

The size in kilobytes to configure the buffer. The default is 32k and the maximum is 64k. Settings are configurable in 2k increments.

**state**

The buffering state, which can be any of the following:

**on**

The data will be buffered.

**off**

The data will not be buffered and all data will be cleared from the buffer.

**pause**

The data will not be buffered, but data in the buffer will not be cleared.

set buffers

## Examples

### Display port buffer configuration for all ports

```
set buffer
```

### Configure buffers

In this example, the set buffer command sets the buffer state for port 1 to on mode and the buffer size to 64 kilobytes.

```
set buffer range=1 state=on size=64
```

## See also

- display buffers on page 59.
- set wlan on page 197.

## set chat

### Purpose

Used to configure, display, remove, or rename entries in the chat table. Chat table entries provide telephone number string translation and can be accessed by any configured script. The chat table holds a maximum of 12 entries.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Configure chat table entries

```
set chat [delay=string][name=chat-name] [range=range]
[retry=number] [wait=string]
```

#### Display chat table entries

```
set chat [range=range]
```

#### Remove chat table entries

```
set chat {rmchat=on range=range | rmchat=chatname}
```

#### Rename a chat table entry

```
set chat name=name newname=new-name
```

### Fields

#### delay

A string of up to 24 characters to substitute into telephone numbers in place of the delay character.

#### name

Configures a name for the chat table entry.

#### range

One of the following:

- A range of ports to which the chat table entry will apply (only 1 for the SP/IA).
- A range of chat table index numbers, which identify chat table entries.

#### retry

The number of times to retry a call. The range is 0 to 99 times.

#### rmchat

Removes the chat table entry specified on the range or name field.

#### wait

A string of up to 24 characters to substitute into telephone numbers in place of the wait character.

set chat

## Examples

### Display entire chat table

```
set chat
```

### Configure a chat table entry

```
set chat name=chat1 star=4452624
```

### Remove an entry from chat table

```
set chat mchat=chat1
```

### Rename a chat table entry

```
set chat name=chat1 newname=chat2
```

## See also

See set script on page 156 for information on creating scripts that use telephone string translation.

## set config

**Purpose** Configures or displays entries in the network parameters configuration table. The network parameters configuration table holds the following information

- Network-related parameters, such as an IP address, mask, and default gateway.
- Information on how ICMP redirect messages are handled.

**Required privileges** Root privileges are required to use this command.

**Syntax**

**Configure network parameters**

```
set config [bootfile=file] [boothost=host-ipaddr]
[circuitbreaker=reset] [dhcp={on | off}] [dns=ip-addr]
[domain=domain] [gateway=ip-addr]
[ip=ip-addr] [optimize={latency | throughput}] [myname=name]
[ramsize=show] [realport=tcp-port] [redirect={listen|ignore}]
[save={on |off}] [securerealport=tcp-port] [sockets=socket-num]
[submask=mask] [tbreak={std|any|none}] [tftpboot={yes|no|smart}]
```

**Display network parameters**

```
set config
```

**Fields**

**bootfile**  
The name of a boot file on a TFTP host. Specify the full path to the file if this is required to satisfy the host's TFTP implementation. This option does **not** apply to PortServer TS 8/16.

**boothost**  
The IP address of a host from which the device server can boot using TFTP. This option does **not** apply to PortServer TS 8/16 devices.

**circuitbreaker=reset**  
Resets the circuit breaker.

**dhcp**  
Enables or disables DHCP (Dynamic Host Configuration Protocol). Turning DHCP on causes the device server to obtain an IP address from a DHCP server. The default is on.

**dns**  
The IP address of a domain name server. This parameter cannot be changed if dhcp=on.

**domain**  
The name of device server's domain.

**gateway**  
The IP address of the default gateway.

**ip**  
The device server's IP address.

**myname**

The device server's DNS name.

**nameserv**

The IP address of a name server in the device server's domain. This option does **not** apply to PortServer TS 8/16 devices.

**optimize**

Configures how the Digi device handles network latency.

**latency**

Choose latency if the Digi device will handle delay-sensitive data.

**throughput**

Choose throughput if overall network throughput is more important than latency. For Digi One IA RealPort, the default is latency. For all other models, the default is throughput.

**redirect**

Specifies how routing redirect messages should be handled.

**listen**

Accept ICMP routing redirect messages. Use this option only if you have not configured the device server to forward RIP packets.

**ignore**

Discard ICMP routing redirect messages

The default is ignore.

**realport**

The TCP port number used for RealPort connections. The default is 771.

**save**

Specifies whether configuration changes are saved. On saves configuration changes to flash memory. Off means that changes will be discarded when the device server is reset. The default is on.

**securerealport**

The TCP port number used for secure RealPort connections. The default is 1027.

**sockets**

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

Configuring TCP socket communications involves configuring the Digi device for the following types of connections:

- 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.

The base TCP socket service is used in reverse Telnet, raw, SSH, and SSL/TLS connections to identify the connection type (Telnet, raw, SSH, or SSL/TLS) and a particular port. The base socket can be any number between 2000 - 50,000.

Once the base socket is set, the port accessed and the connection type are determined by the command the user issues to access the port. The formulas for issuing commands are as follows:

Connection Type	Formula
Telnet	base socket + port number
Raw	base socket + 100 + port number
SSH	base socket + 500 + port number
SSL/TLS	base socket + 600 + port number

The following examples illustrate how these formulas work

If Base Sockets is ...	And the user specifies ...	Example	Then, the user establishes ...
1000	telnet <i>ip-address</i> 1002	telnet 192.1.1.1 1002	A Telnet connection to port 2
	telnet <i>ip-address</i> 1102	telnet 192.1.1.1 1102	A raw connection to port 2
	telnet <i>ip-address</i> 1502	telnet 192.1.1.1 1502	An SSH connection to port 2
	telnet <i>ip-address</i> 1602	telnet 192.1.1.1 1602	A SSL/TLS connection to port 2
1121	telnet <i>ip-address</i> 1122	telnet 192.1.1.1 1122	A Telnet connection to port 1
	telnet <i>ip-address</i> 1222	telnet 192.1.1.1 1222	A raw connection to port 1
	telnet <i>ip-address</i> 1622	telnet 192.1.1.1 1622	An SSH connection to port 1
	telnet <i>ip-address</i> 1722	telnet 192.1.1.1 1722	A SSL/TLS connection to port 1

### submask

The subnet mask for the subnetwork.

### tbreak

Sets the Telnet break keystroke.

Once a Telnet connection is initiated, but before the connection is established, the connection can be broken by entering a designated keystroke. This keystroke is determined by these settings.

#### std

Configures tbreak so only ^] (control right bracket) will break a Telnet connection. Example: `set config tbreak=std`

#### any

Configures tbreak so any keystroke will break a Telnet connection. For example: `set config tbreak=any`

#### none

Configures tbreak so no keystroke will break a Telnet connection. For example: `set config tbreak=none`

The default is std.

### tftpboot

(This option does not apply to PortServer TS 8/16)

Specifies booting conditions for the device server.

### yes

Always boot from the TFTP host identified on the boothost field.

**smart**

If the device server cannot boot from the TFTP host identified on the boothost field, boot from the device server's internal flash ROM instead.

**no**

Boot the device server from internal flash ROM.

The default is no.

**Example**

**Display the network parameter configuration table**

```
set config
```

set device

## set device

### Purpose

Used to:

- Configure devices used for outbound connections to use dialer scripts and chat table entries.
- Configure a different baud rate (line speed) for modems and other devices used for outgoing connections than the rate defined on the set line command.
- Display the contents of the device table.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Configure devices

```
set device [baud={no|rate}] [chat={no|index-num|chat-name}]  
[dialer={no|index-num|script-name}] name=name ports=range  
[newname=newname] [p{1-9}] [save={on | off}] [show=on]
```

#### Display device table information

```
set device [{range=range|name=name}]
```

### Fields

#### baud

Specifies the baud rate for the device.

#### no

The baud rate specified on the set line command will be used.

#### rate

The baud rate (line speed) when this device is used. This field overrides the baud rate (for this device) defined on the set line command. The range is 300 to 115,200 bps.

The default is no.

#### chat

Specifies whether a chat table entry is associated with this device.

#### no

A chat table entry is **not** associated with this device.

#### index-num

A chat table entry (index number) associated with this device.

#### chat-name

The name of a chat table entry.

The default is no.

#### dialer

Specifies whether a dialer script is associated with this device.

#### no

A dialer script is not associated with this device.

***index-num***

A script table entry (index number) associated with this device.

***script-name***

The name of a script.

The default is no.

**name**

A user-defined name for the device.

**newname**

A new name for a previously defined device.

**p{1-9}**

Integers (1-9) that can be used in the variable fields of login or dialer scripts.

**ports**

The port or range of ports available to this device (1 for SP/IA).

**range**

A device table entry or range of entries (identified by their index numbers).

**Examples****Display entire device table**

```
set device
```

**Display a range of entries in the device table**

```
set device range=4-7
```

**Configure a device**

In this example, the set device command configures a device to use a dialer script and to override the baud rate specified on the set line command.

```
set device name=OutDev ports=3-5 dialer=modemscp baud=19200
```

**See also**

- set chat on page 87
- set line on page 130
- set script on page 156
- set user on page 185

set dhcp

## set dhcp

### Purpose

Used to:

- Enable/disable DHCP (Dynamic Host Configuration Protocol). Enabling DHCP causes the device server to obtain an IP address from the host server. If DHCP is disabled, a static IP address must be defined for the device server.
- Renew the IP address of the device server. This causes the device server to discard its current IP address and obtain a new one from the host server.
- Display the lease information for the current IP address.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Configure DHCP

```
set dhcp [client_identifier=string][client_id_type=type]  
[keepalive={accept|ignore}] [run={on|off}][renew]
```

#### Display lease information for current IP address

Enter the set dhcp command with no parameters to display the lease information for the current IP address.

```
set dhcp
```

### Fields

#### client\_identifier

A text string consisting of 30 or fewer characters, which must be surrounded by quotation marks if it contains spaces. The default is an empty string. To enter non-printable characters, use hexadecimal format, which is  $\backslash xn$ , where  $n$  is a hexadecimal value (0- F). To use the backslash character as the string, use two consecutive backslashes ( $\backslash\backslash$ ).

#### client\_id\_type

A number between 0 and 255 that can be used to define the type of information in the client\_identifier string. For example, all routers could be assigned 11 as the client\_id\_type.

#### keepalive

Determines which TCP keep-alive attributes are used, those set by the DHCP server or those specified on the set tcpip command.

#### accept

The DHCP server settings are used, and the set tcpip settings are not used.

#### ignore

The set tcpip settings are used, and the DHCP server settings are ignored.

The default is accept. If the DHCP client feature is disabled, this setting has no effect.

**run**

Turns DHCP on or off. The default is on.

You must reboot the device server before this change takes affect.

**renew**

Renews the IP address of the device server.

**Examples****Enable DHCP**

```
set dhcp run=on
```

**Renew the IP address**

```
set dhcp renew
```

**See also**

See set config on page 89 for information on configuring the IP address manually.

set embmodem

## set embmodem

<b>Purpose</b>	Used to configure the embedded modem on the PortServer TS 1/3 + Modem.
<b>Required privileges</b>	Normal users can display information. Root privileges are required to change settings.
<b>Syntax</b>	<b>Configure Embedded Modem</b> <code>set embmodem [reset][init_string="AT Command"]</code>
<b>Fields</b>	<b>init_string</b> An AT command that is sent to the modem after it is reset. The default parameter is ATSO=1 (autoanswer on). The string must be enclosed in double quotes. <b>reset</b> Resets the modem, then sends the initialization string in <code>init_string</code> , or an <code>init_string</code> that was set previously.
<b>Examples</b>	<b>Configure device with embedded modem for autoanswer on</b> <code>set embmodem init_string="ATSO=1"</code> <b>Reset an embedded modem</b> The following command resets an embedded modem, and sends the initialization string that was set in the previous command. <code>set embmodem reset</code>

## set ethernet

**Purpose** Sets and adjusts Ethernet communications parameters.

**Required privileges** Root privileges are required to use this command.

**Syntax** `set ethernet [duplex={half|full|auto}] [speed={10|100|auto}]`

### Fields

#### **duplex**

Determines the mode the Digi device uses to communicate on the Ethernet network. Specify one of the following:

##### **half**

The device communicates in half-duplex mode.

##### **full**

The device communicates in full-duplex mode.

##### **auto**

The device senses the mode used on the network and adjusts automatically.

The default is half.

The value you specify for this field must match the option used by the peer. In other words, if the other side is using auto (negotiating), this device must use auto. If the other side is set for half-duplex, this side must use half-duplex.

#### **speed**

Configures the throughput rate the Digi device will use on the Ethernet network. Specify an appropriate setting for your Ethernet network, which can be one of the following:

##### **10**

The device operates at 10 megabits per second (Mbps) only.

##### **100**

The device operates at 100 Mbps only.

##### **auto**

The device senses the throughput rate of the network and adjust automatically.

The default is auto.

The value you specify for this field must match the option used by the peer. In other words, if the other side is using auto (negotiating), this device must use auto. If the other side is set for 100 Mbps, this side must use 100 Mbps.

set ethernet

**Examples**

**Configure 100 Mbps throughput**

```
set ethernet speed=100
```

**Configure full-duplex mode**

```
set ethernet duplex=full
```

**See also**

set config on page 89.

## set filter

- Purpose** Manages filters that control and record traffic over PPP connections. With the set filter command, you can
- Create filters
  - Display entries in the filter table
  - Display the contents of a filter
- About Filters** Use filters to trigger the following actions on PPP connections:
- Block or pass packets
  - Bring up or reject connections
  - Reset the idle timeout timer
  - Send information to the log file
- Rules for Creating Filters** When creating filters, follow these rules:
- The action a filter takes depends on the contents of the filter and on the type of filter it is defined as on the set user command. If the filter is referenced on the:
    - passpacket field, it will allow packets that meet filter criteria to pass through a serial port and block all others.
    - bringup field, it will bring up a connection when the port handles a packet that meets filter criteria.
    - keepup field, it will reset the timer defined on the set user idletimeout field when the port handles a packet that meets filter criteria.
    - logpacket field, it will send a message to the log file when the port handles a packet that meets filter criteria.
  - Filters are made up of 1 to 32 stanzas, each of which expresses filtering criteria.
  - Filter criteria are called tokens. Examples of tokens include IP addresses, TCP or UDP port numbers, whether a packet is incoming or outgoing, and several others.
  - Tokens must be separated by slashes (/).
  - Stanzas are processed in order. That is, first S1 (stanza 1) is processed and then S2, and so on.
  - As soon as a stanza's criteria is **completely** satisfied, filtering action occurs and subsequent stanzas are ignored. For example, if S1 specifies an IP address of 190.159.146.10 and an ICMP message type 7, a packet from that IP address carrying that ICMP message type will trigger filtering action. Subsequent stanzas will not be processed. Consequently, you must specify **and** relationships (all criteria must be satisfied) in the same stanza and **or** relationships (any of the criterion must be satisfied) in different stanzas.

set filter

- The exclamation mark (!) at the beginning of a stanza changes how the filter acts. When a packet is encountered that meets stanza criteria, the filter does **not** execute the filter function (for example, bringing up a connection) and it does **not** process any more stanzas.

### Maximum Entries in Filter Table

The filter table holds a maximum of 64 entries.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Create filters, add stanzas, or rename filters

```
set filter name=name [newname=name] [s#=token\token\token...]
```

#### Display filter table entries

```
set filter [range=range]
```

#### Display filter stanzas

```
set filter name=name show=on
```

### Fields

#### name

A name for the filter.

#### newname

A new name for a previously defined filter.

#### range

An entry or range of entries in the filters table.

#### show

##### on

Stanzas from the filter identified on the name field will be displayed.

##### off

Stanzas from the filter identified on the name field will **not** be displayed.

The default is off.

#### **s#=token/token/token...**

##### #

The number of a stanza, which can be from 1 to 32.

#### **token/token/token...**

1-32 tokens, which are the criteria by which filtering is accomplished. Separate tokens by a forward slash (/). Tokens can consist of any of the following:

Token Value	Filter Criteria
<i>servicename</i>	A name in the service table that identifies a particular process, such as Telnet (see set service on page 164).
<i>hostname</i>	The name of a host defined in the host table (see set host on page 113).
<i>protocol-number</i>	The number in an IP packet that identifies the protocol to which IP should pass the packet. Use one of the following: 1 for ICMP, 2 for IGMP, 6 for TCP, and 17 for UDP.
<i>ip-addr</i>	An IP address.
<i>ip-mask</i>	An IP mask that modifies the meaning of the <i>ip-addr</i> field.
<i>port-num</i>	A TCP or UDP port number.
<i>port-num-port-num</i>	A range of TCP or UDP port numbers.
rcv	Incoming packets.
send	Outgoing packets.
dst	Destination IP packet fields within the IP packet, such as destination IP addresses, ports, and host names.
src	Source IP packet fields, such as IP addresses, ports, or host names.
syn	Start filtering when the start of a TCP data stream is encountered. This option is always used with the fin option and is used to trigger logging (logpacket field on the set user command).
fin	Stop filtering when the end of a TCP data stream is encountered. This value is always used with the syn option and ends logging (logpacket field on the set user command.).
tcp	TCP packets.
udp	UDP packets.
icmp	ICMP packets. You can also specify a type of ICMP packet. To do so, specify <i>s1=type/icmp</i> , where <i>type</i> is the identifier type of ICMP packet, which can be any of the following identifiers: <ul style="list-style-type: none"> <li>• Echo reply: 0</li> <li>• Destination unreachable: 3</li> <li>• Source quench: 4</li> <li>• Redirect: 5</li> <li>• Echo request: 8</li> <li>• Time exceeded for a datagram: 11</li> <li>• Parameter problem on a datagram: 12</li> <li>• Timestamp request: 13</li> <li>• Timestamp reply: 14</li> <li>• Address mask request: 17</li> <li>• Address mask reply: 18</li> </ul>

## set filter

Token Value	Filter Criteria
! (exclamation)	When a packet is encountered that meets stanza criteria, the filter does not execute the filter function (for example, bringing up a connection) and it does not process any more stanzas.

### Examples

#### Display the filter table

```
set filter
```

#### Display filter stanzas

```
set filter name=filter1 show=on
```

#### Remove a filter from the filter table

```
set filter rmfilter=filter1
```

#### Create a filter on a Source IP Address

```
set filter name=filter1 s1=src/199.86.8.3
```

#### Create a filter on an ICMP packet type

In this example the set filter command creates a filter that uses an ICMP type 13 packet (destination unreachable) as filter criterion.

```
set filter name=filter1 s1=13/icmp
```

### See also

See set user on page 185 for information on associating a filter with a particular user.

**set flow**

**Purpose** Configures or displays flow control options for device server's EIA-232 serial ports.

**Required privileges** Normal users can display information. Root privileges are required to change settings.

**Syntax****Configure flow control options**

```
set flow [aixon={on|off}][altpin={on|off}] [cts={on|off}]
[dcđ={on|off}] [dsr={on|off}] [dtr={on|off}] [forcedcd={on | off}]
[itoss={on|off}] [ixany={on|off}] [ixoff={on|off}] [ixon={on|off}]
[pre-delay=milliseconds]
[post-delay=milliseconds] [range=range] [ri={on|off}]
[rts={on|off|toggle}]
```

**Display flow control options**

```
set flow [range=range]
set flow [range=range] show=rtstoggle
```

**Fields****aixon**

Determines whether the auxiliary flow control characters defined on the set keys command are used for output flow control:

**on**

Auxiliary flow control characters are used.

**off**

Auxiliary flow control characters are not used.

The default is off .

**altpin**

Determines whether the altpin option, which swaps DCD with DSR so that eight-wire RJ-45 cables can be used with modems, is used:

**on**

The altpin option is used.

**off**

The altpin option is **not** used.

The default is off.

**cts**

Determines whether CTS (clear to send) is used for output flow control:

**on**

CTS is used for output flow control.

**off**

CTS is **not** used for output flow control.

The default is off.

**dcd**

Determines whether DCD (data carrier detect) is used for output flow

## set flow

control:

**on**

DCD is used for output flow control.

**off**

DCD is **not** used for output flow control.

The default is off.

**dsr**

Determines whether DSR (data set ready) is used for output flow control.

**on**

DSR (data set ready) is used for output flow control.

**off**

DSR is **not** used for output flow control.

The default is off.

**dtr**

Determines whether DTR (data terminal ready) is used for input flow control.

**on**

DTR is used for input flow control.

**off**

DTR is **not** used for input flow control.

The default is off.

**forcedcd**

Determines whether the port acts as though DCD were always high. The primary implication is that autoconnections are launched as soon as the Digi device completes booting when this field is on and an appropriate incoming device type (see the set ports dev field) is defined for the port. The default is off.

**itoss**

Used only with software flow control (XON/XOFF) and only if ixany=on:

**on**

The character that resumes output is discarded.

**off**

The character that resumes output is **not** discarded.

The default is off.

**ixany**

Used only with software flow control.

**on**

Any received character can restart output when output has been stopped because of software flow control. Specify “on” only when communicating with devices, such as printers and terminals that use software flow control (XON\XOFF).

**off**

Output will resume only when the XON character is received.

The default is off.

**ixoff**

Determines whether to use input software flow control.

**on**

Use input software flow control.

**off**

Do **not** use input software flow control.

The default is on.

**ixon**

Determines whether to use output software flow control.

**on**

Use output software flow control.

**off**

Do **not** use output software flow control.

The default is on.

**pre-delay**

Specifies the time in milliseconds to wait after the RTS signal is turned on before sending data. The range is 0 to 5000 milliseconds, and the default is 0. This option does not apply to PortServer TS 8/16 devices.

**post-delay**

Specifies the time in milliseconds to wait after sending data before turning off the RTS signal. The range is 0 to 5000 milliseconds, and the default is 0. This option does not apply to PortServer TS 8/16 devices.

**range**

A port or range of ports to which this set flow command applies

**ri**

Determines whether RI (ring indicator) is used for output flow control:

**on**

Use RI for output flow control.

**off**

Do **not** use RI for output flow control.

The default is off.

## set flow

### **rts**

Determines whether RTS (request to send) is used for output flow control:

#### **on**

Use RTS for output flow control.

#### **off**

Do not use RTS for output flow control.

#### **toggle**

RTS is turned on when transmitting.

The default is off.

### **show=rtstoggle**

Displays settings related to the RTS toggle feature, which includes information on rts=toggle, post-delay, and predelay.

## Examples

### **Display flow control settings**

```
set flow range=1
```

### **Configure flow control settings**

```
set flow range=1 cts=on rts=on ixoff=off ixon=off
```

## See also

- set keys on page 128
- set line on page 130
- set ports on page 143

## set forwarding

### Purpose

Configures or displays IP routing options.

The device server can be configured in the following ways using this command:

- To function as an IP router using Routing Information Protocol (RIP) to dynamically maintain routes.
- To perform Proxy ARP services.
- To handle various ICMP-related functions.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Configure IP routing options

```
set forwarding [advertise=time] [breakoutsubnets={on | off}]
[icmptdiscovery={on | off}] [icmptsendredirects={on | off}]
[icmptmaskserver={on | off}] [igmp={on | off}]
[poisonreverse={on | off}] [proxyarp={on | off}]
[save={on|off}][state={off | passive | active}]
[splithorizon={on | off}] [timeout=time]
```

#### Display IP routing options

```
set forwarding
```

### Fields

#### advertise

The interval at which the device server advertises its routes. This field is used only if state=active. The range is 10 to 180 seconds. The default is 30 seconds.

#### icmptdiscovery

##### on

Send and answer ICMP Router Discovery packets.

##### off

Do **not** send and answer ICMP Router Discovery packets.

The default is off.

#### icmptmaskserver

##### on

Act as an ICMP mask server.

##### off

Do **not** act as an ICMP mask server.

The default is off.

set forwarding

### **icmpsendredirects**

#### **on**

The device server sends ICMP redirect messages when it detects a host is using a non-optimal route, such as when the host uses the device server to route to a destination that can be reached more efficiently using another router or when the destination host can be reached directly (that is, without the services of any router).

#### **off**

Do **not** send ICMP redirect messages.

The default is off.

### **igmp**

#### **on**

The device server announces itself as a router when it initializes. This means that the device server will be included in the IGMP router's group broadcasts.

#### **off**

The device server does not announce itself as a router when it initializes and will not be included in IGMP router's group broadcasts

The default is off.

### **poisonreverse**

Specifies whether the poisonreverse option is on or off.

#### **on**

The poisonreverse option is on. When this option is on, learned routes **are** propagated over the same interface on which they are learned, but the destination specified in those routes are advertised as unreachable. The splithorizon option must be on if poisonreverse is on.

#### **off**

The poisonreverse option is off.

The default is off.

### **proxyarp**

Specifies whether proxy ARP services are enabled. Proxy ARP is a technique in which a router answers ARP requests intended for another system. By pretending to be the other system, the router accepts responsibility for forwarding packets to that system. Use proxy ARP to route packets to and from serial routes on the same IP subnetwork as the device server's Ethernet interface.

#### **on**

Provide proxy ARP services.

#### **off**

Do **not** provide proxy ARP services.

The default is off.

**splithorizon**

Specifies whether the splithorizon option is enabled.

**on**

The splithorizon option is on. When this option is on, learned routes are **not** propagated from the interface on which they are learned. Use this option only if state=active.

**off**

The splithorizon option is off.

The default is on.

**save**

Specifies whether the configuration will be saved.

**on**

The configuration will be saved.

**off**

The configuration will not be saved, which means that configuration changes will be lost the next time the device server re-initializes.

The default is on.

**state**

The state of routing for the device server.

**off**

Limits routing to static routes defined in the route table. See set route on page 154.

**passive**

Configures the Digi device to use the routing information protocol (RIP) to learn routes but not to propagate them.

**active**

Configures the device server to use RIP to both learn and propagate routing information.

The default is off.

**timeout**

The time in which an entry in the routing table must be updated. If an entry exceeds the value specified here, it will be discarded. This value must be at least six times the advertise value.

The range is 60 to 1080 seconds. The default is 180 seconds.

set forwarding

## Examples

### Display the IP routing table

```
set forwarding
```

### Configure proxy ARP

```
set forwarding proxyarp=on
```

### Configure RIP

In this example, the set forwarding command configures device server to:

- Listen for and advertise RIP routing information every 45 seconds.
- Discard this route from the routing table if a routing update is not received within 270 seconds. This value is derived from the value on the advertise field. The timeout value must be **at least** 6 times the advertise value. Since no timeout is specified, the default (6 times the advertise value) is used.
- Implement split horizon.

```
set forwarding state=active advertise=45 splithorizon=on
```

## See also

See set route on page 154 for information on creating static routes.

## set host

### Purpose

Configures the host table, which contains host name-to-IP address mappings, or displays entries in the host table.

The device's IP component can use the host table and a DNS server to map host names to IP addresses. These mappings allow users to identify hosts by user-friendly names, instead of IP addresses.

Use of the host table is a convenience only. If you do not configure the host table or configure DNS, users identify hosts by IP addresses.

If the device server can access a DNS server, there is no reason to configure the host table. The PortServer TS 8/16 host table can hold up to 64 entries. The host table for other devices can hold up to 20 entries.

You can configure either of the following:

- A host table and DNS
- Either the host table or DNS

If you configure a host table and a DNS server, the device server will attempt to satisfy a request by first searching the host table and then the DNS server.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Configure host table

```
set host ip=ip-addr name=host-name range=<index#>-<index#>
```

#### Display host table entries

```
set host
```

### Fields

#### ip

The IP address to be mapped to the name specified on the name field.

#### name

The name to be mapped to the IP address specified on the ip field.

#### range

One or a range of index numbers that identify entries in the host table.

### Examples

#### Display the entire host table

```
set host
```

#### Display an entry in the host table

```
set host range=1
```

#### Configure a name-to-IP address mapping

```
set host ip=190.150.150.10 name=server1
```

### See also

See set config on page 89 for information on configuring device server to use a DNS server.

set ia

## set ia

### Purpose

Configures Digi devices for industrial automation (IA) protocols.

### Device support

The following table provides information on Digi device support for this command:

Device	Protocol Support
Digi One IA RealPort	All protocols are supported.
Digi One RealPort	IA protocols are not supported.
Digi One TS Digi One TS Wireless	Modbus and User Defined protocols are supported.
PortServer TS 2/4 MEI and Wireless	Modbus and User Defined protocols are supported.
PortServer TS 2/4 non-MEI	IA protocols are not supported.
PortServer TS 8/16	The user defined protocol is supported. All other IA protocols are not supported.

### Required privileges

Root privileges are required to use this command.

**Syntax**

There are several variants of syntax for the set ia command, depending on whether it is being used for serial port-connected devices, network-based masters, or serial master routes.

**Syntax: Serial Port-Connected Devices**

```
set ia serial [acktimeout=time-out] [acktimeoutlimit=retries]
[addextfunc={({range of functions) | all}]
[ansiescape={on | off}] [broadcast={on | off | replace}]
[checksum={bcc | crc}] [duplicatedetection={on | off}] [end=end]
[errorresponse={on | off}] [exttimeout={0-65535ms}]
[fixedaddress={auto | (1-255)}] [messagetimeout=time-out]
[naktimeoutlimit=retries] [polltimeout=milliseconds]
[polltimeoutlimit=retries] protocol=protocol [range=range]
[rmextfunc={({range of functions) | all}] [rttimeout=time-out]
[start=start] [type={master | slave}]
```

See field descriptions on page 116.

**Syntax: Network-Based Masters**

To configure a network-based master, use this syntax. This syntax is required only if you want to do the following:

- Configure one of the timeout values that will be used for communication with a network master (usually, the defaults work).
- Deactivate a class of network masters that use a specific protocol.

```
set ia netmaster protocol [addextfunc={({range of functions) |
all}] [active={on | off}] [broadcast={on | off | replace}]
[connecttimeout=time-out] [errorresponse={on | off}]
[exttimeout={0-65535ms}]
[messagetimeout=time-out]
[rmextfunc={({range of functions) | all}]
```

See field descriptions on page 121.

**Syntax: Network-Based Slaves**

To configure a network-based slave, use this syntax:

```
set ia netslave [active={on | off}] [encoding={tcp | udp}]
[ip=ip-address] port=num protocol=protocol range=range
[reconnecttime=time]
```

See field descriptions on page 122.

**Syntax: Serial Master Routes**

To configure either a network or serial route for a serial master, use this syntax:

```
set ia route [active={on | off}] [encoding={tcp | udp}]
[fixedaddress={auto | (1-255)}] [ip=ip-address] [port=num]
[protaddr=protocol-address] [protocol=protocol] range=range
[reconnecttime=time] table=range
[type={network | serial | empty}]
```

See field descriptions on page 124.

## Fields

### Fields for Serial Port-Connected Devices

The following command fields apply to configuring serial port-connected devices.

#### **set ia serial**

Specifies that this command configures a serial port-connected master or a slave.

#### **acktimeout**

Applies to the DF1 Full-Duplex, DF1 Half-Duplex, FINS, and Hostlink protocols. The period to wait for an acknowledgment from the connected device after sending a message. When this period is exceeded, the Digi device re-sends the message. The range is 0 to 60000 milliseconds. The default is 250 milliseconds.

#### **acktimeoutlimit**

Applies to the DF1 Full-Duplex, DF1 Half-Duplex, FINS, and Hostlink protocols. The number of times that the acktimeout timer can expire before the Digi device discards a message as undeliverable. The range is 0 to 255. The default is 3.

#### **addextfunc**

Applies to the Modbus RTU and Modbus Ascii protocols. Used to add to the list of Modbus functions that will use the exttimeout instead of the messagetimeout. See the exttimeout command for more details.

#### **ansiescape**

Applies to the user-defined protocol. Used to handle protocols that have an ANSI escape character as the first character in the end string (see end command) used to recognize a complete message. The typical example of this is a protocol with a start string (0x10 0x2), the end string (0x10 0x3), and the escape character 0x10 where (0x10 0x10) in the body of a message is used to specify a single 0x10. If a request is:

```
0x10 0x2 0x10 0x10 0x03 0x10 0x3
```

with the ansiescape setting to “on,” this message would get recognized correctly. With the ansiescape feature “off” (0x10 0x2 0x10 0x10 0x3), would get incorrectly recognized as the message and the rest of the message would get thrown away. This happens because the 0x10 0x3 end string is found in the message body and accidentally recognized as the end of the message.

**broadcast**

Applies to the Modbus RTU and Modbus ASCII protocols. Specifies how to handle an incoming Modbus request with a unit ID equal to 0 (the Modbus broadcast address).

**on**

Tells the Digi device to send requests to the destination device and not expect a response message in return.

**off**

Tells the Digi device to throw away the broadcast request.

**replace**

Changes a broadcast request to a normal request by replacing the unit id 0 with a value of 1.

The default is replace.

**checksum**

Applies to the DF1 Full-Duplex and DF1 Half-Duplex protocols. The error-checking method to use on this serial connection. Choose the method required by the device connected to the serial port.

**duplicatedetection**

Applies to the DF1 Full-Duplex and DF1 Half-Duplex protocols.

**on**

Filters out consecutive requests that have identical command, source, and tns bytes. This behavior is necessary for compliance with the DF1 specification.

**off**

Detection of duplicate requests is off.

The default is on.

**end**

Applies to the user-defined protocol. The character string that tells the Digi One IA RealPort that the protocol message is complete. Rules and guidelines for specifying this string are as follows:

- The string can be between 1 and 4 characters long.
- The string can be made up of printable or unprintable characters.
- To use an unprintable character, enter the character in hexadecimal format, that is, `\xhh`, where `hh` is replaced with a hexadecimal number.
- Several unprintable characters can be entered using a shortcut, enabling you to avoid entering hexadecimal digits. They are: `\t` (tab), `\r` (carriage return), `\n` (line feed).
- To use the backslash character as a delimiter, enter two backslashes (`\\`).
- To indicate that the last character should be ignored when determining the end of a message, use a `\*` (backslash asterisk). To indicate that two characters should be ignored, use `\*\*` and so on.

**errorresponse**

Applies to the DF1 Full-Duplex, DF1 Half-Duplex, Modbus RTU, and Modbus ASCII protocols. This parameter specifies whether the Digi Device sends back an error response for a request that can not be routed to the destination device or has timed out. The default for the DF1 protocols is on. The default for the Modbus protocols is off.

**exttimeout**

Applies to the Modbus RTU and Modbus ASCII protocols and is used in place of the messagetimeout setting to handle Modbus requests that have special timing requirements. This field is typically used to accommodate Modbus requests with functions that take a long time to complete. The addextfunc and rmextfunc fields are used to add and remove from the list of Modbus functions that will use the exttimeout setting. The default setting is 15,000ms.

**fixedaddress**

Applies to the Modbus RTU and Modbus Ascii protocols. Used to override the Modbus protocol address (unit id) with a fixed address. A value of auto indicates the protocol address will not be overwritten. The default setting is auto.

**messagetimeout**

Applies to all the serial IA protocols. The period in milliseconds to wait for a response to a request before discarding the message. The range is 0 to 60000 milliseconds. The default is 1000 milliseconds.

**naktimeoutlimit**

Applies to the DF1 Full-Duplex protocol. The number of negative acknowledgments (Naks) the Digi device can receive from the device connected to the serial port before discarding the message as undeliverable. The range is 0 to 255. The default is 3.

**polltimeout**

Applies to the DF1 Half-Duplex protocol. The period a master waits for a response to a poll before either polling again (see the polltimeoutlimit field) or giving up on getting a response. The range is 0 to 60000 milliseconds. The default is 250 milliseconds.

**polltimeoutlimit**

Applies to the DF1 Half-Duplex protocol. The number of polltimeouts allowed before the master gives up on getting a response to a poll. The range is 0 to 255. The default is 3.

**protocol**

The protocol to use for communication between the serial port and the device connected to it. Use the protocol required by the connected device. Specify one of the following:

**compowayf**

The connected device requires the Omron Compowayf protocol.

**df1fullduplex**

The connected device requires the Allen-Bradley DF1 Full-Duplex protocol.

**df1halfduplex**

The connected device requires the Allen-Bradley DF1 Half-Duplex protocol.

**fins**

The connected device requires the FINS protocol.

**hostlink**

The connected device requires the Hostlink protocol.

**modbusascii**

The connected device requires the Modbus ASCII protocol.

**modbusrtu**

The connected device requires the Modbus RTU protocol.

**userdefined**

The connected device requires a serial protocol not explicitly supported by the Digi device, that is, any of the protocols listed in this discussion. This protocol must meet the following conditions: (1) Each message starts with a fixed header string and ends with a fixed trailer string to differentiate messages. (2) Each protocol request is followed by a single response.

**range**

The port to which the master or slave device is connected. The default is port 1.

**rmextfunc**

Applies to the Modbus RTU and Modbus ASCII protocols. Used to remove from the list of Modbus functions that will use the exttimeout instead of the messagetimeout. See the exttimeout field for more details.

**rtutimeout**

Applies to the Modbus RTU protocol. The period in milliseconds to wait for additional characters before determining that a message is complete. The default is 20 milliseconds, and the range is 0 to 60000 milliseconds. Specifying 0 disables this timer.

**start**

Applies to the user-defined protocol. The character string that tells the Digi device that the protocol message has started. Rules and guidelines for specifying this string are as follows:

- The string can be between 1 and 4 characters long.
- The string can be made up of printable or unprintable characters.
- To use an unprintable character, enter the character in hexadecimal format, that is, `\xhh`, where *hh* is replaced with a hexadecimal number.
- There are several unprintable characters that can be entered using a shortcut, enabling you to avoid entering hexadecimal digits. They are: `\t` (tab), `\r` (carriage return), `\n` (line feed).
- To use the backslash character as a delimiter, enter two backslashes (`\\`).
- To indicate that the first character should be ignored when determining the start of a message, use a `\*` (backslash asterisk). To indicate that two characters should be ignored, use `\*\*` and so on.

**type**

Defines whether the serial entity configured with this command is a master or a slave device.

## Fields for Network-Based Masters

The following command fields apply to configuring network-based masters.

### **set ia netmaster**

Specifies that this command configures a master that is located on the network.

### **protocol**

One of the following:

- abethernet, for Allen-Bradley Ethernet.
- ethernetip, for Ethernet/IP.
- modbustcp, for Modbus/TCP.

### **active**

Determines whether this network master accepts incoming connections. The default is on.

### **addextfunc**

Applies to the Modbus TCP protocol. Used to add to the list of Modbus functions that will use the exttimeout instead of the messagetimeout. See the exttimeout field for more details.

### **broadcast**

Applies to the Modbus TCP protocol. Specifies how to handle an incoming Modbus request with a unit id equal to 0 (the Modbus broadcast address).

#### **on**

Tells the Digi device to send requests to the destination device and not expect a response message in return.

#### **off**

Tells the Digi device to throw away the broadcast request.

#### **replace**

Changes a broadcast request to a normal request by replacing the unit id 0 with a value of 1.

The default is replace.

### **connectiontimeout**

Defines the time in milliseconds to wait before closing an idle connection to a master. The range is 0 to 60000 milliseconds. The default is 0, which means this timer is disabled.

### **errorresponse**

Applies to the Allen-Bradley Ethernet and Modbus TCP protocols. This parameter specifies whether the Digi Device sends back an error response for a request that can not be routed to the destination device or has timed out. The default for all protocols is on.

**exttimeout**

Applies to the Modbus TCP protocol and is used in place of the `messagetimeout` setting to handle Modbus requests that have special timing requirements. This is typically used to accommodate Modbus requests with functions that take a long time to complete. The `addextfunc` and `rmextfunc` fields are used to add and remove from the list of Modbus functions that will use the `exttimeout` setting. The range is 0-65,535 milliseconds. The default setting is 15,000ms.

**messagetimeout**

The period to wait for a response to a request from this master to a slave connected to the serial port before discarding the message. The default is 1000 milliseconds, and the range is 0 to 6000 milliseconds.

**rmextfunc**

Applies to the Modbus TCP protocol. Used to remove from the list of Modbus functions that will use the `exttimeout` instead of the `messagetimeout`. See the `exttimeout` field for more details.

**Fields for Network-Based Slaves**

The following command fields apply to configuring network-based slaves.

**active**

Determines whether this network slave is active. The default is on.

**encoding**

Determines the transport service--either TCP or UDP--for communication with the network slave. Use this option only when the `protocol=socket` field is also specified.

**tcp**

Use for connection-oriented service.

**udp**

Use for connectionless service. If you choose UDP, packet delivery is not guaranteed.

The default is `tcp`.

**ip**

The IP address of a network slave.

**port**

The TCP or UDP port number to use when communicating with the network-based slave. The following are default port numbers:

- 502, for Modbus/TCP.
- 2222, for Allen Bradley Ethernet.
- 2101, for TCP or UDP socket connections.
- 44818, for Ethernet/IP.

**protocol**

The network protocol to use to communicate with the slave defined with this command. Use the protocol required by the network-based slave. Specify one of the following:

**abethernet**

The network slave uses the Allen-Bradley Ethernet protocol.

**ethernetip**

For communication with a network-based device that communicates using Ethernet/IP.

**modbustcp**

The network slave uses the Modbus/TCP protocol.

**socket**

The network slave uses TCP or UDP socket communication.

**range**

An identifying number for this slave. Use numbers 1 through 8.

**reconnecttime**

The time to wait between attempts to initialize communication with this slave. The range is 0 to 60000 milliseconds. The default is 4000 milliseconds. Specifying 0 means that the device server does not wait between attempts to initialize communication.

**Fields for Serial Master Routes**

The following command fields apply to configuring a serial master routes.

**protaddr**

Used to accept or ignore messages for a given route based on the protocol address contained in a message. The following lists the valid range of protocol addresses supported by each protocol:

Protocol	Range of Protocol Addresses
Modbus RTU Modbus ASCII	0 to 255
DF1 Full-Duplex and Half-Duplex	0 to 255
Omron Hostlink FINS	0 to 99

CompoWay/F does not support protocol addressing.

**range**

Identifies the route being configured. Use numbers 1 through 12.

**table**

Specifies the route table to configure, which corresponds to a serial port. For one-port devices, this field is optional.

**type**

Specifies the type of route to configure.

**network**

Use network to configure a route to a network based device.

**serial**

Use serial for routes to a serial based device.

**empty**

Use empty to remove a route entry from the route table.

**Fields for Network-Based Routes**

The following command fields are used for configuring a network-based route.

**active**

Determines whether a network route is active.

**on**

Messages will be forwarded to this route. For TCP based network routes, setting active to on initiates a TCP connection to the device specified by the network route.

**off**

Messages will not be forwarded to this route.

**encoding**

Determines the transport service--either TCP or UDP--for communication with the device specified by the network route. Use this option only when the protocol=socket is also specified.

**tcp**

Use for connection-oriented service.

**udp**

Use for connectionless service. If you choose UDP, packet delivery is not guaranteed.

The default is tcp.

**fixedaddress**

Applies to the Modbus TCP protocol. Used to override the Modbus protocol address (unit id) with a fixed address. A value of auto indicates the protocol address will not be overwritten. The default setting is auto.

**ip**

Specifies the IP address of the network route.

**port**

The TCP or UDP port number to use when communicating with the device specified by the network route. The following are default port numbers:

- 502, for Modbus/TCP.
- 2222, for Allen Bradley Ethernet.
- 2101, for TCP or UDP socket connections.
- 44818, for Ethernet/IP.

**protocol**

The network protocol to use to communicate with the device specified by the network route. Specifying socket implies using the same protocol that is being used for the serial port associated with this route. Specify one of the following:

**abethernet**

The network slave uses the Allen-Bradley Ethernet (sometimes called CSP) protocol.

**ethernetip**

For communication with a network-based device that communicates using Ethernet/IP.

**modbustcp**

The network slave uses the Modbus/TCP protocol.

**socket**

The network slave uses TCP or UDP socket communication.

**reconnecttime**

For a TCP based route, this field specifies the time to wait between attempts to establish a TCP connection with the device specified by the route. The range is 0 to 60000 milliseconds. Specifying 0 means that the Digi device does not wait between attempts to establish a connection. The default is 4000 milliseconds.

**Fields for Serial-Based Routes**

The following command fields are used for configuring a serial-based route.

**port**

The serial port number to which messages are routed. The set ia serial command configures the serial port itself.

set ia

## Examples

### Modbus RTU over a TCP tunnel

In this example, set ia commands configure a Modbus master, which is connected to serial port 1 of a Digi device, to communicate with a Modbus slave, which is connected to serial port 1 of another Digi device. The serial protocol for both connections is Modbus RTU, and the network provides a TCP tunnel connection.

Master Side	Slave Side
<pre>set ia serial protocol=modbusrtu type=master range=1  set ia route ip=192.1.1.2 protocol=socket active=on range=1 table=1 protaddr=0-255</pre>	<pre>set ia serial protocol=modbusrtu type=slave range=1</pre>

### Modbus ASCII slave

In this example, a set ia command configures a serial port-connected Modbus slave. The slave uses the Modbus ASCII protocol. Configuration of a network protocol is not required.

```
set ia serial range=1 protocol=modbusascii type=slave
```

### DF1 full-duplex slave

In this example, a set ia command configures a serial port-connected DF1 Full-Duplex slave. Like the previous example, configuration of the network protocol is not required.

```
set ia serial range=1 protocol=df1fullduplex type=slave
```

### DF1 full-duplex master

In this example, set ia commands configure a serial port-connected DF1 Full-Duplex master. Two network-based slaves using Allen Bradley Ethernet are also configured.

```
set ia serial range=1 protocol=df1fullduplex type=master
set ia route table=1 range=1 protocol=abethernet ip=192.2.2.1
active=on
set ia route table=1 range=2 protocol=abethernet ip=192.2.2.2
active=on
set ia route table=1 range=1-2 protaddr=0-255
```

## See also

See set config on page 89 for information on configuring device server to use a DNS server.

## set ippool

<b>Purpose</b>	Creates a pool of IP addresses for serial ports.
<b>Required privileges</b>	Root privileges are required to use this command.
<b>Syntax</b>	<pre>set ippool count=num-ip-addr ip=1st-ip-addr</pre>
<b>Fields</b>	<p><b>count</b> The number of IP addresses in the pool. The count can be from 1 to 64.</p> <p><b>ip</b> The first IP address in the pool.</p>
<b>Example</b>	<p>In this example, the set ippool command configures a pool of four IP addresses. These are 190.175.175.20, 190.175.175.21, 190.175.175.22, and 190.175.175.23.</p> <pre>set ippool ip=190.175.175.20 count=4</pre>
<b>See also</b>	For information on linking a user to the IP address pool, see set user on page 185.

set keys

## set keys

### Purpose

Changes the key or key sequences used to generate certain characters and command functions, or displays current key mappings for these characters and functions.

Use the carat character (^) to indicate that the Ctrl key should be held while pressing another key.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Configure key sequences

```
set keys function=keys [range=range]
```

#### Display current key mappings

```
set keys [range=range]
```

### Fields

#### *function*

One of the following characters or control functions (where ^ means “press and hold the Ctrl key”):

#### **backchar**

The back character. The default is ^b.

#### **eof**

The end of file character. The default is ^d.

#### **erase**

The erase command. The default is ^h.

#### **forwchar**

The forward key (move cursor forward). The default is ^f.

#### **intr**

The interrupt command. The default is ^c.

#### **kill**

The kill character. The default is ^u.

#### **lnext**

The literal next character (interpret the next character literally). The default is ^v.

#### **nextcmd**

Scroll forward through command history. The default is ^n.

#### **prevcmd**

Scroll backward through command history. The default is ^p.

#### **xon**

The XON character. The default is ^q.

#### **xoff**

The XOFF character. The default is ^s.

**xona**

The auxiliary XON character. The default is ^q.

**xoffa**

The auxiliary XOFF character. The default is ^s.

**range**

A range of ports. If you issue the command from a Telnet session, you must specify the range field. If you issue the command from an attached terminal, the command will work for the port to which the terminal is attached unless you use the range field to specify a different port.

**Examples****Display the key table**

In this example, the set keys command, issued from an attached terminal, displays key mapping information for the port on which the terminal is attached.

```
set keys
```

**Change a key**

In this example, the set keys command changes the key that generates an end of file character (eof) for port 1.

```
set keys eof=^h range=1
```

set line

## set line

### Purpose

Configures or displays options associated with a serial line.

### Required privileges

Normal users can display port information. Root privileges are required to change settings.

### Syntax

#### Configure line options

```
set line [baud=bps] [break={ignore|send|escape}]  
[csize={5|6|7|8}] [error={ignore|null|parmrk|dos}]  
[inpck={on|off}] [istrip={on|off}] [onlcr={on|off}]  
[otab={on|off}] [parity={o|e|n|m|s}] [range=range]  
[stopb={1|2}]
```

#### Display line options

```
set line [range=range]
```

### Fields

#### baud

The line speed (bps) for this line. Use one of the following values: 50, 75, 110, 134, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 57600, 76800, 115200, 230400. In addition, PortServer TS 8/16 devices support 100, 3600, and 460800 bps.

The default is 9600.

#### break

Specifies how the Telnet break signal is handled.

#### ignore

The Telnet break signal is ignored.

#### send

Send the Telnet break signal on the serial line when the device server receives a break signal.

#### escape

Send the escape sequence on the serial line when the device server receives a break signal.

The default is ignore.

#### csize

The character size, which can be 5, 6, 7, or 8 bits. The default is 8.

**error**

Determines how the device server handles parity errors on the line.

**ignore**

The device server ignores errors.

**null**

The device server changes the error character to a null character.

**parmrk**

The device server “marks” the error with FF (16450 error byte).

**dos**

The device server marks the error with an error character.

The default is ignore.

**inpck**

Specifies whether input parity checking is on or off.

**on**

Input parity checking is turned on.

**off**

Input parity checking is turned off.

The default is off.

**istrip**

Specifies handling of the high-order bit.

**on**

The high-order bit is stripped from each byte.

**off**

The high order bit is **not** stripped from each byte.

The default is off.

**onlcr**

Specifies handling of new-line characters.

**on**

New-line characters are mapped to carriage return/line feed characters.

**off**

No mapping of new-line characters occurs.

The default is off.

set line

**otab**

Specifies handling of output tabs.

**on**

means that output tabs are converted to eight spaces.

**off**

Output tabs are **not** converted.

The default is off.

**parity**

The parity used for the line.

**o**

Odd parity.

**e**

Even parity.

**n**

No parity.

**m**

Mark parity.

**s**

Space parity.

The default is n (no parity).

**range**

The port or range of ports to which this command applies.

**stopb**

The number of stop bits per character to use on this line. The value used here must match the setting on the device connected to this port. Use 1 or 2 stop bits.

The default is 1 stop bit.

**Examples**

**Display serial line options**

```
set line
```

**Configure baud, parity, and stop bits**

```
set line range=1 baud=150 parity=e stopb=2 csize=6
```

**See also**

See the following related commands for information on configuring serial ports:

- set ports on page 143
- set flow on page 105

## set logins

### Purpose

Use the set logins command to:

- Configure the sequence of events that occurs when a user logs into a port. This includes information the user supplies and prompts and responses.
- Display current login settings.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Configure login sequence

```
set logins [cmdprompt=string] [logprompt=string]
[login={on|off}] [passwd={on|off}] [passprompt=string]
[range=range] [rootprompt=string][verbose={on|off}]
[write={on|off}]
```

#### Display login settings

```
set logins [range=range]
```

### Fields

#### cmdprompt

The prompt displayed to a regular user who has logged in. The maximum length is 31 characters. Enclose this string in quotation marks if it includes spaces.

The default is `digi>` for normal users, and `#>` for root users.

#### login

Specifies whether a user must log into the port.

##### on

A user must log into the port.

##### off

A user is not required to log into the port.

The default is on for inbound dev types. This field is disabled when the port is configured as an auto port. See set ports on page 143 for more information.

#### logprompt

The login prompt displayed. The maximum length is 10 characters.

Enclose this string in quotation marks if it includes spaces. The default login prompt is login:

#### passprompt

The password prompt displayed. The maximum length is 10 characters. Enclose this string in quotation marks if it includes spaces. The default is password:

**passwd**

Specifies whether users are required to supply a password to access the ports specified by the range field.

**on**

Users are required to supply a password to access the ports specified by the range field.

**off**

Users do not supply a password.

The default is on. This field is disabled when the port is configured as an auto port (see set ports on page 143).

**range**

The range of ports addressed by this set logins command. When the set logins command is issued from a Telnet session, this field is required in order to identify the port to which it applies. When set logins issued from an attached terminal, the command applies to the port which the terminal is attached, unless the range field is used to specify another port.

**rootprompt (PortServer 8/16 only)**

The prompt displayed to the root user who has logged in. The maximum length is 31 characters. Enclose this string in quotation marks if it includes spaces.

The default is #>.

**verbose**

Specifies whether the device server displays connection status messages to users before the login prompt.

**on**

The device server displays connection status messages before the login prompt.

**off**

The device server does **not** display connection status messages before the login prompt.

The default is off.

**write**

Specifies whether configuration changes made by regular users can be saved and used for subsequent sessions by that user.

**on**

Configuration changes made by regular users can be saved.

**off**

Configuration changes made by regular users are **not** saved.

## Examples

### Display login information on all ports

```
set logins
```

### Display login information on a range of ports

```
set logins range=1
```

### Configure a port for user configuration

In this example, the set logins command configures a port so that users can save their login-related configuration changes and use them in future sessions:

```
set logins write=on range=1
```

### Configure the command prompt

In this example, the set logins command configures the command prompt. Since there are spaces in the new command prompt, the entry is enclosed in quotation marks.

```
set logins cmdprompt="Ent Cmd:" range=1
```

set menu

## set menu

### Purpose

Use the set menu command to:

- Create menus for users.
- Display menu table entries.
- Display lines of a menu.
- Remove a line from a menu.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Create a menu

```
set menu [c#=command] [m#=string] [range=range] [t#=string]
[name=string]
```

#### Display menu table entries

```
set menu [range=range]
```

#### Display lines of a menu

```
set menu range=range [show={on|off}]
```

#### Remove a line from a menu

```
set menu range=range rmentry=line-num
```

### Fields

#### **c#=command**

A command that is executed when a user selects this menu line.

#### **c**

Specifies that this is a command that is executed when a user selects this menu line.

#### **#**

A line number. Lines appear in numeric order on the menu.

#### **command**

Any command. Enclose commands containing spaces in quotation marks.

#### **name**

A name for the menu. If this parameter is not used, menus are named menuX, where X is the index number of the menu specified on the range field.

Names may be up to 16 characters long. Enclose names containing spaces in quotation marks.

#### **range**

A port or range of ports.

#### **rmentry**

Removes the specified line from the menu.

**m#=string**

A text or informational line for the menu.

**m**

Specifies that this is a text or informational line.

**#**

A line number for the menu. Lines appear in numeric order on the menu.

**string**

A text string. Enclose strings with spaces in quotation marks.

**show=on**

Displays menu entries identified on the range field.

**t#=string**

A title line for the menu.

**t**

Means that this is a title line.

**#**

A line number for the menu. Each menu can have two title lines (t1 and t2).

**string**

A text string. Enclose strings with spaces in quotation marks.

**Examples****Create a menu**

In this example, set menu commands create a menu with active fields that enable users to start connections to hosts named server1 and server2.

```
set menu range=4 t1="Welcome to the Communications Server"
set menu range=4 t2="Make Selection"
set menu range=4 m1="Connect to Server1" c1="connect 1"
set menu range=4 m2="Connect to Server2" c2="connect 2"
```

**Display the menu table**

```
set menu
```

**Display the contents of a menu**

```
set menu ra=1 show=on
```

**See also**

See set user on page 185 (the menu and defaultaccess fields) for information on setting up a user to use a menu.

set modem

## set modem

### Purpose

Use the set modem command to:

- Configure an association between a port and modem test and initialization scripts.
- Display the modem table.
- Clear the association between ports and modem test and initialization scripts.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Configure association between a port and test/initialization scripts

```
set modem [init={no | script / index-num}] [range=range]  
[test={no | script / index-num}]
```

#### Display modem table entries

```
set modem [range=range]
```

#### Clear association between ports and test/initialization scripts

```
set modem [init=no] [test=no]
```

### Fields

#### init

One of the following:

- The name of an initialization script (created with the set scripts command).
- The index number of an initialization script in the scripts table.
- The keyword no, which clears an association between a port and an initialization script.

#### range

The range of ports to which this command applies.

#### test

One of the following:

- The name of a test script (created with the set scripts command).
- The index number of a test script in the scripts table.
- The keyword no, which clears an association between a port and a test script.

**Examples****Display the current port's scripts**

In this example, the set modem command displays the script table.

```
set modem
```

**Display names of scripts associated with a range of ports**

```
set modem range=1-16
```

**Configure an association between a port and test and initialization scripts**

```
set modem test=test1 range=1 init=init1
```

**Clear association between a port and test and initialization scripts**

```
set modem range=1 test=no init=no
```

**See also**

See set script on page 156 for more information on creating modem scripts.

set netlogins

## set netlogins

<b>Purpose</b>	Use the set netlogins command to: <ul style="list-style-type: none"><li>• Configure the sequence of events that occur when a user logs into a server over the network (netlogin).</li><li>• Display current netlogin settings.</li></ul>
<b>Device support</b>	This command is supported on the PortServer TS 8/16 only.
<b>Required privileges</b>	Normal users can display information. Root privileges are required to change settings.
<b>Syntax</b>	<pre>set netlogins [cmdprompt=<i>string</i>] [login={on off}] [logprompt=<i>string</i>] [passprompt=<i>string</i>] [passwd={on off}] [range=<i>range</i>] [rootprompt=<i>string</i>] [verbose={on off}] [write={on off}]</pre>
<b>Fields</b>	<p><b>cmdprompt</b> The prompt displayed to a regular user who has logged in. The maximum length is 31 characters. Enclose this string in quotation marks if it includes spaces. The default is digi&gt; for normal users and #&gt; for root users.</p> <p><b>login</b> Specifies whether a user must log into the port.</p> <p><b>on</b> A user must log into the port.</p> <p><b>off</b> A user is not required to log into the port.</p> <p>The default is on for inbound dev types. This field is disabled when the port is configured as an auto port. See set ports on page 143 for more information.</p> <p><b>logprompt</b> The login prompt displayed. The maximum length is 10 characters. Enclose this string in quotation marks if it includes spaces. The default is login:.</p> <p><b>passprompt</b> The password prompt displayed. The maximum length is 10 characters. Enclose this string in quotation marks if it includes spaces. The default is password:.</p>

**passwd**

Specifies whether users are required to supply a password to access the ports specified by the range field.

**on**

Users are required to supply a password.

**off**

Users do not supply a password.

The default is on. This field is disabled when the port is configured as an auto port (see set ports on page 143).

**range**

The range of ports addressed by this set logins command. When this command is issued from a Telnet session, this command is required in order to identify the port to which it applies. When it is issued from an attached terminal, the command will apply to the port which the terminal is attached unless the range field is used to specify another port.

**rootprompt**

The prompt displayed to the root user who has logged in. The maximum length is 31 characters. Enclose this string in quotation marks if it includes spaces.

The default is #>.

**verbose**

Specifies whether the device server displays connection status messages to users before the login prompt.

**on**

The device server displays connection status messages to users before the login prompt.

**off**

The device server does **not** display connection status messages to users before the login prompt.

The default is off.

**write**

Specifies whether configuration changes made by regular users can be saved and used for subsequent sessions by that user.

**on**

Configuration changes made by regular users can be saved.

**off**

Configuration changes made by regular users are **not** saved.

set netlogins

## Examples

### Display network login information on all ports

```
set netlogins
```

### Display network login information on a range of ports

```
set netlogins range=1-2
```

### Configure a port for user configuration

In this example, the set netlogins command configures a port so that users can save their login-related configuration changes and use them in future sessions:

```
set netlogins write=on range=1
```

### Configure the command prompt

In this example, the set netlogins command configures the command prompt. Since there are spaces in the new command prompt, the entry is enclosed in quotation marks.

```
set netlogins cmdprompt="Ent Cmd:" range=1
```

## See also

set logins on page 133.

## set ports

<b>Purpose</b>	Configures or displays a port's operating parameters.
<b>Required privileges</b>	Normal users can display information. Root privileges are required to change settings.

<b>Syntax</b>	<p><b>Configure operating parameters of a port</b></p> <pre>set ports [auto={on off}] [autoservice={default   raw   rlogin   telnet} [bin={on off}] [dest={ip-adr / none} [dev=device] [dport=tcp-port / none] [edelay=milliseconds] [flushstchar={default   on   off}] [flushstchar={default   on   off}][group={none   group} [id={id-name   none}] [keepalive={on   off}] [p[1-9]=script-param][range=range] [scriptname=name] [sess=sessions] [termtype=type] [uid={id / none}]</pre> <p><b>Display operating parameters of a port</b></p> <pre>set ports [range=range] [show={script   id   autoconnect}]</pre>
---------------	--

<b>Fields</b>	<p><b>auto</b> Determines whether users of the port will bypass device server's login and password sequence and be automatically connected to the destination defined on the dest field.</p> <p><b>on</b> Users are automatically connected to a destination.</p> <p><b>off</b> Users are <b>not</b> automatically connected to a destination. The default is off.</p> <p><b>autoservice</b> Specifies the autoconnection service for this port, which is only used if auto=on. Choose one of the following:</p> <p><b>default</b> Normally means the Digi device uses the Telnet service. The exception is if the dport field is 0 or 513. In that case, rlogin is used.</p> <p><b>raw</b> Data is passed between the serial port and the TCP stream without modification.</p> <p><b>rlogin</b> The Digi device uses the remote login (rlogin) service.</p> <p><b>telnet</b> The Digi device uses the Telnet service.</p>
---------------	--

**bin**

Determines whether Telnet users of the port are provided with Telnet binary connections.

**on**

Telnet users are provided with Telnet binary connections.

**off**

Telnet users are provided with normal (ASCII) connections.

The default is off.

**dest**

The IP address of the destination system to which port users will be routed if auto=on. To disable the field, specify the keyword none.

**dev**

The device type, which defines the device connected to the port. Typically, you can use the following to define the devices listed:

Device Type	dev value
Power units	dev=power
Most printers	dev=prn
Most dumb terminals	dev=term
Most incoming modem connections	dev=min
Most outgoing modem connections	dev=mout
Most bidirectional modem connections	dev=mio
Most RealPort connections	dev=rp
Most reverse Telnet connections	dev=prn
Modem emulation	dev=pm

If the device you are configuring is not one of these listed or requires unusual flow control attributes, use the information in the table to define a device type:

Device Type	Attributes
hdial	<ul style="list-style-type: none"> <li>• The device generates a login when carrier is detected (DCD high) and data is received.</li> <li>• The device closes the port at carrier loss (DCD low).</li> <li>• DTR and RTS are low when the connection is idle.</li> <li>• This type does <b>not</b> support reverse Telnet or RealPort.</li> <li>• This type requires 10-pin cables with DCD and DTR cross-connected or an altpin cable.</li> </ul>
hio	<ul style="list-style-type: none"> <li>• The device generates a login when carrier is detected (DCD high) and data is received.</li> <li>• The device closes the port at carrier loss (DCD low).</li> <li>• DTR and RTS are low when the connection is idle.</li> <li>• This type requires 10-pin cables with DCD and DTR cross-connected or an altpin cable.</li> </ul>
host	<ul style="list-style-type: none"> <li>• The device does not generate a login.</li> <li>• The device opens the port at DCD high and closes the port at carrier loss (DCD low).</li> <li>• DTR and RTS are low when the connection is idle.</li> <li>• This type supports reverse Telnet and RealPort.</li> <li>• This type requires a cable that supports carrier detect (DCD).</li> </ul>
ia	<ul style="list-style-type: none"> <li>• The device never generates a login.</li> <li>• This type usually requires cable support for transmit, receive, and ground only, which means a 3-wire crossover cable will work. Six, eight, and ten wire crossover cables work as well.</li> <li>• Specifying dev=ia enables port support for industrial automation. See "set ia" on page 114.</li> </ul>
min	<ul style="list-style-type: none"> <li>• The device server generates a login when carrier is detected (DCD high).</li> <li>• The device server closes the port at carrier loss (DCD low).</li> <li>• DTR and RTS are high when the connection is idle.</li> <li>• This type requires a 10-pin straight-through cable or an altpin cable.</li> <li>• Do not use dev=min for RealPort and reverse Telnet connections.</li> </ul>
mio	<ul style="list-style-type: none"> <li>• The device generates a login when carrier is detected (DCD high).</li> <li>• The device closes the port at carrier loss (DCD low).</li> <li>• DTR and RTS are high when the connection is idle.</li> <li>• This type requires a 10-pin straight-through cable or an altpin cable.</li> </ul>

Device Type	Attributes
mout	<ul style="list-style-type: none"> <li>The device never generates a login.</li> <li>The device closes the port at carrier loss (DCD low).</li> <li>DTR and RTS are low when the connection is idle.</li> <li>This type requires a 10-pin straight-through cable or an altpin cable.</li> <li>dev=mout supports RealPort and reverse Telnet.</li> </ul>
pm	<ul style="list-style-type: none"> <li>The device never generates a login.</li> <li>This device's characteristics are specific to modem emulation settings for a given port.</li> <li>DTR and RTS are low when the connection is idle.</li> <li>Use dev=pm when initiating communication with the device.</li> </ul>
power (PortServer TS 8/16 only)	<ul style="list-style-type: none"> <li>The device never generates a login.</li> <li>This device's characteristics are specific to power management settings for a given port.</li> <li>DTR and RTS are low when the connection is idle.</li> <li>Use dev=power when initiating communication with the power device.</li> <li>Change from dev=power to other device name to stop communication with power unit.</li> </ul>
prn	<ul style="list-style-type: none"> <li>The device never generates a login.</li> <li>device server ignores carrier.</li> <li>DTR and RTS are low when the connection is idle.</li> <li>This type usually requires cable support for transmit, receive, and ground only, which means a 3-wire crossover cable will work. 6-, 8-, and 10-wire crossover cables work as well.</li> <li>Use dev=prn for reverse Telnet connections.</li> </ul>
rp	<ul style="list-style-type: none"> <li>The device never generates a login.</li> <li>The device ignores carrier.</li> <li>DTR and RTS are low when the connection is idle.</li> <li>This type usually requires cable support for transmit, receive, and ground only, which means a 3-wire crossover cable will work. 6-, 8-, and 10-wire crossover cables work as well.</li> <li>Use dev=rp for RealPort connections.</li> </ul>
term	<ul style="list-style-type: none"> <li>The device generates a login when it receives data.</li> <li>The device ignores loss of carrier (DCD low).</li> <li>DTR and RTS are high when the connection is idle.</li> <li>This type usually requires cable support for transmit, receive, and ground only, which means a 3-wire crossover cable will work. 6-, 8-, and 10-wire crossover cables work as well.</li> <li>Do <b>not</b> use dev=term for RealPort and reverse Telnet connections.</li> </ul>

The default is term.

With mio, mout, min, host, and hdial device types, device server lowers DTR at disconnect and holds it low for two seconds to ensure a clean disconnection.

**dport**

The TCP port for users of autoconnect ports, which is one of the following:

- For Telnet, use 23.
- For Rlogin, use 513.
- For a physical port on the device server, use the base TCP socket number and then the port number. For example (if you use the default base TCP socket number), to indicate an autoconnect Telnet connection to port 12, specify `dport=2012`. Similarly, to indicate an autoconnect raw connection to port 12, specify `dport=2112`. If you specify 0, Rlogin is used.
- None, which disables the field.

The default is 0.

**flushstchar**

Determines whether the first character of an autoconnection is discarded. If you specify `flushstchar=default`, the first character will be discarded for Telnet and Rlogin connections and will not be discarded for raw connections.

**group**

Assigns a group number to this port, which means that this port is part of a hunt group. Outgoing calls specifying this hunt group can then use any available port in the group. Use numbers that will not cause conflicts with regular port numbers. For example, on a four-port device, use numbers 5 to 99. The default is none.

**id**

Specifies a character string for the port, which can be used in console management applications to identify the device connected to the port. If there are spaces in the string, enclose this string in quotation marks.

**keepalive**

Determines whether the keepalive function is implemented with autoconnections. The default is off.

**p[1-9]=*script-param***

Letters and numbers that can be used in the variable fields of login or dialer scripts. This field is used only when the port-based autoconnect feature is on. (See the `dest` option.)

**range**

The port or range of ports to which this command applies.

**scriptname**

The name of a script (defined with the `set script` command) to use with auto connections to automatically log on to a host or run a script on a host.

**sess**

The maximum number of sessions any user can run through this port. The range is 1-9. The default is 4.

## set ports

### **show={autoconnect | *id* / *script*}**

Displays autoconnect and script configuration information for the port specified and information on who is using the port.

### **termtype**

The type of terminal assigned to the port. This information is used during multiscreen and multisession operations and is passed to the host during Telnet negotiations. Use a terminal type that is valid with the host operating system.

### **uid**

An index number in the user table that identifies a particular user for this port. If you use this field, calls from others attempting to use this port will be rejected. Specify none to disable the field.

## Examples

### **Display attributes of the current port**

```
set ports
```

### **Display attributes for a range of ports**

```
set ports range=1
```

### **Configure an autoconnect port**

In this example, the set ports command configures the port so that all incoming users are automatically connected via Telnet to the host specified on the dest field. The port is also available for outgoing connections.

```
set ports range=1 auto=on dest=199.125.123.10 dev=mio dport=23
```

## See also

See the following commands for more information on configuring serial ports:

- set line on page 130
- set flow on page 105
- set keys on page 128
- set logins on page 133
- set powerunit on page 149

## set powerunit

**Purpose** Configures, displays, or clears a power-management configuration.

**Device support** Only PortServer TS 8/16 devices use this command.

**Required privileges** Root privileges are required to use this command.

### Syntax

#### Configure power management

```
set powerunit[alarm1=alarm_threshold...alarm4=alarm_threshold]  
[group=group#] [id=device_id] [outlet=outlet#] [range=port]  
[size=number_of_outlets]  
[temp1threshold=temp_threshold...temp4threshold=temp_threshold ]  
[type=powerunit_manufacturer] [users=user_index-user_index#]
```

#### Display power management configuration

```
set powerunit [range=port][range=port group=group]  
[range=port id=id][range=port outlet=outlet]
```

#### Clear Power Management Configuration

```
set powerunit clear=on range=port
```

### Fields

#### **alarm1=*alarm\_threshold*...alarm4=*alarm\_threshold***

Configures electrical current thresholds at which alarms will be generated. You can set up to four thresholds, depending on the number of current sensors on the power control unit. Alarm1 corresponds to the first sensor on the power control unit, alarm2 to the second, and so on. If the threshold is exceeded, the power unit will emit an audible alarm and an SNMP trap will be generated (if the SNMP agent is configured for this feature). Specify thresholds in tenth of an Amp increments.

#### **group**

A group number, used to assign several power control devices or several outlets to a group that can then be managed as a single entity. Use group numbers 1 through 8.

#### **id**

A text string that can be used to identify individual managed devices (for example, a server or a router) or a group of devices. If you give the same id to multiple devices, they can be managed as a single entity.

#### **outlet**

A particular outlet or range of outlets on the power control unit.

**range**

Identifies the port or ports to which the specified power control unit is connected. You can specify ports using an individual port number, a list of ports separated by commas, or a range of ports using a dash. See the examples that follow.

Example	Range value
Individual port	range=2
List of ports	range=1,3,5
Range of ports	range=1-5

**size**

The number of outlets on the power control unit.

**tempthreshold1=temperature\_threshold, ...  
tempthreshold4=temperature\_threshold**

Configures temperature thresholds at which SNMP traps will be generated. You can set up to four thresholds, depending on the number of temperature sensors on the power control unit. tempthreshold1 corresponds to the first sensor on the power control unit, tempthreshold2 to the second, and so on. If the threshold is exceeded, an SNMP trap will be generated (if the SNMP agent is configured for this feature). Specify thresholds in tenths of a degree Celsius.

**type**

Specifies a power control unit device manufacturer. The only value for this field is baytech.

**users**

Used to assign a user permission to control the outlet. Use the user index number to assign a user to the outlet.

**Examples****Display entire power management configuration**

This example displays the entire power-management configuration.

```
set powerunit
```

**Displaying power management configuration for a port**

This example displays the power-management configuration for port 7.

```
set powerunit range=7
```

**Display configuration for an outlet**

This example displays user permissions for outlet 6.

```
set powerunit range=7 outlet=3
```

**Configure remote power control device (basic)**

This example produces a simple power-management configuration.

```
set powerunit range=8 type=baytech size=10
```

**Configure a current threshold**

This example configures the current threshold for 15 Amps.

```
set powerunit range=8 alarm1=15
```

**Configure a temperature threshold**

This example configures the temperature threshold for 32 degrees C.

```
set powerunit range=8 temp1threshold=32
```

**Configure an ID**

In this example, all the devices connected to outlets 1-4 are assigned an ID, allowing them to be managed as a single unit.

```
set powerunit range=8 outlet=1-4 id=Routers
```

**Configure a group**

```
set powerunit range=8 outlet=1-4 group=3
```

**See also**

See [power](#) on page 70 for information on managing power-management devices.

set radius

## set radius

### Purpose

Use the set radius command to:

- Configure PortServer TS 8/16 to use one or more RADIUS (Remote Authentication Dial-In User Service) servers to authenticate and maintain user profiles on dial-in users.
- Display current RADIUS configuration options.

When device server uses a RADIUS server, it authenticates users by first searching its own user table, and then, if the user is not found, searching the RADIUS server.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Configure Use of RADIUS Servers

```
set radius [accountingsocket=tcp-port] [authsocket=tcp-port]  
[primary=ip-adr] [run={on|off}] [secondary=ip-adr]  
[secret=password] [tolerant={on|off}]
```

#### Display RADIUS Configuration Status

```
set radius
```

### Fields

#### accountingsocket

The TCP port to use for accounting communication. The default is 1813. The primary and the secondary servers are not required to use the same TCP port. However, if they are different, you must issue two set radius commands: one to configure the TCP port for the primary RADIUS server, and one to configure the secondary server.

#### authsocket

The TCP port to use for authentication communication. The default is 1812. The primary and the secondary servers are not required to use the same TCP port. However, if they are different, you must issue two set radius commands: one to configure the TCP port for the primary RADIUS server, and one to configure the secondary server.

#### primary

The IP address of the primary RADIUS server. This is the server that the device server queries first. If this server is down or busy, the device server queries the secondary server (if there is one).

#### run

Specifies whether RADIUS authentication is enabled or disabled.

#### on

Enables RADIUS authentication.

#### off

Disables RADIUS authentication.

The default is off.

**secondary**

The IP address of a secondary RADIUS server.

**secret**

A password used for encryption of messages between the RADIUS server and device server. The server and device server must use the same password. The primary and the secondary servers are not required to use the same password. If they are different, however, you must issue two set radius commands, one to configure the primary RADIUS server and one to configure the secondary server. See the command examples for more information.

**tolerant**

Specifies handling of unrecognized RADIUS attributes.

**on**

Ignore unrecognized RADIUS attributes.

**off**

The connection is denied if unrecognized RADIUS attributes are present.

**Examples****Display status of the current RADIUS configuration**

```
set radius
```

**Configure device server to use a primary RADIUS server**

```
set radius run=on primary=199.150.150.10 secret=xyyzzz
```

**Configure two RADIUS servers**

In this example, the first set radius command configures the primary RADIUS server. The second set radius command configures the secondary server. Two commands are required because the two servers use different passwords (secret field).

```
set radius run=on primary=199.150.150.10 secret=xyyzzz
set radius run=on secondary=199.150.150.22 secret=abbccc
```

set route

## set route

### Purpose

Use the set route command to

- Manually configure IP routes.
- Remove routes from the route table.
- Display the contents of the route table.

The route table holds up to 50 entries.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Configure or remove IP routes

```
set route gateway=ip-adr wanname=name mask=mask metric=hops  
net=net-adr range=range
```

#### Display route table

```
set route
```

### Fields

#### gateway

The IP address of the router that is the next hop to the destination network defined on the net field. Use this field if this router is on the LAN.

You can specify any legitimate or non-legitimate gateway, as long as the IP address for the gateway is not 0.0.0.0.

#### mask

The subnet mask used by the destination network.

#### metric

The number of routers through which a datagram must pass before reaching the destination network defined on the net field.

#### net

The IP network address of the destination network.

#### wanname

The interface to use for this route, which is one of the following:

- For routes over a PPP link: The name of a set user command that defines a PPP user.
- For routes over the Ethernet interface: ether.

**Examples****Display entire route table**

```
set route
```

**Display a range of route table entries**

```
set route range=3-5
```

**Remove an entry from the route table**

```
set route rmroute=on range=2
```

**Configure a route over a WAN connection**

```
set route net=199.150.144.8 mask=255.255.255.0 metric=3  
wanname=user998 gateway=199.150.100.2
```

**See also**

See set forwarding on page 109 for information on configuring device server to use dynamic IP routes maintained by RIP.

set script

## set script

### Purpose

Use the set script command to:

- Define a modem or login script.
- Display entries in the script table.
- Display all stanzas of a script.
- Delete a script from the script table.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Configure or edit a modem or login script

```
set script [name=name] [newname=new-name]  
s{1-24}="stanza-content"
```

The *stanza\_content* value is enclosed in quotation marks.

#### Display entries in script table

```
set script range=range
```

#### Display stanzas of a script

```
set script name=name show=on
```

#### Delete a script

```
set script {rmscript=on name=name / rmscript=name}
```

### Fields

#### name

The name of the script.

#### newname

A new name for the script, identified either by its old name (on the name option) or by an index number in the script table (on the range option).

#### range

An index number in the script table (for display).

#### rmscript

Removes the specified script.

#### s {1-24}=*stanza-content*

The number of a script stanza (1 through 24) and the contents of the stanza. The contents of a stanza-content field must be enclosed in quotation marks. The contents can include any of the commands listed in the following table:

Command	Description	Example
<i>Anp</i>	Sets the following: <ul style="list-style-type: none"> <li>Character size to <i>n</i>, which can be either 7 or 8 bits.</li> <li>Parity to <i>p</i>, which can be one of the following values: 0=no parity, 1=odd 2=even 3=mark</li> </ul>	s1="A70"
<i>Bn</i>	Transmits a break signal <i>n</i> milliseconds long. If <i>n</i> is not specified, the length is 250 milliseconds.	s7="B100"
<i>Cn</i>	Sets carrier loss detection. If <i>n</i> = <ul style="list-style-type: none"> <li>0: carrier loss is not detected.</li> <li>1: the modem hangs up if the port loses DCD.</li> </ul>	S2="C1"
<i>D+m</i>	Raises a modem signal. If <i>m</i> is <ul style="list-style-type: none"> <li>1: DTR is raised.</li> <li>2: RTS is raised.</li> </ul>	
<i>D-m</i>	Lowers a modem signal. If <i>m</i> is <ul style="list-style-type: none"> <li>1: DTR is dropped.</li> <li>2: RTS is dropped.</li> </ul>	
<i>E{string}</i>	Writes the string either to <ul style="list-style-type: none"> <li>A user terminal, if running interactively.</li> <li>To a trace buffer, if running in the background.</li> </ul> <p>This string can include any of the escape commands listed in "Script Escape Commands", which follows this discussion.</p>	S10="E{Please Log In}"
<i>Fn</i>	Pauses for <i>n</i> seconds and flushes input data. The default is 0.	s1="F10"
<i>Gs</i>	Immediately does one of the following, depending on the value of <i>s</i> . If <i>s</i> is: <ul style="list-style-type: none"> <li>The number of a stanza: Control is passed to that stanza.</li> <li>+ (plus): The script is exited with a success message from E string.</li> <li>- (minus): The script is exited with a failure message from E string.</li> </ul>	s2="G7"

Command	Description	Example
Hs	Sets the carrier lost (hang-up) recovery to stanza <i>s</i> , which is the number identifying another stanza or one of the following: <ul style="list-style-type: none"> <li>• + (plus): Exit, indicating success.</li> <li>• - (minus): Exit, indicating a general failure.</li> <li>• * (star): Indicate that the remote system is busy.</li> <li>• = (equal): Indicate that the remote system is down.</li> </ul>	s2="H+"
M{string}	Writes <i>string</i> to a modem. This string can include any of the escape commands listed in "Script Escape Commands" on page 159.	s2="M{at&f;c}"
Nb	Changes the baud rate. The range is 50 to 115,200. Rates under 110 bps should be used only on expansion ports.	s4="N19200"
Pn	Pauses for <i>n</i> seconds. If you do not specify a value for <i>n</i> , the default is 1 second.	s5="P2"
Qn	Sets software flow control. If <i>n</i> is <ul style="list-style-type: none"> <li>• 0: Flow control is disabled.</li> <li>• 1: Flow control is enabled.</li> </ul>	s5="Q0"
Sn	Defines the time to wait (timeout), in seconds, for a modem signal or input data.	s2="S5"
Ts	Defines the timeout recovery state. If the timeout is exceeded, control is passed to this stanza.	s2="T8"
Un	Immediately executes the text of stanza <i>n</i> , as if it were inserted to replace this command. You can nest this command, up to a maximum of 10.	s2="U4"
W+m	Waits for a modem signal to go high. If <i>m</i> is <ul style="list-style-type: none"> <li>• 1: Wait for DCD to go high.</li> <li>• 2: Wait for CTS to go high.</li> </ul>	s6="W+1"
W-m	Waits for a modem signal to go low. If <i>m</i> is <ul style="list-style-type: none"> <li>• 1: Wait for DCD to go low.</li> <li>• 2: Wait for CTS to go low.</li> </ul>	s6="W-1"
[string]s	Defines the <i>string</i> and the stanza to jump to when the <i>string</i> is received on a communications line. This string can include any of the escape commands listed in "Script Escape Commands" on page 159.	s7="[abort]s22"

## Script Escape Commands

The following table describes the escape commands you can use in E, M, and [] command strings.

Escape Sequence	Description
<code>^c</code>	This is the character transmitted by an ASCII keyboard when the CTRL key is held down and the c key is pressed.
<code>\b</code>	Backspace
<code>\f</code>	Form feed
<code>\t</code>	Tab
<code>\n</code>	New line
<code>\r</code>	Return
<code>\\</code>	Backslash
<code>\nnn</code>	Octal byte value <i>nnn</i>
<code>\xhh</code>	Hexadecimal byte value <i>hh</i>
<code>%n</code>	Is a variable, where <i>n</i> is either a telephone number whose value comes from the <i>nn</i> field on the set user command, or one of the following special characters: <ul style="list-style-type: none"> <li>• * (star): Generates a tone equivalent to dialing * on a touch-tone phone.</li> <li>• # (pound): Generates a tone equivalent to dialing # on a touch-tone phone.</li> <li>• =: Causes a pause of 2 seconds.</li> <li>• w: causes a wait for a secondary dial tone.</li> <li>• - (minus): Completely ignored and not passed to the modem.</li> </ul>
<code>%p</code>	Is a variable, where <i>p</i> is an integer from 1 to 9. For login scripts, the value of <i>p</i> comes from the <i>pn</i> field on the set user command. For dialer scripts, options come from the <i>pn</i> field of the set device command.

set script

## Examples

### Configure a login script

This example defines a login script that does the following things:

- Waits for a login prompt and then supplies a login name.
- Waits for a password prompt and then supplies a password.

The commands to define the login script are as follows:

```
set script name=log1 s1="P2[ogin:]2 S10 T4"  
set script name=log1 s2="P1 M{user-ejm\r} S1 [sword:]3 T4"  
set script name=log1 s3="M{my-p-word\r} G5"  
set script name=log1 s4="E{login failed} G-"  
set script name=log1 s5="E{login complete} G+"
```

The actions performed by the script are as follows:

- In stanza S1:
  - P2 means “pause for 2 seconds before executing the rest of the script.”
  - [ogin:] indicates the string to wait for.
  - 2 is the stanza to jump to when the string is received.
  - S10 T4 means “wait up to 10 seconds for the string “ogin:” . If the string does not appear in that time, jump to stanza 4.”
- In stanza S2:
  - P1 means “pause for 1 second.”
  - M means “write the string that follows.”
  - {user-ejm\r} is the string to supply, which is a user name, followed by a carriage return (\r).
  - S1 means “wait 1 second for additional input, which is a password prompt.”
  - [password:] 3 is the string to wait for and the number of the stanza to jump to when the string is received.
  - T4 means “jump to stanza 4 if the S1 period is exceeded.”
- In stanza S3:
  - M{my-p-word\r} is the string to write, which is a password, followed by a carriage return.
  - G5 means “jump to stanza 5.”
- Stanza S4 is the “failure” path for the script.
  - E{login failed} is the string to write to either a terminal or a trace buffer.
  - G- means “exit the script and send a failure message to the user interface.”
- Stanza S5 is the “success” path for the script.
  - E{login complete} is the string to write to either a terminal or a trace buffer.
  - G+ means “exit the script and send a success message to the user interface.”

**Configure a dialer script**

In this example, a telephone number is passed to the modem.

```
set script name=dialer1 s1="M{atdt9524452624\r}"
```

**Display entire script table**

```
set script
```

**Display an entry in the script table**

```
set script range=4
```

**Display all stanzas in a script**

In this example, the set script command displays all stanzas of the specified script:

```
set script name=testmodem show=on
```

**See also**

- set user on page 185 for information on assigning a login script to a user.
- set chat on page 87 for information on telephone number string translation.
- "Filters for PPP Connections" on page 19 for information on using filters for PPP connections.

set secureaccess

## set secureaccess

**Purpose** Disables Digi device services for users of inbound connections.

**Required privileges** Root privileges are required to use this command.

**Syntax** **Disable device servers**  
set secureaccess level={secure | high | normal} service={on | off}

### Display current secure-access settings

```
set secureaccess
```

**Fields** **level**  
Determines which group of services are on, or available, for inbound users. Specify one of the following:

#### secure

SSH is the only service available to inbound users.

#### high

SSH, HTTP, HTTPS, SNMP, RealPort, Secure RealPort, and SSL services are available to inbound users.

#### normal

All services are available.

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

#### service

Turns a service on or off. *service* can be any of the services listed in the following table:

If you specify ...	This service is turned on or off ...
http	HTTP
https	HTTPS
realport	RealPort
reversetcp	Reverse TCP
reversetelnet	Reverse Telnet
rlogin	Remote login
rsh	Remote shell
securerealport	Secure RealPort
securesockets	Secure Socket Layer (SSL)
snmp	SNMP
ssh	SSH
telnet	Telnet

## Examples

### Disable inbound Telnet connections

```
set secureaccess telnet=off
```

### Disable all services except SSH

```
set secureaccess level=secure
```

### Display secure access settings

```
set secureaccess
```

set service

## set service

### Purpose

Use the set service command to

- Configure, or associate, names with TCP and UDP service ports for use in filters.
- Display entries in the service table.
- Remove entries from the service table.

### Allowed Service Numbers

The following table lists the service numbers (TCP and UDP ports) to which you can assign names:

Service	Port Number
FTP	21
NNTP	119
RIP	520
Login	513
Shell	514
SMTP	25
Telnet	23
TFTP	69

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Configure/associate names with TCP service ports

```
set service name=name port={udp:port | tcp:port}
```

#### Display entries in service table

```
set service [range=range]
```

#### Remove entries from the service table

```
set service [rmservice=name | rmserveice=on]
```

**Fields****name**

The name to assign the service.

**port**

The TCP or UDP port number for the service.

**range**

A range of entries in the service table, which is used to identify entries to display or delete.

**{rmservice=*name* | rmservice=*on*}**

Removes a service from the service table.

**name**

The name of a service to be removed from the service table.

**on**

Remove the service or services from the service table identified on the range field.

**Examples****Display the service table**

```
set service
```

**Display a range of entries in the service table**

In this example, the set service command displays a range of entries in the service table.

```
set service range=2-4
```

**Configure an entry in the service table**

In this example, the set service command configures a name for Telnet.

```
set service name=http port=tcp:80
```

**See also**

See set filter on page 101 for information on configuring filters.

set snmp

## set snmp

**Purpose** Configures, enables, and disables a device server's SNMP (Simple Network Management Protocol) agent.

**Required privileges** Normal user may display information. Root privileges are required to change settings.

**Syntax**

```
set snmp [auth_trap={off|on}] [cold_start_trap={on|off}]
[contact=administrator]
[curr_thresh_exc_trap=[on|off]][get_request=community]
[link_up_trap={on|off}] [location=location-string]
[login_trap={on | off}] [name=name-string] [run={off|on}]
[set_request] [temp_thresh_exc_trap={on|off}]
[trap_dest=ipaddress]
```

## Fields

### auth\_trap

Determines whether an SNMP trap is sent when an authentication error occurs.

#### on

The agent sends an authentication trap to the SNMP manager when an authentication error occurs.

#### off

The agent silently ignores SNMP requests that fail authentication.

The default is off.

### cold\_start\_trap

Determines whether an SNMP trap is sent to the SNMP manager when a reboot occurs.

#### on

The agent sends a trap when a reboot occurs.

#### off

A trap is not sent when a reboot occurs.

The default is off.

### contact

A text string that identifies a contact person, usually an administrator. If there are spaces in the text, the entry must be surrounded by quotation marks.

**curr\_thresh\_exc\_trap**

Determines whether an SNMP trap is sent to the SNMP manager when the electrical current threshold on a power control device is exceeded.

**on**

The agent sends a trap when the threshold is exceeded.

**off**

A trap is not sent when the threshold is exceeded.

The default is off.

**get\_request**

The password required to read device server SNMP managed objects. The default is "public".

**link\_up\_trap**

Determines whether an SNMP trap is sent to the SNMP manager when a network link comes up.

**on**

The agent sends a trap when the link comes up.

**off**

A trap is not sent when the link comes up.

The default is off.

**location**

A text string that describes device server's location. If there are spaces in the text, the entry must be surrounded by quotation marks.

**name**

A text string that identifies device server. If there are spaces in the text, the entry must be surrounded by quotation marks.

**login\_trap**

Determines whether the device server sends a trap each time someone attempts to log into the system.

**on**

Send a trap at each attempt to log in.

**off**

Do not send a trap each time someone attempts to log in.

The default is off.

**run**

Specifies whether the SNMP daemon is started.

**on**

Starts the SNMP daemon.

**off**

The SNMP daemon will not start.

The default is off.

set snmp

**set\_request**

Displays a prompt of a password required to write to device server SNMP managed objects. The default is private.

**trap\_dest**

The IP address of the system to which the agent should send traps.

**temp\_thresh\_exc\_trap**

Determines whether an SNMP trap is sent to the SNMP manager when the temperature threshold on a power control device is exceeded.

**on**

The agent sends a trap when the threshold is exceeded.

**off**

A trap is not sent when the threshold is exceeded.

The default is off.

**Examples**

**Display SNMP configuration**

```
set snmp
```

**Configure all trap options**

```
set snmp run=on trap_dest=190.175.178.73 auth_trap=on  
cold_start_trap=on link_up_trap=on curr_thresh_exc_trap=on  
temp_thresh_exc_trap=on
```

## set socketid

**Purpose** Configures the serial port socket ID feature.

Device servers support reverse Telnet and raw reverse Telnet connections, which enable remote users and applications to manage serial devices connected to device server ports. A socket ID is a text string that is sent at the start of a connection between a Digi device's serial port and a remote host. This feature enables easier identification of the managed device.

**Device support** PortServer TS 8/16 devices do not support this command.

**Required privileges** Root privileges are required to use this command.

**Syntax**

**Configure serial port socket ID feature**

```
set socketid range=range [state={on | off}
[string="character-string"]
```

**Display serial port socket ID settings**

```
set socketid [range=range] [verbose]
```

**Fields**

**range**  
The port or ports configured with this command.

**state**  
Turns the serial port socket ID feature on or off for the specified port. The default is off.

**string**  
An identification string, where *character-string* is made up of ASCII characters, surrounded by quotation marks. This string can be 1 to 256 bytes long.

Characters can also be embedded in the string by using escape sequences, as described in the following table:

Embedded character	Escape sequence
Backspace	\b
Form feed	\f
Tab	\t
New line	\n
Return	\r
Backslash	\\
Hexadecimal byte value <i>hh</i>	\xhh

set socketid

**verbose**

Displays the entire identification string when the string exceeds twenty characters. The verbose option is not necessary for strings under twenty characters.

**Examples**

**Display the socketid configuration for all ports**

```
set socketid
```

**Display the socketid configuration for a specific port**

In this example, the set socketid configuration for port 2 is displayed:

```
set socketid range=1
```

**Configure an identification string**

```
set socketid range=1 state=on string="\fDevice 54"
```

**Configure a hexadecimal identification string**

```
set socketid range=1 state=on string="\xae"
```

## set tcpip

<b>Purpose</b>	<p>Configures or displays operating characteristics of the device server TCP component. Configurable options include:</p> <ul style="list-style-type: none"> <li>• The TCP port used by RealPort.</li> <li>• The interval TCP waits before retransmitting an unacknowledged segment.</li> <li>• How TCP handles idle connections.</li> <li>• Socket service values for reverse Telnet connections.</li> </ul>
<b>Required privileges</b>	<p>Normal users can display information. Root privileges are required to change settings.</p>
<b>Syntax</b>	<p><b>Configure or change TCP options</b></p> <pre>set tcpip [keepalive_active={on off}] [keepalive_byte={on off}] [ip_ttl=hops] [keepalive_idle=hours:minutes:seconds] [probe_count=probe-count#] [probe_interval=probe-interval#] [rto_max=timeout#] [tcp_ttl=hops]</pre> <p><b>Display TCP settings</b></p> <pre>set tcpip</pre>
<b>Fields</b>	<p><b>keepalive_active</b> Enables or disables the keep-alive function.</p> <p><b>on</b> Enables the keep-alive function.</p> <p><b>off</b> Disables the keep-alive function.</p> <p>The default is off. However, the keep-alive function can be turned on by an application regardless of this setting. When you change this setting, you must reboot the device server.</p> <p><b>keepalive_byte</b> Specifies whether the device server sends a “garbage” byte of data, or a keep-alive byte, to force the device at the other end of the connection to respond to the keep-alive packet.</p> <p><b>on</b> The device server sends a keep-alive byte of data.</p> <p><b>off</b> The device server does not send a keep-alive byte of data.</p> <p>The default is off. When you change this setting, you must reboot the device server.</p> <p><b>ip_ttl</b> Sets the initial value of the IP time-to-live variable, which defines the maximum number of hops that a packet can survive before being discarded. The default is 64.</p>

**keepalive\_idle=hours:minutes:seconds**

Determines the period a TCP connection has to be idle before the keep-alive option is activated. The range is 10 seconds to 24 hours. The default is 2 hours.

**probe\_count**

The number of times TCP probes the other connection to determine if it is alive after the keep-alive option has been activated. The valid range for probe\_count is 5-30. The default is 10.

Digi recommends that the probe\_count default not be changed unless there is a good reason to change it. Changing the value can adversely affect Telnet connections.

**probe\_interval**

The time in seconds between each keep-alive probe. The range is 10-75 seconds. The default is 75 seconds.

Digi recommends that the probe\_interval default value not be changed unless there is a good reason. Changing the value can adversely affect Telnet connections.

**tcp\_ttl**

The initial value of the TCP time-to-live variable, which defines the maximum number of hops that a packet can survive before being discarded. The default is 64.

**rto\_max**

The TCP maximum retransmission time out in seconds. When one side of a TCP connection sends a packet and does not receive an acknowledgment from the other side within the timeout period, the sending station retransmits the packet and sets an exponential backoff timeout. This is done for each successive retransmit until the maximum retransmission timeout is reached. Then, the TCP connection resets.

**Examples**

**Configure keep-alive options**

In this example, the device server TCP component is configured to do the following:

- Begin sending keep-alive probes after a TCP connection has been idle for 10 minutes.
- Send up to 15 probes.
- Send a probe every 50 seconds.

```
set tcpip keepalive_active=on keepalive_idle=0:10:0 probe_count=15
```

**Configure TCP maximum retransmission timeout value**

In this example, the device server TCP component is configured to attempt to reconnect a dormant connection for up to 100 seconds.

```
set tcpip rto_max=100
```

## set telnetip

### Purpose

Creates, displays, or removes entries in the Telnet IP address table.

- Creates configuration profiles for Telnet communication with particular devices. That is, the set telnetip command links an IP address to particular Telnet operating parameters.
- Displays Telnet IP address table entries.
- Before removing Telnet table entries, it may be helpful to use set telnetip without any options to display the existing Telnet table entries and their corresponding index numbers.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Display current Telnet values for device server

```
set telnetip
```

#### Add entry to Telnet table

Use this form of the set telnetip command to add an entry to the Telnet table. The table can hold up to 30 entries.

```
set telnetip ip=ip-addr [mask=mask]  
[mode={none|crbin|telprnt|striplf}] range=port
```

### Fields

#### ip

The IP address to add to the Telnet table.

#### mask

The value of the mask to use for the IP address entered. The default is 255.255.255.255.

#### mode

The Telnet mode.

#### none

No special Telnet mode is set.

#### crbin

Sets a Telnet binary connection where carriage returns are added with line feeds.

#### telprnt

Used for a Telnet print connection.

The default is none.

#### range

The range of index entries to remove.

### Examples

#### Display Telnet table entries

```
set telnet
```

#### Add a Telnet table entry

```
set telnet ip=199.86.5.56 mask=255.255.255.0 mode=none
```

set terms

## set terms

### Purpose

Use the set terms command to:

- Define terminal types and the escape sequence a terminal uses when initiating and maintaining multiple sessions.
- Display entries in the term table.

The set terms command configures device server to handle terminals that are **not** connected over a network.

### Required privileges

Normal users can display information. Root privileges are required to change settings.

### Syntax

#### Configure terminals

```
set terms [clrseq=escape-seq] [npages=pages]  
[swtseq=SessNumSequence] termttype=type
```

If users are to use the Ctrl key in a key sequence defined by this command, use a carat character (^) in place of the Ctrl key when you configure the sequence.

#### Display entries in the term table

```
set terms [range=range]
```

### Fields

#### clrseq

The escape sequence that clears the terminal's current screen. This escape sequence should be the one specified by your terminal's manufacturer.

#### npages

The number of sessions available to this terminal type. This number should be the same as the number of pages of screen memory available on the terminal. The range is 1-9.

#### swtseq

A number that identifies the session and the escape sequence used to access that session. This number should be the sequence specified by your terminal's manufacturer.

There are no spaces between the number identifying the session and the key sequence used to access that session.

#### range

The range of term table entries to display or remove.

#### termttype

A name for the terminal type. This name must match the name specified on the termttype field of the set ports command, and used by hosts on your network for this type of terminal.

The device server provides two default terminal types: wy60 and wy60-e. Use the set terms command to display options associated with these types of terminals.

**Examples****Display entire term table**

```
set terms
```

**Display a range of entries in the term table**

```
set terms range=4-6
```

**Configure a terminal type**

```
set terms termttype=Jet npages=4 clrseq=^! swtseq=1^]  
swtseq=2^[swtseq=3^} swtseq=4^{
```

set time

## set time

**Purpose** Configures or displays the time and date in PortServer TS 8/16 devices.

**Required privileges** Root privileges are required to use this command.

**Syntax**  
`set time [{AM|PM}] [date=mn.day.yr] [dayofweek=day]  
[hrmode={12|24}] [time=hr.mn.sec]`

### Fields

#### **{AM|PM}**

The period of the day when hrmode=12.

#### **date**

The month (expressed numerically), day, and year (use only two digits for the year), separated by periods.

#### **dayofweek**

The day of the week (sun, mon, tue, wed, thu, fri, sat).

#### **hrmode**

Either 12 or 24.

#### **time**

The hour (24-hour clock), minute, and second, separated by periods.

### Examples

#### **Display the current time and date**

```
set time
```

#### **Set the time and date**

```
set time time=17.05 date=12.25.97
```

**set trace**

**Purpose** Configures a device server for tracing, or displays tracing information.

**Required privileges** Root privileges are required to use this command.

**Syntax****Configure tracing**

```
set trace [loghost=ip-addr][mask=type:severity]
[mode={historical | concurrent}] [state={on|off|dump}]
[syslog={on|off}]
```

**Display status of tracing information**

```
set trace
```

**Fields****loghost**

The IP address of a host to which trace messages should be sent. This host must be running the syslog daemon.

**mask=*type:severity***

Specifies the the type and severity level of events that should be traced.

***type***

One of the entries listed in the following table:

Type	Trace events associated with ...
addp	ADDP
arp	Address Resolution Protocol
cache	Routing cache
connect	connect functionality
dhcp	DHCP
dialer	Dial-out ports
dns	Domain Name System
esc	Escape sequence
ether	Ethernet
fwdr	Routing (forwarded IP packets)
ia	Industrial Automation (IA) protocols
icmp	Internet Control Message Protocol
inetd	Internet daemon (based on received packets)
ip	Internet Protocol
lpd	Line Printer Daemon
lpd_a	Line Printer Daemon (ASCII)

set trace

Type	Trace events associated with ...
lpd_h	Line Printer Daemon (hex)
netd	Net Daemon
pm	Modem Emulation Module
portsw	Portswitcher software
power	Powerunit (PortServer TS 8/16 only)
ppp	Point-to-Point Protocol
radius	RADIUS. Digi One and PortServer TS 2/4 devices do not support this feature.
realp	RealPort
rlogin	Rlogin
routed	Route Daemon
serial	Serial ports
snmp	Simple Network Management Protocol
stream	STREAMS internal data processing methodology
tcp	Transmission Control Protocol
telnet	Telnet
udp	User Datagram Protocol
udpser	Serial over UDP
user	Users
vj	Van Jacobsen header compression
wan	Wide-area network connections
*	All entities listed in this table

**severity**

The severity level, which can be one of the following:

Severity	Description
+ (plus sign)	Used to add other severity levels to the trace. This can be used to specify multiple severity trace levels on a single command or to specify multiple trace commands that add levels of severity. See the set trace examples for clarification.
- (minus sign)	Used to subtract severity levels from the trace. See the set trace examples for clarification.
critical or c (the default)	Tracing is done on only the most severe events. This level produces the least amount of trace data.
warning or w	Tracing is done on critical events and on less severe events as well. This level produces more trace data than the critical severity level, but less than info severity level.
info or i	Tracing is done on many events. It produces more trace data than previous severity levels.
debug or d	The severity level to use for debugging. Do not use this level for anything but debugging.

**mode**

Specifies the mode, or handling, of trace messages.

**historical**

All trace messages stored in the buffer may be displayed by issuing the following command: set trace state=dump.

**concurrent**

All trace messages are printed to the administrative terminal when state=on.

**state**

Specifies whether trace messages are displayed.

**on**

All messages in the trace buffer are displayed. Once the messages are displayed, the state remains on.

**off**

Tracing is off.

**dump**

All messages in the trace buffer are displayed. Once the messages are displayed, the state returns to off.

The default is off.

set trace

**syslog**

Specifies whether trace messages are sent to a host.

**on**

Trace messages are sent to the host identified on the loghost field.

**off**

Trace messages are not sent to a host.

The default is off.

**Examples**

**Display current trace settings**

```
set trace
```

**Dump a trace**

This example dumps a previously recorded trace of ARP events.

```
set trace mask=arp:warning mode=historical state=dump
```

**Configure tracing for future critical events**

```
set trace mask=arp:critical mode=concurrent state=on
```

**Use the + sign to extend the trace**

This example configures tracing for info, warning, and debug trace levels.

```
set trace mask=arp:i+w+d
```

**Use the - sign to subtract a severity level**

This example subtracts the warning severity level from the trace settings specified in the previous example.

```
set trace mask=arp:-w
```

## set udpdest

### Purpose

Configures destinations for serial over UDP communication.

The UDP destination table can hold up to 64 entries per port.

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.

Configuring UDP multicast communications involves configuring the Digi device for the following types of connections:

- 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.

### Required privileges

Anyone can display the UDP destination table. Root privileges are required to add entries.

### Syntax

#### Configure destinations

```
set udpdest [description="string"] [ipaddress=dest-ip]
[ipport=port] port=serial-port range=index
```

#### Remove destinations

```
set udpdest rmudp=on range=index port=serial-port
```

#### Display destinations

```
set udpdest [port=serial-port range=index]
```

### Fields

#### description

A description of the destination, used for easy identification. This description can be up to 16 characters long. If it includes spaces, surround the entire string in quotation marks.

#### ipaddress

The destination's IP address.

#### ipport

The UDP port number that will be used for communication with the destination.

#### port

The port or ports on which the serial device or devices reside. Enter this information in any of the following ways: port=1, port=1-2, port=1,2, port=1,2-4.

set udpdest

**range**

The index number or numbers that identify entries in the UDP destination table. Enter this information in any of the following ways: range=1, range=1-2, range=1,2, range=1,3-4.

**rmudp=on**

Removes the entries from the UDP destination table identified on the port and range fields.

**Examples**

**Display entries in the UDP destination table**

```
set udpdest port=1-2 range=1,2-4,6
```

**Remove entries from the UDP destination table**

```
set udpdest rmudp=on port=1-2 range=1,2-4,6
```

**Configure entries in the UDP destination table**

In this example, two entries are configured for the UDP destination table.

```
set udpdest port=1 range=1,2 ipaddress=192.2.2.2 ipport=50
```

**Change an entry in the UDP destination table**

In this example, one of the entries configured in the previous example is changed, that is, a different UDP port number is assigned one of the destinations.

```
set udpdest port=1 range=2 ipport=51
```

**See also**

set udpserial on page 183.

## set udpserial

**Purpose** Configures operating parameters for serial over UDP communication.

**Required privileges** This command requires root privileges.

**Syntax**

```
set udpserial [delimiters=string]
[overflowpolicy={forward | flush}] range=ports [rmax=max]
[rtime=time] [stripdelimiters={on | off}]
```

### Fields

#### **delimiters**

The string in the serial data that tells the Digi device that the message is complete and should be forwarded to the destination. If you do not specify a delimiter, the Digi device will forward a message based on the number of bytes accumulated in the buffer (rmax field.) and on the period to wait for the buffer to fill (rtime field.).

Rules and guidelines for specifying this string are as follows:

- The string can be between 1 and 4 characters long.
- The string can be made up of printable or unprintable characters.
- To use an unprintable character, enter the character in hexadecimal format, that is, `\xhh`, where *hh* is replaced with a hexadecimal number.
- There are several unprintable characters that can be entered using a shortcut, enabling you to avoid entering hexadecimal digits. They are: `\t` (tab), `\r` (carriage return), `\n` (line feed).
- To use the backslash character as a delimiter, enter two backslashes (`\\`).

There is no default delimiter.

#### **overflowpolicy**

Determines how the Digi device responds when the buffer that holds the serial data overflows. Choose one of the following:

##### **forward**

Forwards the buffer's contents to the destination.

##### **flush**

Discards the buffer's content.

The default is to forward the data.

#### **range**

The port or ports to which this command applies. Enter this information in any of the following ways: `port=1`, `port=1-2`, `port=1,2`, `port=1,2-4`.

#### **rmax**

The maximum number of bytes the buffer can accumulate before the Digi device forwards the contents to the destination. The range is 1 to 65,535 bytes. The default is 1024 bytes.

set udpserial

**rtime**

The period to wait for the buffer to fill before forwarding it to its destination. The range is 1 to 60,000 milliseconds. The default is 100 milliseconds.

**stripdelimiter**

Determines whether the Digi device strips the delimiter string from the message before sending the message to the destination.

**Examples**

**Discard the message when the buffer fills**

In this example, the serial message will be forwarded to the destination when two consecutive tab characters are encountered in the data stream. If the buffer fills before this delimiter string is encountered, the message is discarded.

```
set udpserial range=1 delimiter=\t\t overflowpolicy=flush
```

**Configure the wait period**

In this example, the time to wait for the end of a message is configured for 200 milliseconds, which doubles the default value.

```
set udpserial range=1 rtime=200
```

**See also**

set udpdest on page 181.

## set user

### Purpose

Does the following:

- Displays configuration attributes stored in the user table, such as whether a user must supply a password.
- Configures a range of options associated with users, such as whether the user automatically connects to a host or is required to supply a password.

Note: The user option SSH version 2 encryption for secure communication (SSH2) is only supported on the server version and not on the client version.

### Device support

The number of entries that can be stored in the user table varies by device.

- The PortServer TS 8/16 user table holds up to 64 entries. To accommodate additional users, PortServer TS 8/16 can use a RADIUS server. See set user on page 185.
- The Digi One and PortServer TS 2/4 user table holds up to 9 users.

### Required privileges

Root privileges are required to use this command.

### Syntax

#### Configure user attributes

```
set user [accesstime=time][addrcompress={on|off}][asynmap=map][
autoconnect={on|off}][autohost=ip-addr][autoport=tcp-port][
autoservice={default|telnet|rlogin|raw}][bringup=filter][
chapid=id][chapkey=key][commandline={on|off}][
compression={vj|none}][connectesc={off | esc-char}[
defaultaccess=service][device=device-name][dialout={on|off}][
downdly=seconds][flushstchar={default | on | off}][
idletimeout=time][ipaddr=ip-addr][ipmask=mask][
keepalive={on | off}][keepup=filter][killescchar=character][
loadkey=host:key][localbusydly=seconds][localipaddr=ip-addr][
loginscript=script][logpacket=filter][maxsessions=number][
menu={off|index-num}[mtu=bytes][n1, n2=phone-number][
name=name][netrouting={off|send|rec|both}][netservice={on|off}][
network][newname=string][outgoing={on|off}][
p1,p2...=script-parm][papid=id][pappasswd=password][
passive={on|off}][passpacket=filter][password={on|off}][
ports=ports][pppauth={none|pap|chap|both}][protocol=ppp][
protocompress={on|off}][range=range][rloginesc=char][
rmkey={on | off}][rmtbusydly=seconds][sessiontimeout=seconds][
telnetesc=character][vjslots=number]
```

#### Display entries from user table

```
{set user {[name=name]|[range=range]} |
set user name=name network}
```

#### Remove entry from user table

```
set user [range=range] [rmuser={on|name}]
```

set user

## Fields

### **accesstime (PortServer TS 8/16 devices only)**

The period in which the user can access the device server. Use the accesstime field to restrict the user's access to the time specified.

To specify day or days and hours, use the keywords in the following table:

Period	Keyword
Working week (Monday-Friday)	wk
Sunday	su
Monday	mo
Tuesday	tu
Wednesday	we
Thursday	th
Friday	fr
Saturday	sa

Specify hour ranges in the form: hr:min-hr:min or hr-hr. Use spaces to separate keywords and then enclose the entire string in quotation marks. For example:

Example	Provides access ...
accesstime=wk9:00-17:00	Monday through Friday from 9:00 a.m. until 5:00 p.m.
accesstime="wk9:00-17:00 su0-23"	Monday through Friday from 9:00 a.m. until 5:00 p.m. and all day Sunday.
accesstime="su mo fr"	All day Sunday, Monday, and Friday.

### **addrcompress**

Specifies whether the device server attempts to negotiate address compression on PPP connections.

#### **on**

The device server attempts to negotiate address compression.

#### **off**

The device server does **not** attempt to negotiate address compression.

The default is on.

**asynctmap**

A mask for PPP connections that defines which of the 32 asynchronous control characters to transpose. These characters, in the range 0x00 to 0x1f, are used by some devices to implement software flow control. These devices may misinterpret PPP transmission of control characters and close the link. This mask tells PPP which characters to transpose.

The default is FFFF, which means transpose all 32 control characters. Any combination is valid. The following are the masks most likely used:

**FFFFFFFF**

Transpose all control characters.

**00000000**

Transpose none.

**000A0000**

Transpose Ctrl-Q and Ctrl-S.

**autoconnect**

Specifies whether the user is automatically connected to another system.

**on**

A Telnet or Rlogin user will be automatically connected to another system without accessing the device server command line once the user has satisfied login and password requirements. If you specify on, you should also specify the autohost and autoport or autoservice fields.

**off**

The user will **not** be automatically connected to another system.

The default is off.

**autohost**

The IP address of a host to which this Telnet or Rlogin user should be automatically connected. Use this field only if you specify autoconnect=on.

**autoport**

The TCP port to use for the automatic connection. Use this field only if you specify autoconnect=on.

If you specify autoconnect and do not specify a TCP port, the port will be determined by the autoservice field, or—if there is no autoservice field specified—the default, port 513, which is Rlogin.

### **autoservice**

An alternate way to specify a TCP port for an autoconnect user (see the `autoport` field). Use this field only if you specify `autoconnect=on`. Specify one of the following services:

- `telnet`
- `rlogin`, or remote login
- `raw`, which means that data is passed between the serial port and the TCP stream without modification.
- `default`, which normally means the Digi device uses Telnet. The exception is if the `autoport` field is 0 or 513. In that case, `rlogin` is used.

The default is the value of the `autoport` field.

### **bringup**

The name of a filter, defined on the `set filter` command, that the device server uses to initiate a remote connection to a PPP user. If you do not use a `bringup` filter, the PPP connection will always be up. If you use a `bringup` filter, you should also use a `keepup` filter to ensure that the connection is not closed prematurely. This filter must have been created before you can reference it on this field.

### **chapid**

A character string that identifies the outbound PPP user using CHAP authentication. This is equivalent to a user or login name. The string must be 16 or fewer characters and must be recognized by the peer.

### **chapkey**

A character string that authenticates the outbound PPP user using CHAP authentication. This is equivalent to a password. The string must be 16 or fewer characters and must be recognized by the peer.

### **commandline**

Specifies whether a user can access the device server command line to issue commands.

#### **on**

A Telnet, Rlogin, PPP user can access the device server command line to issue commands.

#### **off**

A user **cannot** access the command line and **cannot** issue commands.

The default is `on`.

**compression**

Specifies whether compression is used on PPP connections.

**vj**

Van Jacobsen header compression is used on PPP connections.

**none**

Header compression is not used on PPP connections.

The default is vj, that is, Van Jacobsen Header compression is on.

**connectesc**

The escape character for users using the connect command. The default escape character is Ctrl [ (Control key and left bracket).

**defaultaccess**

Restricts the service accessible to the user. The options are:

**commandline**

The device server command line is displayed to the user.

**menu**

A menu is displayed to the user. If you specify this option, you must also specify a menu number on the menu field.

**autoconnect**

The device server automatically connects the user to the destination specified on the autohost field.

**netservice**

Starts PPP services. For inbound PPP users, defaultaccess=net service is required. Do **not** use net service for outbound PPP users.

**outgoing**

This user is limited to outgoing connections.

The default is commandline.

**device**

The name of a device or a device pool, defined with the set device command, used for outbound PPP connections.

**dialout**

Specifies whether an outbound PPP connection is started.

**on**

Starts an outbound PPP connection. A dialer script requires this field to be on to initiate outbound connections.

**off**

Disconnects an outbound PPP connection.

The default is off.

**downldly**

The number of seconds the dialer script should delay before attempting to establish a PPP connection with a previously inaccessible host. The range is unlimited. The default is 0, which means do not delay in making the attempt to reconnect.

**flushstchar**

Determines whether the first character of an autoconnection is discarded. If you specify flushstchar=default, the first character will be discarded for Telnet and Rlogin connections and will not be discarded for raw connections.

**idletimeout**

The maximum time in seconds that a PPP user's connection can be idle before the user is disconnected. The range is 0 to unlimited. The default is 0, which means that the user will never be disconnected for lack of connection activity.

**ipaddr**

The remote PPP user's IP address. Outbound PPP users can normally use the default. Possible values are:

**A specific IP address, in dotted decimal format**

For inbound PPP users, using a specific IP address means that this is the IP address to assign to the client. For outbound PPP users, using a specific IP address means that the server must recognize this address as its own or the call will not be completed.

**negotiated or 0.0.0.0**

For inbound PPP users, this means that the client will provide an address.

**ippool or 255.255.255.254**

The device server provides an address for the peer from its IP address pool. This value (ippool) can be used by inbound PPP users only.

The default is negotiated. Normally, outbound PPP users can use the default.

**ipmask**

The IP mask to apply to the address specified on the ipaddr field. When you specify a specific IP address on the ipaddr field, this field modifies the meaning of the IP address for routing purposes. The default is 255.255.255.255.

**keepalive**

Determines whether the keepalive function is implemented with autoconnections. The default is off.

**keepup**

The name of a keepup filter, defined with the set filter command, that the device server uses to maintain PPP connections. A keepup filter is one in which the reception of certain types of packets are indications to device server that the connection should be maintained.

**killscchar**

The kill character, which is used to close sessions. The default is ^u.

**loadkey=host:key**

This field applies to the devices listed in the following table:

Device	Required Hardware	Required Firmware
Digi One TS	50000771-01A or higher	82000747a or higher
PortServer TS 2	50000771-02A or higher	
PortServer TS 4	50000771-03A or higher	
PortServer TS 8	All levels	82000684c or higher
PortServer TS 16	All levels	

Where:

**host**

The IP address or DNS name of a host from which the SSH2 public key will be downloaded (using TFTP) to the Digi device.

**key**

The name of a DSA file on the host, which contains the SSH2 DSA public key. If your host's implementation requires a complete path to this file, specify the path here as well.

**localbusydly**

The number of seconds that device server delays before retrying to establish a PPP connection that could not be made because local ports were unavailable. The range is 0 to an unlimited number of seconds. The default is 0, which means there will be no delay.

**localipaddr**

The IP address of the local end of a PPP link, which can be one of the following:

**0.0.0.0**

For outbound PPP users, specifying this value means that the user will request an IP address from the remote server. Inbound PPP users do not use 0.0.0.0.

**A specific IP address**

For outbound users, specifying a specific IP address means that the Digi device will attempt to use this IP address. The remote server must agree to this request. For inbound PPP users, this IP address must be unique. That is, no other user can use this IP address and this **cannot** be the IP address of the Ethernet interface.

**loginscript**

The name of a script, defined with the set script command, to use to log in to a remote system.

Login scripts are seldom required. Use them when you are configuring Digi-device-to-Digi Device connections and the Digi device that is to be accessed requires the user to supply a password and does **not** use RADIUS. If you want to use the generic login script that comes with your Digi device, specify loginscript=loginscript. Do not use this script to log into Microsoft Windows systems.

**logpacket**

The name of a filter designed to write to the log file whenever device server handles a particular type of packet on PPP connections.

**maxsessions**

The maximum number of ports that a Telnet or Rlogin user can be logged into at the same time. A value of 0 means that the user can be simultaneously logged into all ports specified on the ports field.

**menu**

Specifies whether a menu is presented to the user, and if so, which menu.

***index-num***

The menu, identified by an index number in the menu table, that will be presented to this user.

**off and 0 (zero)**

No menu is presented to the user.

The default is off.

**mtu**

The maximum transmission unit (frame size in bytes) to use for this PPP connection. For PPP connections, the MTU is negotiated, so enter 1500, the largest size device server will permit the remote host to send. For PPP users, the range is 128 to 1500 bytes, and the default is 1500 bytes.

**n1,n2...**

Phone numbers (up to 10) to dial to request a PPP outgoing connection, which dialer scripts reference. If you enter more than one number, when device server encounters a busy signal, it tries these numbers in the order specified here. This field is required for outbound PPP connections that use modems. You can enter this number as digits only, with dashes (-) separating digits, or with commas.

**name**

The name that identifies this user.

**netrouting**

Specifies how Routing Information Protocol (RIP) routing updates are handled on connections to this PPP user. Use this field only if the user is an IP router.

**off**

This user is not included in RIP updates.

**send**

Propagate RIP updates to this user, but do not accept RIP updates from this user.

**receive**

Accept RIP updates from this user, but do not send RIP updates to this user.

**both**

RIP updates will be sent to and received from this user.

The default is off .

**netservice**

Specifies whether PPP connections are allowed.

**on**

Allows PPP connections for the user.

**off**

Allows no PPP connections for the user.

To configure inbound PPP users, you must specify netservice=on.

**network**

Displays network-related options associated with the user specified on the name field.

**newname**

A new name for a previously defined user.

**outgoing**

Specifies whether the user can initiate outgoing serial connections.

**on**

The user can initiate outgoing serial connections. For outbound users, outgoing=on is required.

**off**

The user cannot initiate outgoing connections

**p1, p2 ...**

Letters and numbers that can be used in the variable fields of login or dialer scripts. p1 is typically used to supply user names and p2 passwords.

**papid**

A character string that identifies the outbound PPP user using PAP authentication. This is equivalent to a user (or login) name. The string must be 16 or fewer characters and must be recognized by the peer.

**pappasswd**

A character string that authenticates the outbound PPP user using PAP authentication. This is equivalent to a password. The string must be 16 or fewer characters and must be recognized by the peer.

**passive**

Specifies whether the device server waits for the remote system to begin PPP negotiations, or can initiate PPP negotiations on its own.

**on**

The device server waits for the remote system to begin PPP negotiations.

**off**

The device server may initiate PPP negotiations.

The default is off.

Do not set both sides of a PPP connection to passive=on.

**passpacket**

The name of a filter designed to allow packets meeting filter criteria to pass through device server serial ports on PPP connections.

**password**

Specifies whether a device server password is required of this user.

**on**

A device server password is required of this user.

**off**

A password is not required of this user.

The default is on.

**ports**

A port or range of ports that this user can access.

**pppauth**

Determines whether authentication is required for inbound PPP connections and, if so, what kind.

**none**

The remote user does not require PPP authentication.

**chap**

CHAP authentication is required.

**pap**

PAP authentication is required.

**both**

Both CHAP and PAP authentication is required.

The default is none.

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

**protocompress**

Specifies whether the device server attempts to negotiate protocol compression on PPP connections.

**on**

The device server attempts to negotiate protocol compression on PPP connections.

**off**

The device server will **not** negotiate protocol compression.

The default is on.

**protocol=ppp**

Specifies that this is a PPP user, which is required for all PPP users.

**range**

Identifies an entry or range of entries in the user table to display or remove.

**rloginesc**

A different escape character than the ~ (tilde) character. This character is used for disconnecting from the remote host.

**rmkey**

Enables or disables the SSH2 public key defined on the loadkey field.

**on**

Enables the SSH2 public key defined on the loadkey field.

**off**

Disables the SSH2 public key defined on the loadkey field.

The default is on.

### **rmtbusydly**

The number of seconds that device server delays before reattempting a connection to a remote system that was previously inaccessible. The range is 0 to an unlimited number of seconds. The default is 0, which means no delay.

### **sessiontimeout**

The maximum time in seconds that a user may be connected. The range is 0 to an unlimited number of seconds. The default is 0, which means that there is no limit.

### **telnetesc**

The Telnet escape character for this user. The default is ^] (Ctrl and right bracket).

### **vjslots**

The number of slots used for Van Jacobsen header compression. The number of slots you configure should correspond to the expected maximum number of simultaneous connections using Van Jacobson header compression on this WAN interface. To avoid excessive processor usage, configure only the number you will need.

The default is 16 and the range is 4 to 255.

## **Examples**

### **Display entire user table**

```
set user
```

### **Display a range of entries in the user table**

```
set user range=2-7
```

### **Display a single user**

```
set user ra=1
```

### **Configure an autoconnect user**

```
set user name=user4 autoconnect=on autohost=199.193.150.10  
autoport=23 defaultaccess=autoconnect
```

### **Configure an inbound PPP user**

```
set user name=pppin protocol=ppp defaultaccess=netservice  
netservice=on  
set user name=pppin ippaddr=ip-pool localipaddr=143.191.3.4
```

### **Configure an outbound PPP user**

```
set user name=pppout protocol=ppp papid=pppout pappasswd  
set user name=pppout device=genmdm localipaddr=0.0.0.0 outgoing=on  
nl=4452624
```

## set wlan

**Purpose** Configures wireless devices, or displays the status of wireless devices, by displaying entries in the wireless LAN (wlan) configuration table.

**Device support** This command is only available for the Digi One TS Wireless, PortServer TS 2 MEI Wireless, and PortServer TS 4 MEI Wireless.

**Required privileges** Root privileges are required to use this command.

### Syntax

#### Configure entries

```
set wlan [authentication={open_system|shared_key}]
[auto_ssid={on|off}]
[country_code={United_States|other_country_code_string}]
[density={low|medium|high}]
[diversity={primary|secondary|tx_pri_rx_div}]
[encryption_key=key][encryption_mode={none|64_bit|128_bit}]
[rts_threshold=threshold][fragmentation_threshold=threshold]
[ssid=id-string]
```

#### Display status of wireless devices / Display entries in the wlan table

```
set wlan
```

or:

```
show wlan
```

### Fields

#### authentication

Specifies the authentication used for the wireless device.

#### open\_system

The wireless device uses open system authentication.

#### shared\_key

The wireless device uses shared key authentication. If authentication is changed to shared\_key and encryption key length is zero, the user is warned. Authentication is unaffected by the setting for encryption mode.

The default is open\_system.

**auto\_ssid**

Specifies whether the wireless device automatically detects available Set Service identifiers (SSIDs) or uses a configured SSID.

**on**

The wireless device automatically detects available SSIDs in its neighborhood and arbitrarily selects an SSID. If the arbitrarily chosen SSID is using encryption that does not match the current encryption mode and key, the device will be unable to associate with an access point.

**off**

The wireless device will use the configured SSID. Setting `auto_ssid` to off is not allowed if SSID is not set to some value other than "".

The default is on.

**country\_code**

The country code for the device's radio. The default is United States. Enter "set wlan ?" at the command line to get the list of country codes supported by the firmware release in your device.

**density**

The number of access points in the vicinity.

**low**

One wireless access point is in the vicinity.

**medium**

Two wireless access points are in the vicinity.

**high**

Three wireless access points are in the vicinity.

The default is low.

**diversity**

The antenna choice for transmit and receive.

**primary**

Use the primary antenna for transmit and receive.

**secondary**

Use the secondary antenna for transmit and receive.

**tx\_pri\_rx\_div**

Use the primary antenna for transmit and both antennae for receive.

The default is `tx_pri_rx_div`.

**encryption\_key**

A zero, ten, or 26 digit (depending on encryption mode) hexadecimal encryption key. Ignored if `encryption_mode=none`.

TEnter either zero digits (""), 10 digits, or 26 digits. No other lengths are accepted. If the key does not have the right number of digits for the current encryption mode, or if the encryption key length is changed to zero and authentication is `shared_key`, a warning is displayed.

Authentication is not affected by the setting for `encryption_mode`.

Encryption key is a read-only field, it cannot be displayed.

**encryption\_mode**

The encryption mode, which can be one of the following:

**none**

The device does not encrypt data packets.

**64\_bit**

The device uses WEP 64 encryption. This option requires a 5 byte (10 digit) encryption key.

**128\_bit**

The device uses WEP 128 encryption. This option requires a 13 byte (26 digit) encryption key.

The default is none.

If encryption mode is changed to 64 or 128, and the encryption key is not of the correct length, the user is warned.

**fragmentation\_threshold**

The number of bytes used for the fragmentation boundary for directed messages. The range is 256 to 2346 (even numbers only). The default is 2346.

**rts\_threshold**

The number of bytes used for the RTS/CTS handshake boundary. The range is 0 to 3000. The default is 1600.

**ssid**

The desired Set Service Identifier (SSID) for the wireless device. The SSID is an ASCII printable character string ranging from 1 to 32 bytes in length (excludes the backslash character “\”). Specifying `ssid=""` causes the SSID field to be cleared and `auto_ssid` to be set to on unless `auto_ssid` is also specified in the same `set wlan` command. Specifying any string other than `""` causes `auto_ssid` to be set to off, unless `auto_ssid` is also specified in the same `set wlan` command. Not used by the wlan device if `auto_ssid=on`. The default is “digi”.

### **Fields displayed by set wlan**

When using set wlan or show wlan to display the status of wireless devices, the following information is displayed:

- The current settings for all of the configuration fields except encryption\_key (which cannot be read)
- Current link status
- Current channel
- Current SSID
- Radio firmware version and hardware ID
- Receive signal strength
- Current transmit power
- Current transmit speed
- A list of visible networks, including BSSIDs of Access Points and their associated SSIDs.

The access point with which the radio is currently associated is displayed with asterisks to the left of the information.

In addition to the configurable fields and their current settings, set wlan displays the following information about the wireless device:

#### **access\_points**

A list of detected access points including the following information for each: Channel, SSID, bssid, average noise level, average signal level.

#### **current\_channel**

Indicates which channel is currently being used in the wireless device.

#### **current\_link\_status**

Indicates the current status for the link between the radio and the Access point.

#### **current\_ssid**

Indicates which SSID is currently being used by the wireless device. This may be different than the SSID requested in the set ssid command.

#### **current\_transmit\_speed**

The current transmit speed for the radio. Can be 1, 2, 5.5, or 11 MB.

#### **radio\_firmware\_version**

The version of the firmware in the radio. It is displayed in the form x.xx, where x is the major revision and xx is the minor revision.

#### **radio\_hardware\_revision**

The hardware revision of the radio. It is displayed in the form *n*, where *n* is a digit indicating the revision

#### **receive\_signal\_strength**

The current receive signal strength as reported by the radio. Ranges are from 0 – 100. The value displayed indicates the signal strength as follows:

Value Range	Receive Signal Strength
0-25	Very Low
26-49	Low
50-74	Strong
75-100	Excellent

**Example****Configure wireless devices**

```
set wlan ssid="homeBase" encryption_mode=128
encryption_key=ab1F793f01578ebf567afeb567
set wlan ssid="homeBase" em=128 ek=ab1F793f01578ebf567afeb567
```

**Display current settings for a wireless device**

```
set wlan
```

Which displays the following:

The Wireless LAN is: Not Activated

```
Diversity                : tx_primary_rx_div
Country Code             : United States
RTS Threshold            : 1600
Fragmentation Threshold : 2346
Authentication           : open_system
Density                  : low
Auto SSID                : Off
Desired SSID             : "latency"
Current SSID             : "latency"
Encryption Mode          : none
Current Channel          : 1
Current Link Status      : Associated
Receive Signal Strength  : 55
Current Transmit Speed   : 11 Mb
Radio Hardware Revision  : 1
Radio Firmware Revision  : 3.70
```

**Visible Networks:**

```
SSID                    : "beethoven"
BSSID                   : 00:90:d1:08:9c:54
Channel                 : 11
Average Noise Level     : 0
Average Signal Level    : 49

SSID                    : "beethoven"
BSSID                   : 00:a0:f8:9e:90:e4
Channel                 : 8
Average Noise Level     : 0
Average Signal Level    : 16

SSID                    : "beethoven"
BSSID                   : 00:40:96:a0:a5:95
```

set wlan

```
Channel                : 5
Average Noise Level    : 0
Average Signal Level   : 60

*SSID                  : "latency"
*BSSID                 : 00:02:2d:7f:a7:a9
*Channel               : 1
*Average Noise Level   : 0
*Average Signal Level  : 59
```

**See also**            show on page 203

**show**

**Purpose** Displays the following information on Digi One and PortServer TS 2/4 devices:

- Configuration settings.
- Current versions of the Boot, POST, and OS components.

**Device support** This command applies to Digi One and PortServer TS 2/4 devices.

**Required privileges** Anyone can use this command.

**Syntax** `show option [range=range]`

**Fields** **option**  
One of the following options:

Option	Displays events associated with ...	Works with Range Field
altip	set altip setting	yes
arp	set arp settings	yes
auth	set auth settings	yes
boot	boot version. This option applies to PortServer TS 8/16 devices only.	no
buffers	set buffers. This option applies to Digi One TS and PortServer TS 2/4 devices running firmware 82000747a or higher and PortServer TS 8/16 devices running firmware 82000684c or higher.	yes
chat	set chat settings	yes
config	set config settings	no
device	set device settings	yes
dhcp	set dhcp setting	no
ethernet	set ethernet settings	no
flow	set flow settings	yes
forwarding	set forwarding settings	no
host	set host settings	yes
ia netmaster	set ia netmaster settings	no
ia route	set ia netslave settings	no
ia serial	set ia serial settings	yes
ippool	set ippool settings	no

show

Option	Displays events associated with ...	Works with Range Field
keys	set keys settings	yes
lines	set line settings	yes
logins	set logins settings	yes
menu	set menu settings	yes
modem	set modem settings	yes
ports	set ports settings	yes
radius	set radius settings	no
route	set route settings	yes
script	set script settings	yes
secureaccess	set secureaccess settings	no
service	set service settings	yes
snmp	snmp settings	no
socketid	socketid settings. This option does <u>not</u> apply to PortServer TS 8/16 devices.	yes
tcpip	set tcpip settings	no
telnetip	set telnetip settings	yes
terms	set terms settings	yes
time	set time settings. This option applies to PortServer TS 8/16 devices only.	no
trace	set trace settings	no
udpdest	set udpdest settings	yes
udpserial	set udpserial settings	yes
user	set user settings	yes
version	Version of POST, Boot, and EOS running on the device server.	no
wlan	set wlan settings	no

### range

A configuration table entry or range of entries.

### Examples

#### Display current versions of POST, Boot and EOS

```
show version
```

#### Display settings for a particular user

```
show user range=3
```

**status****Purpose**

Displays information about your current Telnet or connect session.

**Required privileges**

Anyone can use this command.

**Syntax**

```
status
```

**Example**

In this example, the status command provides information on the user's current Telnet session.

```
status
```

**See also**

See close on page 54. Typically, the status command is used to determine which Telnet sessions to close.

telnet

## telnet

### Purpose

Establishes a Telnet session with a remote system.

### Required privileges

Anyone can use this command.

### Syntax

```
telnet {hostname | host-ip-addr} [tcp-port]
```

### Field Descriptions

#### **hostname**

The name of the host to which you want a Telnet session. DNS must be configured on the device server to use this option.

#### **host-ip-addr**

The IP address of the host to which you want a Telnet session.

#### **tcp-port**

The TCP port assigned the Telnet application on the remote system. The default is 23, the port typically used for Telnet.

### Examples

#### **Establish a Telnet session using a host name**

In this example, the telnet command establishes a Telnet session using a host name. The default TCP port (23) is used.

```
telnet host1
```

#### **Establish a Telnet session using an IP Address**

In this example, the telnet command establishes a Telnet session using an IP address. The default TCP port (23) is used.

```
telnet 192.192.150.28
```

#### **Establish a Telnet session to a device server port from the LAN**

In this example, a user on the LAN initiates a Telnet connection to port 4 on a device server named host-1.

```
telnet host-1 2004
```

## traceroute

**Purpose** Displays a list of routers through which an IP packet passes on its way to a particular destination.

**Required privileges** Anyone can use this command.

**Syntax** `traceroute ip-addr|name`

**Field** ***ip-addr | name***  
Either the IP address or the DNS name of the host to which you want a route traced.

**Examples** **Trace a route using an IP address**

```
traceroute 199.150.150.74
```

**Trace a route using a name**

In this example, the traceroute command traces a route to a host using a host name.

```
traceroute poe
```

uptime

## **uptime**

**Purpose** Displays the amount of elapsed time since the last reboot.

**Required privileges** Anyone can use this command.

**Syntax** `uptime`

**Example** `uptime`

## wan

**Purpose** Initiates and controls wide-area network (WAN) connections, or displays the status of current WAN connections.

**Required privileges** Anyone can display the status of WAN connections. Root privileges are required to initiate or control WAN connections.

**Syntax** **Initiate and control WAN connections**  
`wan [close=user-name] [initmodem=range] [start=user-name]  
[testmodem=range] [verify={all|user-name}]`

**Display status of WAN connections**

`wan [range=range]`

### Fields

**close**

Closes an outbound connection. The connection is identified by a user name.

**initmodem**

Executes the modem initialization script associated with the port or ports specified, where *range* specifies either a port or range of ports.

**start**

Places the connection in the start-up condition. The connection is identified by a user.

**testmodem**

Executes the modem test script associated with the port or ports specified. See set modem on page 138 for information on test scripts.

**verify**

The verification performed by the command.

**all**

Verifies that all connections are associated with real users, that is, users that are defined in the configuration.

**waname**

Verifies that the user has been defined in the configuration.

Only incorrectly configured WAN interfaces produce a message in response to this command. If WAN interfaces are configured correctly, no message is returned.

wan

## Examples

### Initiate a WAN connection

```
wan start=user-ppp01
```

### Close a WAN connection

```
wan close=user-ppp01
```

### Display WAN status information

In this example, the wan command displays the status of the connection on port 2.

```
wan range=2
```

## See also

- set modem on page 138
- set filter on page 101

## who

**Purpose** Displays a list of current device server users.

**Required privileges** Anyone can use this command.

**Syntax** `who [range=tty-tty]`

**Field** **range**  
Either a tty connection or a range of connections identified by tty connection number.

**Examples** **Display a list of all current users**

```
who
```

**Display a range of users**

```
who range=5-10
```

who

**A**

- abbreviating commands 49
- abort output signal 79
- access control
  - See security features
- access permissions
  - configuring 83
  - displaying 83
- access time 186
- add line feed characters 66
- address compression 186
- Address Resolution Protocol (ARP)
  - tracing events associated with 177
- admin command 51
- Allen-Bradley DF1 Full-Duplex protocol 116, 119
- Allen-Bradley DF1 Half-Duplex protocol 116
- Allen-Bradley Ethernet protocol 125
- alternate IP addresses 80
- altip table
  - configuring entries in 80
  - displaying entries in 80
  - removing entries from 74
- answering calls 25
- are you there signal 79
- arp table
  - adding ethernet address 81
  - configuring entries in 81
  - displaying entries in 81
  - removing entries from 74
- async map 186
- asynchronous control characters 187
- auth table
  - configuring entries in 82
  - displaying entries in 82
  - removing entries from 74
- authentication 195
  - for wireless devices 197
  - open system 197
  - shared key 197
- autoconnect
  - configuring ports 143
  - configuring users 187

**B**

- baud rate, configuring 130
- bidirectional modem connections 144
- block or pass packets 101
- boot command 52
- break signal 79
- break signal handling 130
- bring up or reject connections 101
- bringup filter 19, 188
- buffers 59

**C**

- CHAP authentication 38, 188, 195
- character size, configuring 130
- chat scripts, configuring 87

## chat table

- how to configure 88
- removing entries from 74
- circuit breaker 45, 57
- clear errors 57
- clear statistics 63
- clear the maximum current detected 71
- close command 54
- closing a connection 54
- closing a WAN connection 210
- command line
  - accessing 11
  - configuring access to 38, 188
  - restricting user access to 189
- command prompt 133
- commands
  - abbreviating 49
  - descriptions 51–211
  - navigation and editing keys 49
  - online help for 49
  - syntax conventions 50
- compression 189
- compression on PPP connections 185
- configuration
  - displaying 56
- configuration management
  - copying configuration to and from remote host 48
  - copying to a remote host or terminal 56
  - displaying configuration 56
  - displaying current Boot, POST, and OS components for a device 203
  - overview 48
  - resetting configuration to defaults 48
  - restoring defaults 52
  - restoring from a remote host or terminal 56
  - upgrading firmware 48
- configuration table
  - removing entries from 74
- configure a device 95
- configure access for two IP addresses 84
- configure mixed access 84
- configure no access for an IP Address 84
- configuring outbound PPP user 17
- connect command 55, 189
- connect session status 205
- connections 209
- control a device with a device range 71
- control a device with an ID 71
- copying the configuration to a host or terminal 56
- country code 198
- cpconf command 56
- create a menu 137
- CSP protocol 125
- current time and date 176

**D**

- date and time, setting 176

- default gateway, configuring 89
- default service for user 189
- density 198
- destinations for serial over UDP communication 181
- device table
  - configuring entries in 94
  - removing entries from 74
- device type
  - bidirectional modem connections 144
  - default on set ports command 146
  - dumb terminals 144
  - hdial 145
  - hio 145
  - host 145
  - ia 145
  - incoming modem connections 144
  - min 144, 145
  - mio 144, 145
  - modem emulation 144
  - mout 144, 146
  - outgoing modem connections 144
  - parameter on set ports command 144
  - pm 144, 146
  - power 144, 146
  - power units 144
  - printers 144
  - prn 144, 146
  - RealPort connections 144
  - reverse Telnet connections 144
  - rp 144, 146
  - term 144, 146
- DF1 Full-Duplex protocol 116
- DF1 Half-Duplex protocol 116
- DHCP
  - See Dynamic Host Configuration Protocol
- dialer script 161
- dialout connections, enabling 185
- dip switches 57
- disable device servers 162
- disabling inbound Telnet connections 163
- disabling services 44, 163
- disconnecting calls 25
- display buffers command 59
- display command 57
- display configuration 56
- display errors 57
- display operating options 66
- display outlet status 71
- display power unit status 71
- display statistics 63
- displaying attributes ports 148
- displaying Boot, POST, and OS components of a device 203
- displaying current device server users 211
- displaying current secure-access settings 162
- displaying device configuration settings 203
- displaying login information for ports 135
- displaying operating parameters of a port 143
- displaying the current time and date 176
- DNS
  - See domain name system
- domain name system
  - configuring a host file 33
- Domain Name System (DNS)
  - configuring a host file 33
  - tracing events associated with 177
- dumb terminals 144

- Dynamic Host Configuration Protocol (DHCP)
  - enabling/disabling 96
- E**
  - echo replies 68
  - embedded modem
    - configuration 98
    - configuring 48
    - set embmodem command 98
  - encryption 43, 198
  - encryption key 198
  - erase character 79
  - erase line signal 79
  - error handling on lines 131
  - errors
    - displaying and clearing 57
  - escape character 79
  - ethernet connection
    - configuring 89
    - set ethernet command 99
  - Ethernet interface
    - communications parameters 99
    - configuring 12
  - event tracing 177
  - exit command 61
- F**
  - filter
    - bringup 19, 188
    - configuring 19, 101
    - criteria 19
    - displaying the filter table 101
    - for PPP connections 19
    - keepup 19, 190
    - logpacket 19
    - passpacket 194
    - using with TCP service ports 164
  - filter table
    - creating entries in 101
    - displaying entries in 101
    - removing entries from 74
  - filters
    - passpacket 19
  - FINS protocol 116
  - flow control
    - configuring 105
    - displaying current parameters 105
  - forwarding 109
  - frame protocol 63
  - FTP service 164
- G**
  - go ahead signal 79
- H**
  - hdial device type 145
  - help 49
  - help command 62
  - high-order bit handling 131
  - hio device type 145
  - host connection, testing 68
  - host device type 145
  - host table
    - configuring 113
    - displaying entries in 113
    - removing entries from 74, 113
  - Hostlink protocol 116, 119

hunt group 80, 147

## I

ia device type 145

### ICMP

configuring ICMP router discovery 109

mask server 109

routing redirect messages 90

idle timeout 190

### IGMP 110

### inbound ports

configuring access to 37

incoming modem connections 144

### industrial automation (IA)

configuring 20

device type for 145

DF1 full-duplex master 126

DF1 full-duplex slave 126

for network-based masters 115, 121

for network-based routes 124

for network-based slaves 115, 122

for serial master routes 115

for serial port-connected devices 115, 116

for serial-based routes 125

Modbus ASCII slave 126

Modbus RTU over a TCP tunnel 126

set ia command 114

info command 63

initialization script 138

initiate a connection on a port 55

initiating a WAN connection 210

input parity checking 131

### Internet Control Message Protocol (ICMP)

tracing events associated with 177

### Internet Protocol 177

interrupt process signal 79

### IP address

configuring 12

displaying lease information for 96

for a remote user 190

renewing 96

### IP routing

configuring 28, 109

configuring or removing 154

displaying the routing table 109

static routes 154

IP routing table 112

### ippool table

configuring entries in 127

removing entries from 74

## K

keepalive function 190

keepup filter 19, 190

keepup filter 190

key mappings 128

kill character 191

kill command 65

## L

lease information for an IP address 96, 98

line options 130

line speed 130

line, configuring 130

load key 191

load new boot code 52

load new firmware from a TFTP host 52

load new POST code 52

logging on to a remote system 78

login prompt 133

login script 192

Login service 164

### logins

configuring 133

displaying current settings 133

over a network (netlogin) 140

prompt for 133

scripts for 156

logpacket filter 19

loose source routing 69

## M

### menu table

configuring entries in 136

displaying entries in 136

removing entries from 74

### menus

configuring 136

configuring for users 192

displaying 136

removing 136

min device type 144, 145

mio device type 144, 145

Modbus ASCII protocol 119

### Modbus protocol

configuration guidelines 20

displaying information for 64

set ia command 114

Modbus RTU protocol 119

mode command 66

### modem

connections for 144

scripts for 156

set modem command 138

test and initialization scripts for 138

### modem emulation

answering calls 25

cable signal assignments 24

common user scenarios 22

configuring 22

device type for 144

disconnecting calls 25

originating calls 25

### modem table

displaying entries in 138

mout device type 144, 146

## N

network configuration parameters

displaying 89

network login (netlogin) 140

network parameters

configuring 89

displaying 89, 193

network statistic tables 63

network statistics

clearing and displaying 63

new-line character handling 131

newpass command 42, 67

NNTP service 164

no option signal 79

## O

Omron Compowayf protocol 119

online help 49, 62

open system authentication 197

- operating system, updating 53
- originating calls 25
- outbound ports
  - configuring access to 38
  - restricting access to 82
- outgoing modem connections 144
- output devices 94
- output tab handling 132

**P**

- PAP authentication 194, 195
- parity 132
- passpacket filter 19, 194
- password
  - configuring for login prompt 134
  - creating 67
  - issuing 42
  - prompt for 133
  - requiring of a user 194
- ping Command 68
- pm device type 144, 146
- Point-to-Point Protocol (PPP)
  - configuring connections 13
  - configuring users 195
- poison reverse, configuring 110
- ports
  - buffers 59
  - configuring 143
  - configuring device types 144
  - killing a session on 65
  - operating parameters for 143
  - reconnecting to 73
- power
  - command 70
  - device type 144, 146
  - over serial ports 45
  - power-management configuration 149
  - units 144
- powerunit table
  - configuring entries in 149
  - displaying entries in 149
  - removing entries from 74
- PPP
  - address compression 186
  - authentication 195
  - closing connections 209
  - compression 185
  - configuring 13
  - configuring connections by set user
    - command 185
  - configuring inbound PPP user 196
  - configuring outbound PPP user 196
  - enabling and disabling connections for users 193
  - filters for connections 19
  - inbound connections for 14
  - initiating connections 209
  - negotiations 194
  - outbound connections for 17
  - protocol compression 195
  - users 13, 195
- printers 144
- prn device type 144, 146
- protocol
  - statistics for 63
- protocol compression 195
- protocols
  - Address Resolution Protocol (ARP) 81

- Allen-Bradley Ethernet 125
- CSP 125
- DF1 Full-Duplex 116
- DF1 Half-Duplex 116
- Dynamic Host Configuration Protocol (DHCP) 89, 96
- FINS 116
- for industrial automation devices 20, 114
- frame 63
- Hostlink 116, 119
- Internet Protocol 177
- Modbus 20, 114
- Modbus ASCII 119
- Modbus RTU 119
- Omron Compowayf 119
- Point-to-Point protocol (PPP) 13, 195
- Routing Information Protocol (RIP) 109
- Simple Network Management Protocol (SNMP) 34, 166
- user-defined 21, 114, 119
- wlan 63
- proxy ARP 31
  - configuring 110
  - services 109

**Q**

- quit command 72

**R**

- RADIUS
  - set radius command 39, 152
  - using 39
- RealPort
  - access to output ports 84
  - configuring 12
  - connections 144
- RealPort connections 144
- rebooting
  - device server 52
  - time since last 208
- remote login (rlogin) 78
- reset the idle timeout timer 101
- resetting the circuit breaker 45
- restoring configuration
  - from a host or terminal 56
  - to defaults 52
- restricting access to the device 185
- reverse Telnet connections 144
- RIP
  - See Routing Information Protocol
- rlogin command 78
- root session
  - temporary 51
  - terminating 72
- route table
  - configuring entries in 154
  - displaying contents of 154
  - removing entries from 74
  - removing routes from 154
- routing
  - configuring dynamic routes 109
  - configuring static routes 154
  - tracing of 207
- Routing Information Protocol (RIP)
  - configuring 109
  - configuring dynamic routes using 30
  - service number for 164
  - updating 193

rp device type 144, 146

## S

script

- assigning to ports 138
- clearing association with ports 138
- creating 156
- deleting 156
- dialer script 161
- displaying 156
- login 160, 192
- removing from the scripts table 156

script table

- configuring entries in 156
- deleting scripts from 156
- displaying entries in 156
- removing entries from 74

secure access 162

secure communication 43

security features

- configuring 36
- configuring SSH version 2 encryption 43
- controlling access to command line 38
- controlling access to inbound ports 37
- controlling access to outbound ports 38
- controlling access to services 44
- controlling access to the configuration 36
- issuing user passwords 42
- restricting access to inbound ports 38
- using CHAP authentication for PPP users 38
- using RADIUS to authenticate users 39

send command 79

send information to the log file 101

serial line options 130

serial over UDP communication

- configuring 183
- displaying statistics for 64
- operating parameters for 183

serial port

- configuring 130
- local IP address 191
- socket ID feature 169

serial port settings 13

service table

- configuring entries in 164
- displaying entries in 164
- removing entries from 74

services

- FTP 164
- Login 164
- NNTP 164
- RIP 164
- set service command 164
- Shell 164
- SMTP 164
- Telnet 164
- TFTP 164

session

- clearing 65
- resetting 65
- terminating 61, 72

session timeout 196

set arp command 81

set auth command 82

set buffers command 85

set chat command 87

set config command 89, 93

set dhcp command 96

set embmodem command 98

set ethernet command 99

set filter command 101

set flow command 105

set forwarding command 109

set host command 113

set ia command 114

set ippool command 127

set keys command 128

set line command 130

set logins command 133

set menu command 136

set modem command 138

set netlogins command 140

set ports command 143

set powerunit command 149

set radius command 152

set route command 154

set script command 156

set secureaccess command 162

set service command 164

Set Service Identifier (SSID) 199

set snmp command 166

set telnetip command 173

set terms command 174

set time command 176

set trace command 177

set udpserial 183

set user command 185

using filters with 19

set wlan command 197

shared key authentication 197

Shell service 164

show command 203

Simple Network Management Protocol (SNMP)

configuring 166

set snmp command 166

simple ping 69

SMTP service 164

SNMP

See Simple Network Management Protocol

socket ID feature 169

split horizon, configuring 111

SSH version 2 encryption 43

SSIDs 198

start bits, configuring 130

statistics 63

status command 205

stop bits, configuring 130, 132

strict source routing 69

synchronize process signal 79

syntax conventions 50

## T

TCP options 171

TCP service ports 164

TCP socket service 91

Telnet

binary connections 144

changing options for a session 66

command 206

connection status 206

displaying options for a session 66

displaying status of current session 205

escape character for 196

establishing a connection 206

IP address table 173

service number for 164

- telnetip table
  - configuring entries in 173
  - displaying entries in 173
  - removing entries from 74
- temporary root session 51
- temporary root session, initiating 51
- term device type 144, 146
- term table
  - configuring entries in 174
  - displaying 174
  - displaying entries in 174
  - removing entries 174
  - removing entries from 74
- terminal types 174
- terminals
  - configuring 174
  - configuring screen memory 174
  - escape sequences 174
- test script 138
- TFTP host, configuring 89
- TFTP service 164
- time and date, setting 176
- traceroute command 207
- tracing a route 207
- tracing, configuring 177
- tunnel 126
- turn on binary mode 66

## U

- UDP destination table 181
  - configuring entries in 181
  - displaying entries in 181
  - removing entries from 181
- UDP See User Datagram Protocol
- uptime command 208
- user attributes
  - common configurable user features 47
  - configuring 46, 185
- User Datagram Protocol (UDP)
  - tracing events associated with 178
- user table
  - configuring entries in 185
  - displaying entries in 185
  - removing entries from 74, 185
- user-defined protocol
  - configuration guidelines 21
  - field for 119
  - set ia command 114
- users
  - configuring 185
  - displaying 185
  - displaying current users 211
  - removing 185

## V

- Van Jacobsen header compression 178, 189, 196

## W

- wan command 209
- WAN connections
  - closing 209
  - configuring routes over 155
  - initiating and controlling 209
- WEP 128 encryption 199
- WEP 64 encryption 199
- who command 211
- wide-area network (WAN) connections 178, 209
- wireless devices
  - configuring 27, 197
  - set wlan command 197
- wireless LAN configuration table
  - configuring entries in 197
  - displaying entries in 197
- wlan protocol 63